The author(s) shown below used Federal funds provided by the U.S. Department of Justice and prepared the following final report:

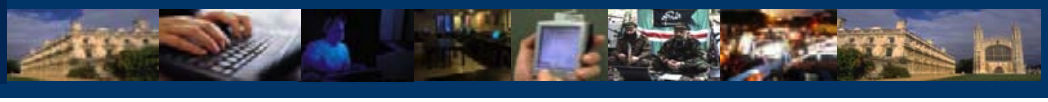
Document Title:	**The Impact of Information Security in Academic Institutions on Public Safety and Security: Assessing the Impact and Developing Solutions for Policy and Practice**
Author(s):	**Steffani A. Burd**
Document No.:	**215953**
Date Received:	**October 2006**
Award Number:	**2004-IJ-CX-0045**

This report has not been published by the U.S. Department of Justice. To provide better customer service, NCJRS has made this Federally-funded grant final report available electronically in addition to traditional paper copies.

Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions

Strengthening Our Infrastructure and Public Safety



The Impact of Information Security in Academic Institutions on Public Safety and Security:

Assessing the issues and developing solutions for policy and practice

For more information, please contact:
Steffani A. Burd, Ph.D.
sburd@infosecurityresearch.org
917.783.8496

This project was supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

ABSTRACT

Academic institutions face a barrage of information security incidents such as data theft, malicious software infections, hacks into their computer networks, and infiltration of other entities via their networks. Adverse impacts of these incidents include compromised private data and intellectual property, substantial financial losses, and potential threats to critical infrastructure, public safety, and national security. Despite these issues, little research has been conducted at the policy, prac theoretical levels, and few policies and cost-effective controls have been developed.

The purpose of this research study was to address the need for objective data and to develop a practical roadmap for policy and practice. Study design incorporated quantitative field survey, qualitative interview, and empirical network analysis methods. Seventy-two information security professionals in academic institutions completed the survey, twelve professionals participated in the interviews, and two institutions provided network activity data. Response rates were, respectively, 12%, 80%, and 100%. Instrumentation included the Information Security in Academic Institutions (ISAI) survey, ISAI interview protocol, and Higher Education Network Analysis (HENA) tool.

Results indicate that, overall, academic institutions are currently developing a baseline level of security. Participants' strengths include their information security professionals' dedication, use of evaluation techniques, and range of technologies implemented. Challenges they face involve improving existing practices, boosting awareness and senior administration's sponsorship, and tightening policies. The proposed roadmap involves six steps with recommendations and tips for tailoring the roadmap to each institution's needs. To ensure that academic institutions do not become the weakest link in America's information security chain, future research should focus on developing best practices, enhancing assessment technologies, quantifying vulnerabilities and threats, and exploring effective policies.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

EXECUTIVE SUMMARY

Background

Academic institutions face a barrage of information security incidents such as data theft, malicious software infections, hacks into their computer systems, and infiltration of other entities via their networks. Adverse impacts of these incidents include compromised private data and intellectual property, substantial financial losses, and potential threats to critical infrastructure, public safety, and national security. Despite these issues, little research has been conducted at the policy, practice, or theoretical levels, and few policies and cost-effective controls have been developed.

The purpose of this research study was three-fold: 1) create an empirically-based profile of issues and approaches; 2) develop a practical roadmap for policy and practice; and 3) advance the knowledge, policy, and practice of academic institutions, law enforcement, government, and researchers.

Method

Study design incorporated three methods: quantitative field survey; qualitative one-on-one interviews; and empirical assessment of institutions' network activity. Seventy-two information security professionals in academic institutions completed the survey, twelve professionals participated in the interviews, and two institutions provided network activity data. Response rates were, respectively, 12%, 80%, and 100%. Instrumentation included the Information Security in Academic Institutions (ISAI) survey, ISAI interview protocol, and Higher Education Network Analysis (HENA) tool. Survey data collection involved simple random sampling from the Department of Education's NCES IPEDS database, recruitment via postcard, telephone, and email, web-based survey administration, and three follow-ups.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Interview data collection involved a combination of simple random and convenience sampling, recruitment via telephone and email, and face-to-face or telephone interviews. Network analysis data collection involved convenience sampling, recruitment via telephone and email, installing HENA on participants' systems, and six months of data collection.

Results

Results indicate that, overall, academic institutions are currently developing a baseline level of security. This study's participants have a number of strengths to leverage, particularly their information security professionals' dedication, wide use of evaluation techniques, and range of technologies implemented. Participants also face several challenges in maintaining information security at their institutions. High-impact challenges that are within the information security professionals' control revolve around improving existing practices, boosting awareness and senior administration's sponsorship, and tightening information security policies. Fortunately, these challenges are inter-related, so improvement in one area will facilitate improvement in the others. The following paragraphs briefly summarize the project's findings.

Environment. Over three-fourths of participants reported the number of attacks on their institutions this year has increased or remained the same, as compared to last year. They have experienced a range of results of information security incidents; the most frequently cited were laptop theft, copyright infringement, denial of service attacks, bot infections, and unauthorized access to their information, systems or networks. Of note is that over half of these incidents relate directly to potential compromise of personally identifiable information. Fortunately, laws and regulations appear to be improving information security at participants' institutions; overall, participants rated their impact as moderate to high. The most influential laws and regulations were the Family Educational Rights and Privacy Act

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

(FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLB), Sarbanes-Oxley, and California Law SB1386. Participants' strategic objectives reflected a mix of concerns for the end-users, the institution, legal compliance, and their own professional standards; the three most frequently reported strategic objectives were to protect end-users' privacy, fulfill ethical responsibility, and fulfill legislative regulation. Participants also reported a wide range of challenges to maintaining information security at their institutions. The two most frequently cited high-impact challenges were privacy concerns and academic freedom, and roughly two-thirds of the top ten high-impact challenges concerned the awareness and support of senior executives and end-users. Consistent with these challenges, results indicated that information security at the participants' institutions typically lacks full-time support and accountability. Over half of the participants' institutions do not employ a full-time Information Security Officer or person with a similar role, and over half have zero full-time staff members dedicated to information security.

Policy. Developing, distributing, and enforcing formal information security policies are areas that typically need greater attention. Specifically, less than one quarter of the participants have a formal policy in place, and almost half of the participants use a combination of formal and informal policy. While roughly two-thirds of participating institutions have provided their end users with the information security policy within the past 12 months, less than half of participating institutions have required their end users' officially agreement to the information security policy within the past 12 months. Further, while violations of the information security policy involve a range of internal and external consequences, their enforcement is variable; over half of the participants indicated that the consequences for violating the information security policy over the past 12 months has been either inconsistent or there is no real consequence.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information. Participants in this study share sensitive information – that is, personally identifiable information (e.g., social security number, date of birth, medical data) and non-public information (e.g., technical, medical, government-related research data) - with a variety of government agencies; the three most frequently cited were the Department of Education, Student and Exchange Visitor Information System (SEVIS), and Internal Revenue Service (IRS). They use a broad range of methods to protect their sensitive information; the three most frequently used methods are firewalls, role-based access control, and physical separation.

People. Participants use a relatively wide range of methods to raise awareness of information security in their institutions. Methods that were cited as most frequently used were emails to users, posting information on the website, and tips and techniques. The methods that were rated as most effective were emails to users, tips and techniques, mandatory part of orientation, and formal courses offered by IT department. Almost ninety percent of participants do not require end users to attend mandatory awareness and training sessions before being granted access to the network. However, for the eleven participants that do require mandatory awareness and training, over ninety percent of these mandatory methods are rated as either moderately or very effective.

Process This study measured several processes, including assessments and evaluations, patch management, use of standardized computers, and contingency planning and incident response. Participants in this study have conducted a variety of assessments over the past year; the most frequently conducted were vulnerability assessments and audits. They have also used a range of techniques to evaluate their information security over the past year; the most frequently used were network traffic flow reports, help desk calls, firewall logs, reports from staff, and incidents. Similarly, methods to justify information security expenditures were also broadly used: the two most frequently

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

cited methods were requirement of law or regulation and reaction to major incident. Patch management methods for computers varied in extent of usage and effectiveness. For example, while the two methods most frequently used for patch management of computers owned by the institutions were MS AutoUpdate and manual application of patches, manual application was rated by less than one-fourth of the institutions as very effective. The high effectiveness of standardized computer usage is notable; all three institutions (100%) that issue standardized computers on a mandatory basis rated this practice as "very effective". Contingency planning and incident response are areas for improvement; overall, participants tended not to have documented contingency and incident response plans. Slightly over one third of participants have a documented IT disaster recovery in place. Further, less than a quarter have a documented cyberincident plan or plan for notifying individuals about private information access. Interestingly, however, over one-third of participants have an in-house forensic analysis capability.

Technology. Overall, participants have implemented a broad range of technologies (i.e., network monitoring, identity management, peer-to-peer networking, identity management, filtering, wireless, encryption, instant messaging). The three technologies most frequently implemented were anti-virus software, spam filtering, and perimeter firewalls. The top ten technologies that participants rated as "in progress or piloting" were single sign on, monitor for rogue devices, and encrypt data on network or computers. The ten technologies that participants most frequently rated as "considering in the next twelve months" included intrusion prevention systems, single sign on, and digital signatures.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Outcomes. Over three-fourths of participants consider their organization "somewhat prepared" or "well prepared" to defend against a major information security incident – that is, an incident that would compromise the confidentiality, integrity, or availability of their institution's information or systems. Over three-fourths of participants also indicated that their institution is "more prepared than two years ago" to defend against a major information security incident. While this progress is heartening, a source of concern is the disparity between participants' other responses and their perception of little likelihood their institution may compromise other entities. Specifically, over half of the participants rated the likelihood that their institution may compromise individuals, other organizations, or critical infrastructure as "low". Almost half of them rated the likelihood as "moderate", and just one-twentieth of the participants rated the likelihood that their institution may compromise individuals, other organizations, and critical infrastructure as 'high". Interestingly, almost five percent of participants rated the likelihood as "none".

Network Analysis. Outcomes as assessed using the Higher Education Network Analysis (HENA) tool, developed in this research study, are consistent with the survey and interview data. First, the number of inbound attacks is quite high; the two participants experienced almost two million attempted attacks violating their firewall or intrusion detection/intrusion prevention rule sets in just four months. The vast majority of attacks (N = 1,752,367; 96%) were inbound; less than one-hundred thousand (N = 75,114; 4%) attacks were outbound. A variety of attack types were employed for both inbound and outbound attacks. The types of <u>inbound</u> attacks reflect attempted database attacks, reconnaissance efforts, and Internet vandalism; attacks against database services represented over one-third of the inbound attacks. The <u>outbound</u> attack types were related to denial of service attempts, reconnaissance efforts, and a Sober virus outbreak.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Despite participants' perception that the likelihood of compromising other entities is low, network analysis results indicate high levels of international interactions (see Exhibit 1 below). Specifically, one hundred seventy three (173) countries were involved in inbound attacks on the participating institutions. The three countries most frequently associated with attacks on the two participating institutions were the United States, Republic of Korea, and China. Eighty-seven (87) different countries were involved in outbound attacks from the participating institutions. The three countries associated with the most frequent targets of the participants were the United States, Denmark, and Malaysia.

Exhibit 1. "Top 10" Countries Associated with Attacks

Inbound Attacks

Country	# Attacks
United States	647,770
Republic of Korea	288,307
China	216,738
Netherlands	137,254
Canada	76,043
Taiwan	53,376
United Kingdom	42,737
Germany	33,461
Japan	25,497
Sweden	24,809

Outbound Attacks

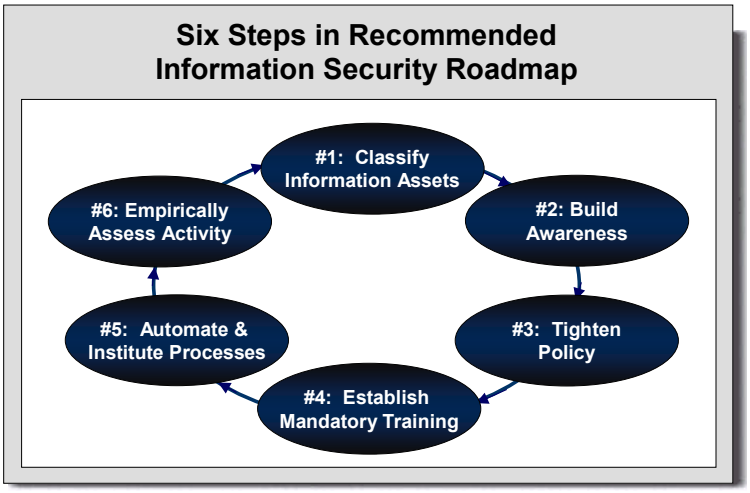
Country	# Attacks
United States	40,019
Denmark	6,441
Malaysia	4,152
Germany	3,098
Switzerland	1,317
Unknown	1,287
China	1,261
United Kingdom	581
Republic of Korea	424
France	414

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Discussion

Based on this study's results and other relevant research, a data-based roadmap of practical recommendations for policy and practice was developed. This "information security roadmap" focuses on challenges that are high-impact and under the control of information security professionals. To maximize both resource allocation and protection of information assets and systems, the roadmap is based on a risk management approach. Six inter-related steps (see Exhibit 2 below) are recommended for participants in achieving a baseline level of information security: 1) locate and classify information assets; 2) build awareness; 3) tighten security policy; 4) establish mandatory training; 5) automate and institute processes; and 6) empirically assess activity.

Exhibit 2. Information Security Roadmap



This study contributes to policy, practice and theory at the national, state, local, and individual institutional levels in four ways. First, this study represents the initial attempt to assess the link between information security incidents, approaches, policy, and practice in academic institutions and as they relate to the broader picture. Using this information, participants are able to develop data-based, focused remediation approaches for improving information security. Additionally, other researchers

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

may use this study's sanitized, anonymized databases as a baseline for their research. Second, this study furthers the definition of illicit Internet activity metrics. The "hard metrics" obtained through the HENA tool include frequency, protocol, and type of attack, as well as country affiliation and detailed information regarding the top ten attackers and targets. In conjunction with traditional metrics obtained through survey and interview methods, these hard metrics offer direct insights into improving controls and processes. Third, this study supplies government and law enforcement agencies with an objective profile of issues and remediation approaches that are proactive, cost-effective, and facilitate information sharing. Law enforcement agencies that are collaborating with academic institutions to address cyberintrusions may use these findings in conjunction with their efforts to promote proactive partnering between academic institutions and law enforcement agencies. Fourth, this study raises several interesting policy-related opportunities at the federal, state, and local levels. For example, an approach that bridges the gap between several federal mandates (e.g., President's National Strategy to Secure Cyberspace, DHS's National Infrastructure Protection Plan, NIST's FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems) and academia involves establishing a minimum baseline of information security for academic institutions. This baseline could serve as an incentive for obtaining research funding, in a model similar to the NSA NIETP/NSF relationship, or as a requirement for accreditation and operational funding, in a manner similar to the Department of Education's Title IV status. At the state policy level, the assessment techniques developed in this study could be used in shaping state-level legislation based on empirical data or in evaluating the current state of information security of institutions in specific jurisdictions to solicit appropriate resources. At the local level, a proactive campaign by local law enforcement on "hot topics" would be beneficial.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

This exploratory study indicates that information security in academic institutions is an area that needs additional empirically-based research. Future research studies should focus on: a) quantifying the threat that academic institutions pose to public safety and security; b) assessing the types and volume of illicit and transnational criminal activity occurring in academic institutions; and c) empirically determining the impact of information security policies and practices on academic institutions' information security posture. Additionally, a very promising area of future research involves empirically assessing the actual network activity of academic institutions to understand impacts on critical infrastructure and linkages to transnational crime.

In conclusion, as illicit activity via the Internet burgeons and perpetrators move from better-protected private and government entities to softer targets, academic institutions may represent a disproportionate threat to public safety. This concern is compounded by the increasing inter-connectedness between academic, government, military, private sector, and critical infrastructure entities. All of our systems are connected and problems in one sector directly affect others. Unless we diagnose the unique vulnerabilities that exist in higher education and realign how those networks interoperate and share information securely, our systems will remain insecure and public safety and homeland security will suffer as a result.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

TABLE OF CONTENTS

INTRODUCTION 1

Background 1

Purpose, Goals, and Objectives 5

Research Question and Hypotheses 6

METHOD 10

Study Design 10

Component #1: Quantitative Field Survey 10

Component #2: Qualitative One-on-One Interviews 26

Component #3: Empirical Analysis of Network Activity 31

RESULTS 40

Evaluation Criteria for Project Objectives 40

Overview of Findings 42

Detailed Findings 48

Environment 48

Attacks and Results of Incidents 48

Impact of Laws and Regulations 50

Strategy 51

Strategic Objectives 51

Challenges 52

Stakeholders' Priorities 54

Responsibility and Staffing 55

Budget 56

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Policy 58
Formality and Sponsorship 58
End Users and the Policy 59
Consequences and Enforcement 61
Information 62
Sharing Sensitive Information 62
Methods for Protection 63
Vetting Procedures for Staff 64
People 65
Methods for Raising Awareness 65
Mandatory Awareness and Training 66
Certifications 67
Practices 68
Assessments and Evaluations 68
Patch Management 70
Standardized Computers 72
Contingency Planning and Incident Response 73
Technology 77
Technologies Implemented 77
Technologies in Progress or Being Piloted 83
Technologies Being Considered 84
Technologies Not Being Considered 85

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Outcomes 86

Likelihood Institution May Compromise Others 86

Preparation for a Major Incident 87

Empirical Analysis of Network Activity 89

Number of Attacks 89

Types of Attacks 89

Protocol of Attacks 92

Countries Associated with Attacks 94

Top 10 Individual Attackers 97

Top 10 Individual Targets 98

Linking Network Analysis Results to Actions 99

DISCUSSION 104

Roadmap for Improving Information Security in Academic Institutions 104

Tailoring the Roadmap for Each Institution's Needs 124

Contributions of the Study 125

Future Research 128

END NOTES 133

APPENDIX A 136

APPENDIX B 141

APPENDIX C 195

APPENDIX D 219

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

INTRODUCTION

Background

America's colleges and universities face a barrage of information security incidents such as data theft, malicious software infections, hacks into their computer networks and infiltration of other entities via their networks. Academic institutions are vulnerable to exploitation due to a combination of several factors, including: (a) abundant private and research data; (b) relatively open networks with significant bandwidth, high end-user turnover, at-risk activities, and a decentralized structure; and (c) extensive cyberlinks with the government, military, private sector, and other academic institutions. Adverse impacts of information security incidents include compromised private data and intellectual property, substantial financial losses, and potential threats to critical infrastructure, public safety and national security. Despite these issues, little research has been conducted at the policy, practice, or theoretical levels, and few policies and cost-effective controls have been developed.

The Internet's Changing Environment

Information security incidents are burgeoning due to a combination of technological, socioeconomic, cultural, political, and legal forces. In an increasingly connected and complex global computing environment, the safety buffer between systems – particularly those related to national security and critical infrastructure – is dramatically reduced. Illicit internet activity has evolved from a game for "script kiddies" into a robust black market for individual actors, criminal networks and terrorists (McAfee, July 2005). Emerging issues that exacerbate the situation include botnets (networks of "zombie" computers), spyware, phishing, and carding sites that sell stolen identities and credit card numbers (Time Magazine, August 2005; IEEE, December 2005).

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

As targets in the private sector and government are better protected, perpetrators are shifting to softer targets such as academia, home users, and the mobile workforce. Academic institutions are particularly attractive targets due to their unique characteristics (e.g., open culture, sensitive information, diverse users and access methods, and high-risk activities), as described below.

Tension between culture and security. Inherent tension exists between the academic culture and security requirements. The culture of academia is built on openness, free speech, learning, information sharing and experimentation. Attempts to limit this culture may be met with a backlash from students, faculty, staff, and the institutions' senior administration.

Sensitive information. Academic institutions house private information about faculty, staff, students, alumni, and research subjects (e.g., social security number, date of birth, driver's license number, financial and medical information, grades). In addition, academic institutions have been at the forefront of research and development efforts for all technology innovations in the country. In some cases, this private data and intellectual property are strictly governed by security policies; nonetheless, huge gaps endanger the security of personal and intellectual information.

Diverse users and access methods. Academic networks are routinely used by diverse users with different responsibilities and access methods. Users - including students, faculty, staff, contractors, and guests - access institutions' systems via on-campus and remote logins from a variety of locations (e.g., residence halls, classrooms, computer centers, other campuses and, increasingly, wireless networks). System administrators face an extraordinarily un-standardized network environment and an average turnover rate of first- and second- year students of 50% (Washington Post.com, Sept 4, 2003).

High-risk activities on academia's networks. A critical attribute of academic institutions is the high-risk activities on their networks, including peer-to-peer (P2P) networking, instant messaging and e-learning. Innovations in sharing information have created some of the most severe security and privacy vulnerabilities, and academic institutions are particularly at risk due to their open culture.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security Threats Faced by Academic Institutions

Information security threats that may originate from the "inside" (e.g., students, staff, faculty) or the "outside" (e.g., hackers, terrorists, organized criminals) have created serious concerns for academia's networks. Those with malicious intent can exploit academic institutions' vulnerabilities with little risk of detection, as described in the following paragraphs.

Stealth attacks. Academic institutions provide excellent targets and may also serve as a gateway to sensitive targets with which they share information. The recent Stakkato Incident, in which several research institutions, military entities and NASA were breached by a Swedish teenager (CNN.com, May 10, 2005) demonstrates the vulnerabilities of academic institutions and critical infrastructure. Terrorist, organized criminal, and espionage groups can exploit these weaknesses and cause harm with attacks ranging from distributed-denial-of-service attacks to viruses with damaging payloads.

Botnet Threats. Because of their open nature, academic networks may be disproportionately vulnerable to bot infections. In "Botnets: What You Need to Know" (Nov 2004), the Multi-State Information Sharing Analysis Center (MS-ISAC) provided three examples of botnet infections, all of which were traced back to academic institutions. In one case, an infected computer had 7,200 connections to other compromised computers worldwide. The student who owned the infected machine, which was acting as a zombie botnet controller, had no idea the computer was infected.

The attacks that go unnoticed. Incidents that are identified may not be as dangerous as those not detected. For example, the only symptom of a bot infection may be slow computer response times; academia's network administrators may have difficulty managing a network of 100,000 computers and noticing traffic patterns of zombies. Frequently, breaches - particularly stealth probes and attacks - are only identified by coincidence.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Impact on Public Safety, Policy and Practice

In an increasingly complex and interconnected computing environment, the impact of security breaches extend beyond academic institutions. Compromised private data, financial losses, and potential attacks on critical infrastructure affect individuals, other entities, and public safety and security.

Compromised private data. Incidents involving the theft of data belonging to students, applicants, faculty, and staff are increasing at an alarming rate, as are the access points for system breaches. For example, personal data of 178,000 current and former students, applicants and employees was compromised when the Financial Aid Office's server at San Diego State University was hacked (San Francisco Chronicle, April 2004). An attack on two servers at the University of Colorado's health center resulted in the compromise of 43,000 Social Security Numbers (SSNs), names, dates of birth, and addresses (CNET, July 2005). Records with SSNs and birthdates for 197,000 people, from students to corporate recruiters, were illegally accessed from the University of Texas (Statesman.com, April 2006).

Financial losses. A gradual, but certainly crippling effect on public safety and security arises from financial losses incurred by institutions, since if losses continue at this rate the government may have to intervene. An informal survey of nineteen research universities (The Chronicle of Higher Education, March 19, 2004) shows that each spent an average of $299,579 during a five-week period undo the havoc wrought by the Blaster worm. Of the universities surveyed, Stanford University spent the most: $806,000 to repair 6,000 computers and 18,420 hours to rebuild machines.

Attack on the U.S. critical infrastructure. Perhaps the most frightening incident in which academic institutions' vulnerabilities can be exploited is a distributed-denial-of-service-attack (DDOS) on the U.S. critical infrastructure, in which university computers unwittingly serve as zombies. Elements of this type of attack have already occurred. The DDOS attack on Microsoft (February 2004) demonstrates speed and effectiveness of this method. The compromise of 911 systems (November 2003) demonstrates the catastrophic effect on public safety.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

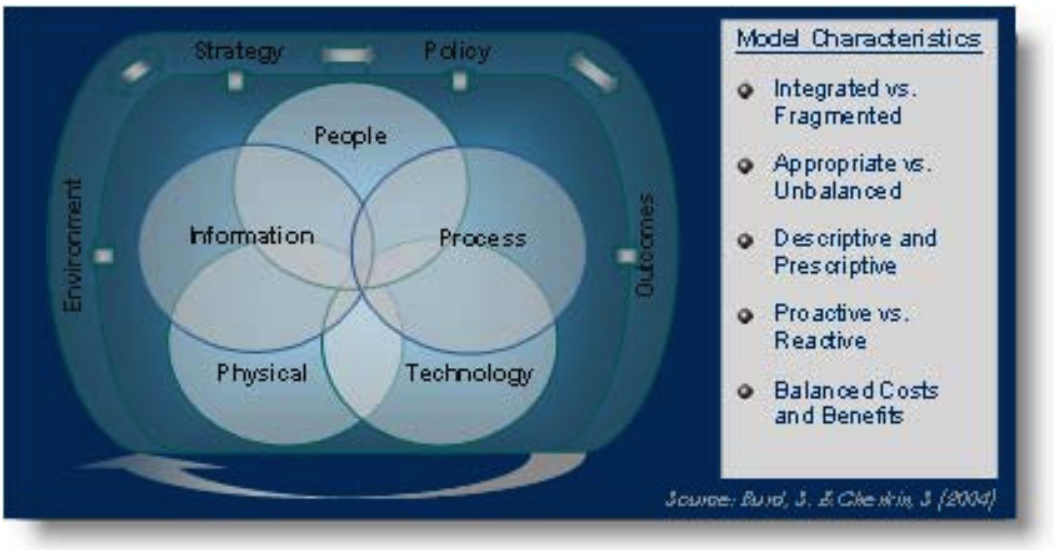
Purpose, Goals, and Objectives

Despite the critical information security issues faced by academic institutions, little research has been conducted at the policy, practice or theoretical levels to address these issues, and few policies and cost-effective controls have been developed.

The purpose of this research study was to address this dearth of research in two ways: first, to create an empirically based profile of information security issues in academic institutions; and second, to develop a practical roadmap for policy and practice at the federal, state, and local levels.

The goals of this project were three-fold. The first goal was to create an empirically-based profile of the information security issues and approaches of academic institutions. The basis of the information security profile was the Information Security Model (see Exhibit 1 below), which addresses information security in the context of the institution's environment, strategy, policy, information, people, processes, technology, physical environment, and outcomes. This model was also used to integrate the study's quantitative survey and network analysis data with qualitative interview data to develop a holistic, balanced, and proactively-oriented profile of information security in academic institutions.

Exhibit1. Information Security in Academic Institutions (ISAI) Model



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The second goal was to develop a practical roadmap for policy and practice at local, state, and national levels to enhance information security in academic institutions. The practical roadmap for policy and practice highlights critical issues, prioritizes improvement opportunities, lists effective and ineffective approaches academic institutions are implementing, and provides a means to evaluate and balance the costs of security with the value of assets protected.

The third goal of this study was to advance the knowledge, policy-making and practices of organizations and individuals that impact information security in academic institutions. Targets for project findings included academia, law enforcement, researchers, government, public/private partnerships, and the public as appropriate. Relevant information was communicated via written, presentation, and media channels.

Research Question and Hypotheses

To address the purpose, goals and objectives of this study, one research question and eight areas of inquiry were tested. Several sub-areas of interest are associated with each area of inquiry; in this study, they are labeled as "hypotheses". Note, however that since this is an exploratory study, these hypotheses are quite general and should be refined and tested in future studies.

The overall research question was:

"What is the impact of information security in academic institutions on public safety and security?"

The areas of inquiry were based upon the project's literature review, the Information Security in Academic Institutions (ISAI) model, and interviews with information security professionals in the academic, public, and private sectors.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The eight general areas of inquiry and their associated hypotheses are listed below.

Environment

- The number of attacks on academic institutions has increased this year as compared to last year.
- Information security incidents in academic institutions involve a wide range of results, particularly unauthorized access to personally identifiable information.
- Laws and regulations have had little impact on improving information security in academic institutions over the past year.

Strategy

- Key infosecurity objectives are to fulfill senior administration directives and to avoid negative publicity.
- Faculty and students have the lowest priority ratings for information security; IT staff and senior administration have the highest priority ratings for information security.
- Infosecurity policies are typically sponsored by the IT Department rather than senior administration.
- Less than half the institutions employ an Information Security Officer or person with a similar role.
- Over half of the institutions have conducted zero or one information security assessments within the past twelve months.
- The budget for information security is less than 5% of the central IT budget for over three-fourths of institutions.

Policy

- Most institutions rely on a combination of informal and formal information security policies.
- Most of the institutions' end users are provided with the information security policy and are required to officially agree an electronic or written version of this policy.
- Consequences for violating the information security policy are inconsistently enforced.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information

- Over three-fourths of institutions share sensitive information with a variety of government agencies.
- Methods to secure sensitive information are consistently used by less than half of the participants.
- Less than half the academic institutions use criminal background checks or reference checks on a regular basis.
- Less than half the institutions have conducted an information asset classification in the past 12 months.

People

- Academic institutions use a range of awareness and training methods; however, few of these methods are considered very effective.
- Less than one-fourth of institutions have mandatory awareness and training methods; however, most of these methods are considered very effective.
- Over half the institutions seek information security certifications when hiring or promoting staff.

Process

- Automatic patch management is the most effective, but not most frequently used, method for patching computers owned and not owned by academic institutions.
- Less than one-quarter of institutions issue standardized computers; those that do so rate this practice as very effective.
- Over three-fourths of institutions have a documented IT disaster recovery plan in place.
- Almost half the institutions have documented plans for cyberincident response and for notifying individuals that their private data has been compromised.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Technology

- Over three-fourths of institutions have implemented network monitoring techniques such as anti-virus software and firewalls.
- More than half the institutions have implemented peer-to-peer techniques such as shaping bandwidth.
- More than half the institutions have implemented encryption technologies for data in transit, on the networks, and backup locations.
- Over three-fourths of institutions are not considering filtering technologies such as web, instant messaging or wireless content filtering.

Outcomes

- Over half the institutions consider the likelihood of compromising individuals, other entities or critical infrastructure as moderate or high.
- Over half the institutions consider themselves as somewhat prepared for a major information security incident.
- Over three-fourths of institutions consider themselves more prepared now than two years ago for a major information security incident.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

METHOD

Study Design

Study design incorporated three research methods: a quantitative field survey, qualitative one-on-one interviews, and an empirical assessment of institutions' network activity. This combination of methods provided a robust data set from which insights for the current study and directions for future research could be obtained. The unit of analysis for all three design components was the academic institution. The subjects, materials and procedures for the three components of this research study are presented in the following pages.

Component #1: Quantitative Field Survey

Subjects

Information security professionals (e.g., Information Security Officers, IT Directors, CIOs) of seventy-two (72) academic institutions across the U.S. participated in the quantitative survey component of this research study. Basis for participation in the survey was voluntary. Criteria for inclusion in the sample frame included characteristics of both institutions and individuals. Inclusion criteria for *institutions* were: 1) Title IV status, as designated by the Department of Education; 2) jurisdiction within the U.S.; 3) degree-granting status; and 4) non-administrative office status. The criterion for inclusion of *individuals* within the institutions was role (e.g., information security professional, IT Director, CIO, or other professional responsible for information security within the academic institution). Criteria for exclusion of *institutions* from the sample frame, which paralleled criteria for inclusion, were: 1) non-Title IV status; 2) jurisdiction outside the U.S.; 3) non-degree-granting status; and 4) administrative office status. The criterion for exclusion of *individuals* within the institutions was role (e.g., non-security or non-IT role). Please refer to Appendix B for more details about the inclusion and exclusion criteria.

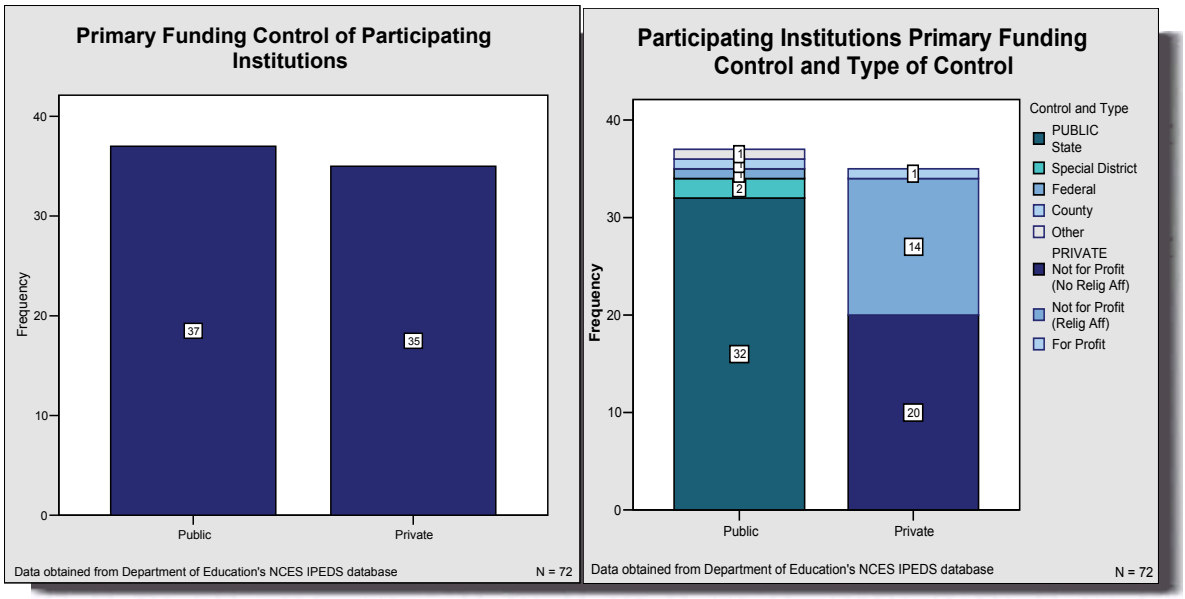
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Characteristics of Subjects

Characteristics of subjects that participated in the survey component of this study are described in the following pages. Specifically, characteristics of the seventy-two (72) *institutions* participating in the survey include: funding control; highest degree offered; Carnegie classification; total student enrollment; region; degree of urbanization; membership, accreditation and special groups served. The characteristics of *individual* respondents within the institutions include title and level.

Funding Control. Institutions participating in the study are relatively evenly split between public (N = 37; 51%) and private (N = 35; 49%) funding control. Within the institutions that are publicly funded, control is primarily at the state level (N = 32; 86%); the remainder of the institutions are controlled at the special district level (N = 2; 5%), federal level (N = 1; 3%) and county level (N = 1; 3%). Within the institutions that are privately funded, slightly over one half are not-for-profit institutions with no religious affiliation (N = 20; 57%). The remaining privately funded institutions are not-for-profit institutions with religious affiliation (N = 14; 4%) or for-profit institutions (N = 1; 3%). Please see Exhibit 2 below for a graphical presentation of participants' funding control.

Exhibit 2. Primary Funding Control of Participating Academic Institutions

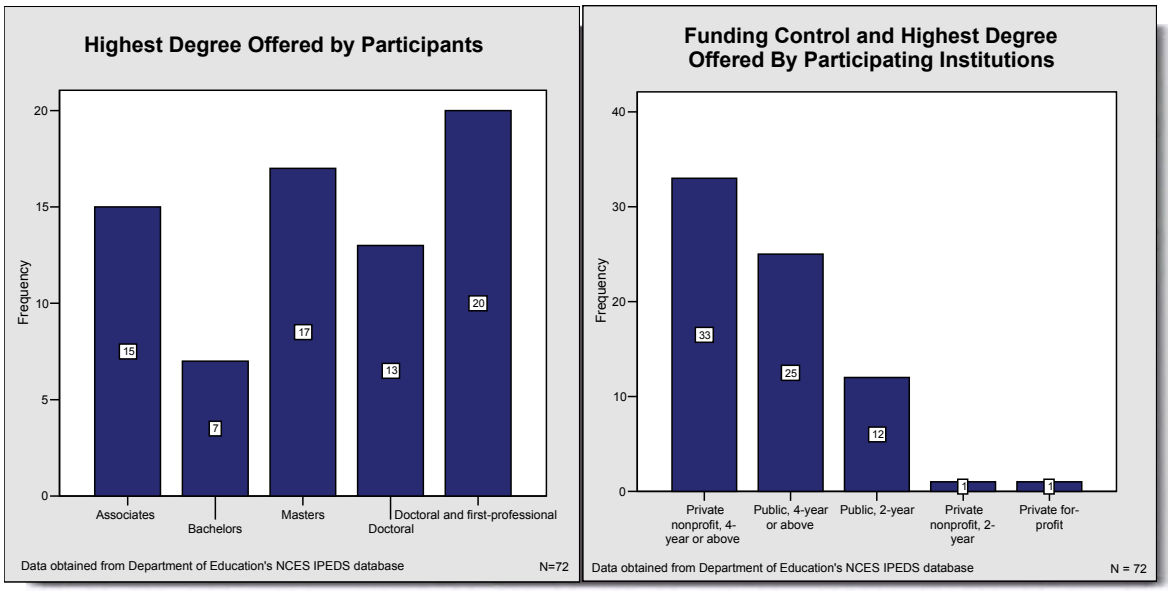


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Highest Degree Offered and Highest Degree by Funding Control. The survey sample is comprised of a range of highest degrees offered. Specifically, the highest degrees offered by institutions in the sample include associates (N = 15, 21%), bachelors (N = 7; 10%), masters (N = 17; 24%), doctoral (N = 13; 18%) and doctoral and first professional (N = 20; 28%) degrees.

Participating institutions can also be considered in terms of their highest degree offered and funding control. Most participants in the survey are public 4-year or above (N = 25; 35%) and private not-for-profit 4-year or above (N = 33; 46%) institutions. Less than one-quarter of participants are public 2-year institutions (N = 12; 17%) or private not-for-profit 2-year institutions (N = 1; 1%). One institution is private for-profit (1%). Exhibit 3 presents information for both highest degree offered and highest degree by funding control.

Exhibit 3. Highest Degree Offered by Participants and Highest Degree by Funding Control

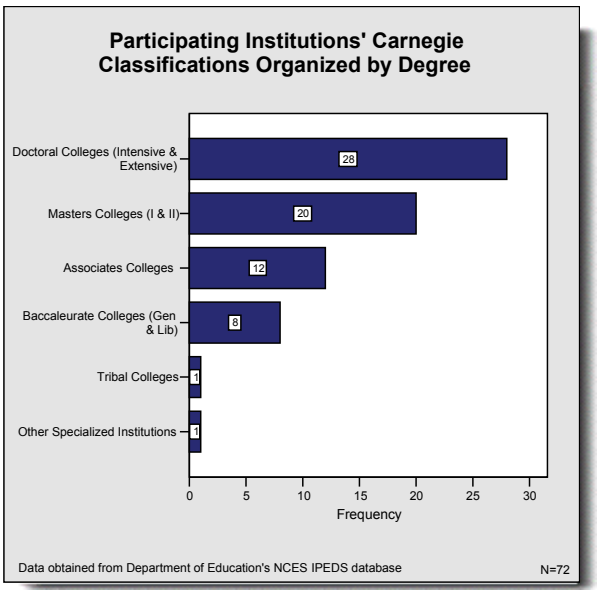


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Carnegie Class. Carnegie Class data was collected to ensure comparability of results in this survey with those of other relevant surveys (e.g., EDUCAUSE, other higher education studies). *Doctoral/ research institutions* typically offer a wide range of baccalaureate programs and graduate education through the doctoral level. *Masters colleges and universities* generally offer a wide variety of baccalaureate programs and graduate education through the master's level. *Baccalaureate institutions* are primarily undergraduate institutions with a major emphasis on baccalaureate programs. *Associates institutions* offer associate-level degrees and certificate programs but, with very few exceptions, do not award baccalaureate degrees. *Specialized institutions* offer degrees ranging from bachelor- to doctoral-level in a single field.

As illustrated in Exhibit 4 below, almost three-fourths of the sample consists of institutions offering a bachelors degree or above, including doctoral institutions (N = 28; 40%), masters institutions (N = 20; 29%), and baccalaureate institutions (N = 8; 11%). Almost one-fourth of the sample is comprised of associates institutions (N = 12; 17%), one institution (1%) is a Tribal college and one institution (1%) is categorized as "Other Specialized Institution".

Exhibit 4. Carnegie Class of Participating Institutions

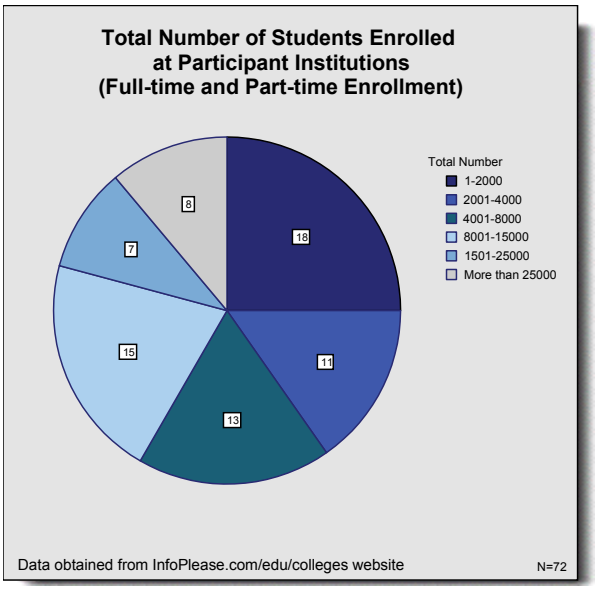


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Total Student Enrollment. The total number of students enrolled on a full-time or part-time basis at participating institutions ranges from 678 to 50,995 students. Full-time and part-time enrollment was selected to reflect the total number of students routinely accessing the institutions' networks. The categories for number of students enrolled (e.g., 1 – 2,000, 2,001 – 4,000) were based on survey research questions by EDUCAUSE to ensure comparability of results across studies.

The sample is relatively distributed across total number of students enrolled on a full-time and part-time basis. Approximately one-fourth of the participants have a total enrollment of 1 – 2,000 students (N = 18; 25%), and slightly less than one-fourth of participants have a total enrollment between 2,001 – 4,000 students (N = 11; 15%), 4,001 – 8,000 students (N = 13, 18%), or 8,001 – 15,000 students (N = 15; 21%). Approximately one-eighth of the participating institutions have a total enrollment of 15,001 – 25,000 students (N = 7; 10%) and more than 25,000 students (N = 8; 11%).

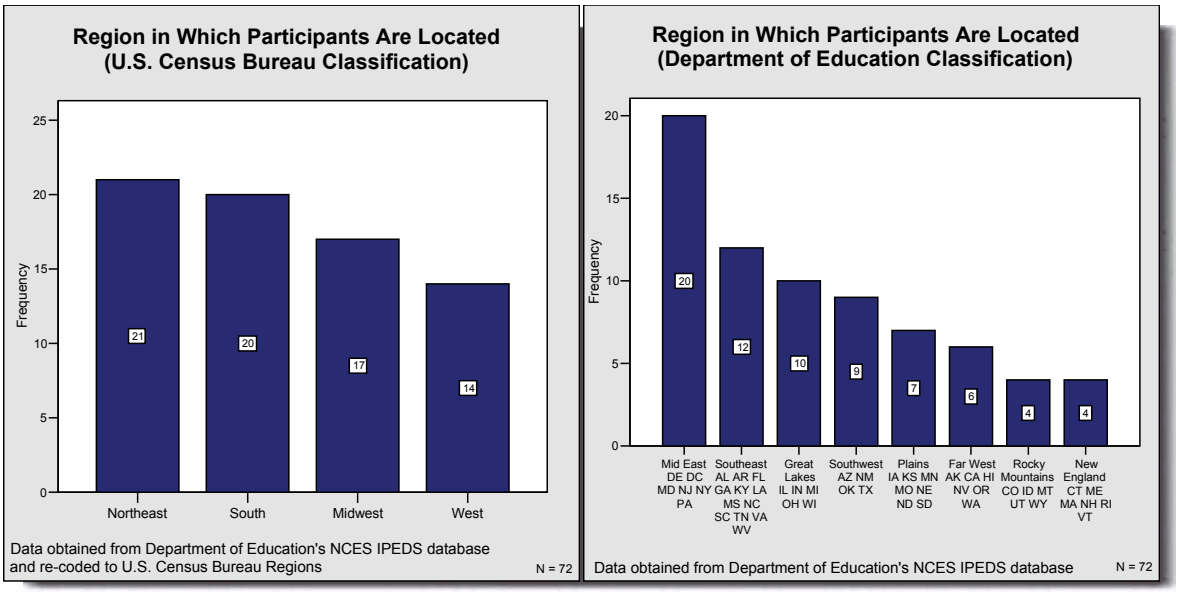
Exhibit 5. Total Student Enrollment for Participating Institutions



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Region. Participating institutions are roughly evenly distributed across the four U.S. Census regions. Specifically, twenty-one institutions (29%) are located in the Northeast, twenty (28%) are in the South, seventeen institutions (24%) are in the Midwest, and fourteen (19%) are located in the West. The Department of Education's region classification provides a slightly different perspective and further granularity. Slightly over one half of the participating institutions are from the East Coast of the U.S. Specifically, twenty institutions (28%) are located in the Mideast (i.e., DE, DC, MD, NJ, NY, PA), twelve institutions (17%) are located in the Southeast (i.e., AL, AK, FL, GA, KY, LA, MS, NC, SC, TN, VA, WV), and four institutions (6%) are located in New England (i.e., CT, ME, MA, NH, RI, VT). Slightly less than one quarter of participating institutions are located in the Midwest: ten institutions (14%) are located in the Great Lakes (i.e., IL, IA, MI, OH, WI) and seven (10%) are in the Plains (i.e., IA, KS, MN, MO, NE, ND, SD). Just over a quarter of participants are located the West Coast: nine institutions (12%) are located in the Southwest (i.e., AZ, NM, OK, TX), six (8%) are located in the Far West (i.e., AK CA, HI, NV, OR, WA), and four institutions (6%) are in the Rocky Mountains (i.e., CO, ID, MT, UT, WY).

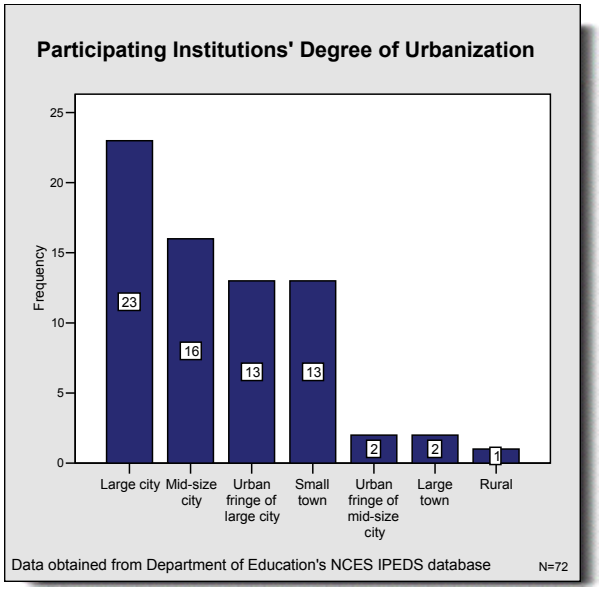
Exhibit 6. Regions in Which Participating Institutions are Located



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Degree of Urbanization. Participating institutions tend to be located in urban areas. Specifically, almost three-fourths of the participants are located either in a large city (N = 23; 32%), urban fringe of a large city (N = 13; 18%), or a mid-size city (N = 16; 22%). The remainder are located in small towns (N = 14; 18%), large towns (N = 3; 3%), the urban fringe of a mid-size city (N = 2; 3%), or in a rural location (N = 1; 1%).

Exhibit 7. Participating Institutions' Degree of Urbanization

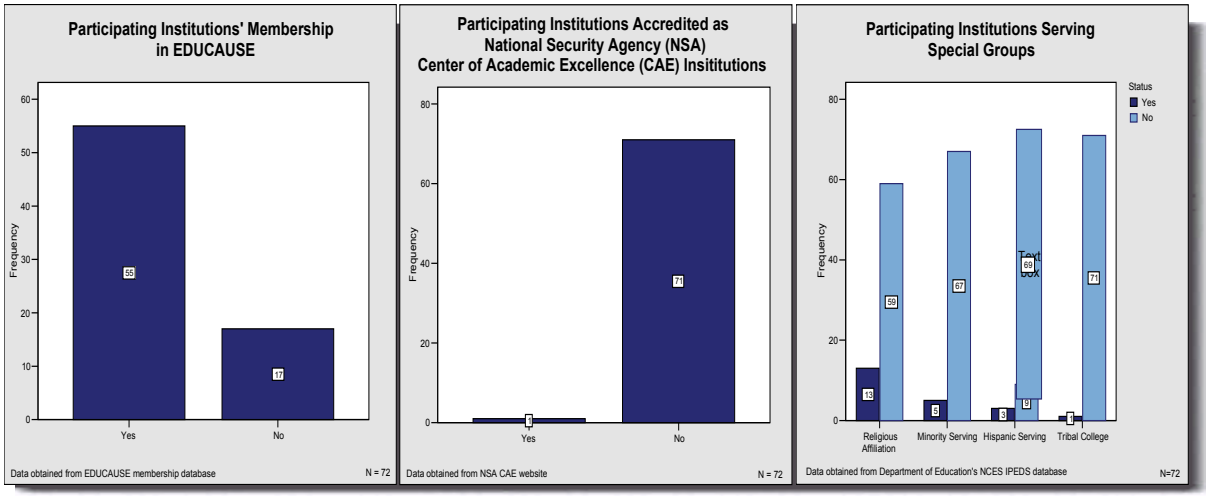


Membership, Accreditation, and Special Groups Served. Over three-fourths of participants (N = 56; 78%) are members of EDUCAUSE, a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. One participant (1%) is a designated National Center of Academic Excellence in Information Assurance Education; this means its information assurance teaching curriculum has passed a rigorous review to be eligible for the program, which is jointly sponsored by the National Security Agency and Department of Homeland Security. Both of these distributions are roughly representative of the larger academic institution population.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Most of the participants are not classified by the Department of Education as serving special interest groups. Specifically, thirteen institutions (18%) have a religious affiliation; five 7%) are minority serving; three (4%) are Hispanic serving; and one (1%) is a Tribal college. Exhibit 8 below provides a graphical representation of participants' membership, accreditation, and special groups served.

Exhibit 8. Participating Institutions' Membership, Accreditation, and Special Groups Served

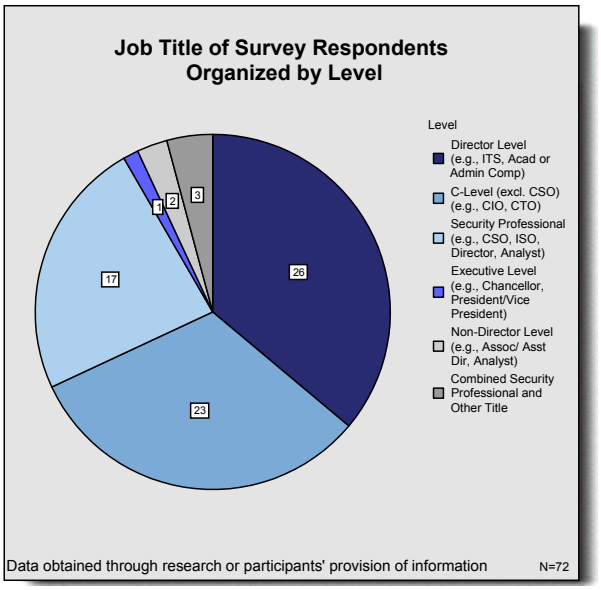


Individual Respondents' Characteristics. Individual professionals responsible for information security at their institutions that completed the survey tended to be Directors, C-Level executives, or Information Security professionals. Specifically, twenty-six professionals (36%) hold positions such as Director of Information Technology Services, Academic Computing, or Administrative Computing. Twenty-three professionals (32%) are C-Level executives such as Chief Information Officer or Chief Technology Officer (note that Chief Security Officer/Chief Information Security Officer is considered as an Information Security professional for this study). Twenty professionals (28%) are Information Security professionals such as Chief Security Officer/Chief Information Security Officer, Director of Information Security, Information Security Analyst, or combined role specializing in Information Security and another position. One professional (1%) is at the Executive level (e.g., Chancellor, President/Vice

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

President) and two professionals (3%) are at the non-Director level (e.g., Associate or Assistant Director, Analyst).

Exhibit 9. Individual Participants' Title and Level



Sampling Procedures

The Department of Education's National Center for Education Statistics (NCES) Integrated Postsecondary Education Data System (IPEDS) database was the source of data for the survey's sample frame. This database was selected because the Department of Education is the federal agency responsible for: (a) collecting data on America's schools and disseminating research; (b) focusing national attention on key educational issues; (c) establishing policies on federal financial aid for education, and distributing as well as monitoring those funds; and (d) prohibiting discrimination and ensuring equal access to education. The National Center for Education Statistics (NCES) annually collects comprehensive data about Title IV institutions, and the IPEDS database contains all variables needed to identify and characterize institutions selected for the sample frame.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The survey sample frame was obtained through two rounds of simple random probability sampling from the Department of Education's NCES IPEDS database to create a sample frame representative of the general population of Title IV, degree-granting academic institutions across the U.S. The first sample frame size was three hundred (300) academic institutions, based on a targeted sample size of one hundred (100) institutions and a predicted response rate of 30%. This targeted sample size (100 institutions) was deemed adequate for accomplishing the data analyses planned to assess patterns and trends in the institutions' objectives, issues and approaches.

The first sample frame was obtained by selecting one out of every 14 institutions from the NCES IPEDS database of 4,184 institutions. This sampling rate was obtained by dividing the desired sample frame size of 300 institutions by the 4,814 institutions in the database, which produced a fraction of approximately 1/14. A randomized starting point was selected to ensure that there was a chance selection process; the random number function in Microsoft Excel (using the formula =RAND()*14) yielded a randomized starting point of 12. Since the IPEDS list was ordered alphabetically according to state and institution name, the database was examined to ensure that the sample frame resulting from one random start would not have a recurring pattern that might be systematically different from sample frames resulting from other starts. No reordering of the database or adjustment of selection intervals was required. Thus, starting on the 12th entry of the IPEDS database, every 14th institution thereafter was included in the sample frame.

A second simple random sample frame from the Department of Education's NCES IPEDS database was obtained three months later due to a response rate lower than the predicted 30% response rate. The expected response rate was adjusted from 30% to 15%, so an additional 300 academic institutions were required for the sample frame to achieve the targeted 100 participating institutions. A simple

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

random sample of the IPEDS NCES database was conducted a second time. Again, a randomized starting point was selected to ensure that there was a chance selection process; the random number function in Microsoft Excel (using the formula =RAND()*14) yielded a randomized starting point of 8. Thus, starting on the 8th entry of the IPEDS database, every 14th institution thereafter was included in the sample frame. When institutions randomly selected matched the first randomly selected institution, that institution was skipped and the next institution was selected.

Examination of institutional characteristics (e.g., funding, region, total enrollment) yielded no significant differences; thus, the two sample frames were used to obtain participants for the survey component of this study. Recruitment procedures involving email, telephone, and email invitations were used with all 600 academic institutions in the sample frame. The final sample size for the survey component of this research study was 72 institutions, representing a 12% response rate.

Materials

The Information Security in Academic Institutions Survey (Burd, S. & Cherkin, S., 2004) is comprised of fifty-five (55) items organized in five sections: Environment, Policy, Controls, Challenges, and Resources. Fifty-three of these items are closed-response format: twenty-eight items are interval or scale items; twenty-six items are ordinal or scale items. Two items are open-response format. The survey is best administered on the web (e.g., via Zoomerang on-line survey program) to accommodate the five skip-jump series of questions. The survey requires between 15 and 25 minutes to complete.

Explanatory notes, presented at the beginning of the survey, described the purpose of the survey and addressed respondent-related issues such as selection, voluntary participation, and anonymity of results. It also outlined the survey's timing and contents, provided a thank you and date to expect results, and defined key terms used throughout the survey.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The first section of the survey, *Environment*, contained four items addressing the environment in which academic institutions operate. Items included number of attacks experienced over the past 12 months, results of incidents over the past 12 months, the impact of laws and regulations on improving information security, and an estimate of the likelihood the institution may compromise other entities.

The second section, *Policy*, contained six items related to the institution's information security policy – that is, the aggregate of directives, regulations, rules and practices that prescribe how each institution manages, protects, and distributes its information. Items addressed the existence of an Information Security Officer role, responsibility for information security, the formality of the institution's information security policy, consequences for violating the policy, and enforcement of consequences.

The third section, *Information Security Controls*, was the longest portion of the survey with 17 items. The first sub-section, *Operational Practices*, addressed assessments completed over past 12 months, patch management techniques, use of standardized computers, handling of private or sensitive information, and approaches used to evaluate information security effectiveness at the institution. The second sub-section, *Incidents and Disaster Management*, included questions about whether the institution has documented plans for IT disaster recovery, cyber incident response, and notifying individuals of private information exposure. Other topics, such as collaboration with law enforcement and groups to whom the institution has reported incidents in the past 12 months were addressed. The third sub-section, *Awareness and Training*, addressed methods to raise awareness, techniques for mandatory training and awareness, and effectiveness ratings for mandatory training and awareness techniques. The final sub-section, *Technology*, addressed the use of key technology-driven approaches such as network monitoring, instant messaging, wireless networking, and encryption.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The fourth section of the survey, *Challenges*, provided participants with the opportunity to rate the impact of different issues concerning the institution's culture, end user awareness and knowledge, technology issues, and structure and systems.

The fifth and final section, *Resources*, addressed strategic inputs to the institution's information security policy and practices. Its eight items addressed strategic objectives, priority of information security for stakeholders, and sponsorship of the institution's information security policy.

The last two questions in the survey asked participants to rate the institution's current level of preparedness to defend against a major incident and to describe this current level of preparation compared to two years ago. A section was also provided for additional comments or suggestions and provision of the title and contact details for participants who may have not been the original survey recipients. A thank-you and team members' contact details for questions were also included.

As this survey was rather lengthy, demographic information about the participating institutions was collected independently by the principal investigator and research team.

ISAI Survey Development. Development of the ISAI survey involved five steps. First, a focused literature review of information security- and academic institution- related surveys was conducted to identify key surveys (e.g., FBI/CSI, EDUCAUSE), relevant items, critical findings and subject matter experts with whom to liaise. Second, interviews with practitioners in information security (e.g., FBI, NSA, NIST, InfraGard, EDUCAUSE) and academic institutions were conducted. Third, results of the literature review and interviews were integrated with the ISAI model. Fourth, the survey was piloted with five information security professionals of academic institutions and six information security experts; revisions were made based on these pilots. Fifth, the survey was posted onto the web-based survey

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

administration program, Zoomerang, modified as necessary for on-line administration, tested with all project team members, and posted for administration.

Reliability and Validity

The reliability of the Information Security in Academic Institutions survey was assessed via internal consistency estimates. Cronbach's (1951) coefficient alpha was selected because it is a widely used measure of reliability and is appropriate for use with multi-point, continuous scale items. Other methods of assessing reliability (e.g., scoring reliability, inter-rater reliability, reliability over time, alternate form reliability) were not applicable because: (a) the measure was scored through computer tabulation of self-report data; (b) ratings were derived through self-administration of the measure on the Internet rather than direct observation of participants; (c) the measure was administered once because the study was a one-shot design; and (d) one version of the measure was administered to participants.

Eight scales were developed based on a combination of the study's underpinning model, hypotheses, and the survey's structure. These scales included: Environment, Strategy, Policy, Information, People, Process, Technology, and Outcomes. Overall, items in the scales were relatively highly inter-correlated, indicating homogeneity of items comprising the scales. Below is a brief description of the scales, their reliability, and relevant information.

The "Information" scale (alpha= .8779) was comprised of three items: agencies with which the institutions share sensitive information; methods to secure sensitive information on the network; and extent of usage of methods to secure sensitive information. "Process" was divided into three separate scales as the underpinning constructs these scales were measuring were conceptually distinct. The "Metrics" scale (alpha = .9194) was comprised of three items: assessments in 12 months; methods to evaluate information security; and methods to justify expenditures. "Patch Management and

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Standardized Computers" (alpha= .7158) items included: patch management – computers owned by institution; patch management – computers not owned by institution; and use of standardized computers. The "Disaster and Contingency Plans" scale (alpha= .9968) was comprised of nine items which addressed types of documented plans, when these plans were tested, and in-house forensics capability. The "Technology" scale (alpha= .9652) was comprised of six items, including network technologies, instant messaging technologies, wireless technologies, identity management technologies, filtering technologies, peer-to-peer technologies, and encryption technologies. The "Outcomes" scale (alpha= .6261) was comprised of three items: potential impact on other entities; prepared for an incident; prepared for an incident compared to two years ago.

Three of the hypothesized scales had very poor internal consistency reliability, indicating that the items comprising these scales did not tap the same construct. These scales included: "Environment" (alpha= -.0679), which was comprised of "attacks over past 12 months", "results of incidents", and "combined impact of laws"; "Strategy" (alpha= -.0385), which was comprised of "critical objectives", "challenges to information security", "priority of information security"; and "Policy" (alpha= -.1098) comprised of "policy formality", "sponsorship level", "end users provide and agree to infosecurity policy", "consequences of violation", and "characteristics of consequences".

Procedures

The Department of Education's NCES IPEDS database provided general contact information for the 600 academic institutions in the sample frame. In addition, the specific professional responsible for information security in each of the 600 institutions had to be identified. Through research on the Internet and the telephone, key information such as the appropriate professional's telephone number,

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

email address and title were identified. A database for tracking participants and recruitment procedures was created.

Recruitment procedures involving mail, telephone, and email invitations were used with all 600 institutions in the sample frame. The two sample frames of 300 institutions were treated identically; the only difference was a three-month difference in contact dates.

Initial contact with potential participants was via a postcard invitation (see Appendix B). This double-sided postcard, outlining the study's objectives, conditions of participation, contents and expected outcomes, was sent to the professional responsible for information security at each institution. Two weeks later, using a standardized telephone script (see Appendix B), the principal investigator, strategic development director and survey telemarketer called each institution to invite the professional responsible for information security to participate in the study. This telephone invitation was followed up by an email invitation to participate in the study (see Appendix B), which reiterated the study's objectives, contents, intended outcomes, conditions of participation, and included a link to the on-line survey.

One month later, the principal investigator, strategic development director, and survey telemarketer conducted a follow-up telephone call (see Appendix B for the script) to each potential participant that had not yet completed the study. As with the initial telephone invitation, this call was followed up by an email invitation to participate in the study (see Appendix B). Three weeks later, the process was completed for the second follow-up with potential participants that had not yet completed the survey. Three weeks after the second follow-up, the process was repeated for the third follow-up with potential participants that had not yet completed the survey. A thank-you email (see Appendix B) was sent to all participants once was data collection was closed in December 2005.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Component #2: Qualitative One-on-One Interviews

Subjects

Information security professionals from twelve(12) academic institutions provided a second, qualitative source of data for this research study through participation in one-on-one semi-structured interviews. Basis for participation in the interviews was voluntary. Inclusion criteria for *institutions* in the interview component of this study were: 1) Title IV status; 2) jurisdiction within the U.S.; 3) degree-granting status; and 4) non-administrative office status. The criterion for inclusion of *individuals* within the institution was role (e.g., information security professional, IT Director, CIO, or other professional responsible for information security within academic the academic institution). Exclusion criteria for *institutions* from the interviews, which paralleled criteria for inclusion, were: 1) non-Title IV status; 2) jurisdiction outside the U.S.; 3) non-degree-granting status; and 4) administrative office status. The criterion for exclusion of *individuals* within the institutions was role (e.g., non-security-related role or non-IT-related role). Please see Appendix C for more details about inclusion and exclusion criteria for the study's one-on-one interviews.

Characteristics. Characteristics of subjects that participated in the interview component of this study are described in the following pages. Characteristics of the twelve (12) *institutions* participating in the survey include: funding control; highest degree offered; Carnegie classification; total student enrollment; region; degree of urbanization; membership, accreditation and special groups served. Characteristics of *individual* respondents within the institutions include title and level.

Funding Control. Institutions participating in the interviews were evenly split between public (N = 6; 50%) and public (N = 6; 50%) funding control. Within the six institutions that are publicly funded, control is primarily at the state level (N = 5; 83%), with one institution controlled at the federal

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

level (N = 1; 17%). All of the institutions that are privately funded are not-for-profit institutions; two-thirds (N = 4; 66%) have no religious affiliation and one-third (N = 2; 33%) have a religious affiliation.

Highest Degree by Funding Control and Highest Degree Offered. All of the interview participants are four-year or above institutions. Half of these institutions are public (N = 6; 50%) and half are private not-for-profit (N = 6; 50%). The highest degree offered by most of these participants is a graduate degree. Specifically, the highest degree offered by five of the institutions is the doctoral degree (N = 5; 42%), followed by doctoral and first professional degrees (N = 2; 28%), bachelors degree (N = 3; 25%), and masters degree (N = 2; 17%).

Carnegie Class. Participants' Carnegie Class categories include doctoral (intensive and extensive) institutions (N = 6; 50%), masters (I and II) institutions (N = 3; 25%), baccalaureate (general and liberal arts) institutions (N = 2; 1%), and specialized institution (N = 1; 8%).

Total Student Enrollment. The total number of students enrolled on a full-time or part-time basis at participating institutions ranges from 847 to 49,203 students. Approximately one-third of participants in the interviews were from institutions with a total enrollment of more than 25,000 students (N = 4; 33%). The rest of the institutions were roughly evenly distributed in their total enrollment, with just over fifteen percent of the participants having a total enrollment of 1 – 2,000 students (N = 2; 17%), less than one-tenth having a total enrollment between 2,001 – 4,000 students (N = 1; 8%), just over fifteen percent with 4,001 – 8,000 students (N = 13, 18%), and just under having 8,001 – 15,000 students (N = 15; 21%). This distribution is slightly different from survey participants, in which just over ten percent had more than 25,000 students (N = 8; 11%).

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Region. Half of the interview participants are from the Northeast region of the U.S. Specifically, six institutions (50%) are located in the Northeast; two (17%) are in the South; two (17%) are in the Midwest, and two institutions (17%) are located in the West. The Department of Education's region classification provides further granularity. Two-thirds of the interview participants are from the East Coast of the U.S. Specifically, six institutions (50%) are located in the Mideast (i.e., DE, DC, MD, NJ, NY, PA) and two institutions (17%) are located in the Southeast (i.e., AL, AK, FL, GA, KY, LA, MS, NC, SC, TN, VA, WV). Less than one quarter of participants are located the West Coast: one institution (8%) is located in the Southwest (i.e., AZ, NM, OK, TX) and one institution (8%) is located in the Far West (i.e., AK CA, HI, NV, OR, WA). Less than one quarter of participating institutions are located in the Midwest: two institutions (17%) are located in the Great Lakes (i.e., IL, IA, MI, OH, WI).

Degree of Urbanization. Interview participants tend to be located in urban areas. Specifically, almost three-fourths of the participants are located either in a large city (N = 3; 25%), urban fringe of a large city (N = 2; 17%), or a mid-size city (N = 3; 25%). The remainder are located in the urban fringe of a mid-size city (N = 2; 17%) or a small town (N = 2; 17%).

Membership, Accreditation, and Special Groups Served. Almost all of the interview participants are EDUCAUSE members (N = 11; 92%) and two-thirds of the institutions are National Security Agency (NSA) CAE-accredited (N = 4; 33%). The EDUCAUSE distribution is roughly representative since most of these participants are doctoral-level institutions; the CAE distribution is higher than the larger academic institution population. Most of the participants do not serve special interest groups: classification by the Department of Education indicates that one institution (8%) has religious affiliation, two institutions (17%) are minority serving, one institution (8%) is Hispanic serving, and none of the institutions (0%) are a tribal college.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Sampling. The Department of Education's National Center for Educational Statistics (NCES) Integrated Postsecondary Education Data System (IPEDS) database provided the basis for the interview sample frame. This database was selected to ensure that survey and interview data sample frames were comparable. The desired sample frame size was twenty (20) academic institutions, based on a targeted sample size of fifteen (15) institutions and a predicted response rate of 80%. Institutions were selected from the database using stratified sampling (funding control, region) then selected from this list using convenience sampling. This strategy was selected because the researchers wanted to leverage their personal relationships to ensure honest answers to potentially sensitive questions and to recruit institutions with certain characteristics (e.g., rural, minority-serving, military) for the study.

Materials. The Information Security in Academic Institutions interview protocol (Burd, S. & Cherkin, S., 2005) is comprised of forty-seven (47) items organized in five sections: Environment, Approaches, Challenges, Resources, and Insights. Items were a combination of closed-response and open-response formats. The interview can be administered in person or on the telephone, and it is recommended that the participant have a copy of the protocol to ensure the questions are clearly understood. Each interview requires approximately one hour to complete. Please see Appendix C to review the ISAI interview protocol.

Interview protocol development involved three steps. First, results of the focused literature review for the survey were used to identify key critical findings and un-explored issues that should be addressed in the interviews. Second, three information security practitioners were consulted to review the interview protocol as it was being developed. Third, the interview protocol was piloted with three information security professionals; revisions were made based on these pilots. Note that the interview

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

protocol was based on the ISAII model and was intended to provide insight into the development and findings of the quantitative survey portion of this study.

Procedures

Recruitment procedures involved three steps. First, the principal investigator, strategic development director and survey telemarketer called the information security professional in each institution to invite him/her to participate in a one-on-one semi-structured interview (see Appendix C for the telephone script). This telephone invitation was followed up by an email invitation to participate in the interview and contained an overview of the study and the interview process and protocol (see Appendix C for the email and interview overview). If the participant immediately agreed to participate, the interview was scheduled and completed either in person or via telephone. If the participant did not immediately agree to participate, the team member who originally contacted the information security professional called again two weeks later. As with the original invitation, the telephone call was followed up with an email invitation to participate in the interview and an overview of the interview process and protocol.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Component #3: Empirical Analysis of Network Activity

The network analysis component of this research study provides independent, objective data regarding exposure of academic institutions' systems and their potential threats to other entities. Outcomes of this assessment include: 1) empirical baseline of the level of "exposure" (i.e., attacks on the institutions) and "threat" (i.e., potential attacks on other organizations via institutions); 2) confirmation or contradiction of survey and interview data; and 3) insight into links between other entities' impact on academic institutions and the institutions' impact on other entities. To accomplish this objective assessment of participants' network activity, the research team developed the Higher Education Network Analysis (HENA) tool, which is described later in this section of the document.

Subjects

Two academic institutions participated in the Network Analysis component of this research study for six months (January 1, 2006 - June 30, 2006). Criteria for inclusion in the study were: 1) Title IV status; 2) jurisdiction within the U.S.; 3) degree-granting status; 4) non-administrative office status; and 5) ability to provide access to the institution's network over eleven months for tool development and data collection. Exclusion criteria were: 1) non-Title IV status; 2) jurisdiction outside the U.S.; 3) non-degree granting status; 4) administrative office status; and 5) inability to provide access to the institution's networks for eleven months.

Characteristics. While the participating institutions are similar in highest degree offered and Carnegie Classification, they differ in terms of funding control, total student enrollment, region, degree of urbanization, membership, accreditation, and special groups served. Specifically, one of the participants is a publicly funded institution with control at the state level; the other participant is a private, not-for-profit institution. Both participants offer primarily baccalaureate degrees and above,

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

with the doctorate as highest degree offered (one participant's Carnegie Class is Doctoral/Research Universities - Extensive and the other's is Doctoral/Research Universities - Intensive). The two participating institutions' sizes are quite different; the publicly funded participant has a total enrollment of over 61,000 undergraduate, graduate, and professional full-time and part-time students on four campuses, while the privately funded participant has a total enrollment of approximately 2,800 full-time and part-time students on one campus. Participants are located in disparate regions (U.S. Census Bureau classification): one participant is located in the Northeast and the other is located in the West. One participant is located in a mid-size city and the other is located in a large city. The two participants also have different membership and accreditation. One of the participants is an EDUCAUSE member and not a National Security Agency (NSA) Center of Academic Excellence, while the other participant is not an EDUCAUSE member and is an NSA Center of Academic Excellence. Neither of the participants is classified by the Department of Education as serving special groups; that is, neither participant is listed in the historically black, Hispanic-serving, or Tribal institution categories.

Sampling. Participants in this study were identified and recruited through a "sampling of convenience" approach. Specifically, institutions that met the criteria for inclusion in the study and with which members of the research team had professional relationships and were identified and approached. InfraGard (www.infragard.net), a not-for-profit public-private sector partnership to protect critical infrastructure sponsored by the Federal Bureau of Investigation, was extremely fruitful for recruiting participants. Both institutions that participated in the network analysis were approached through InfraGard contacts.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Procedures

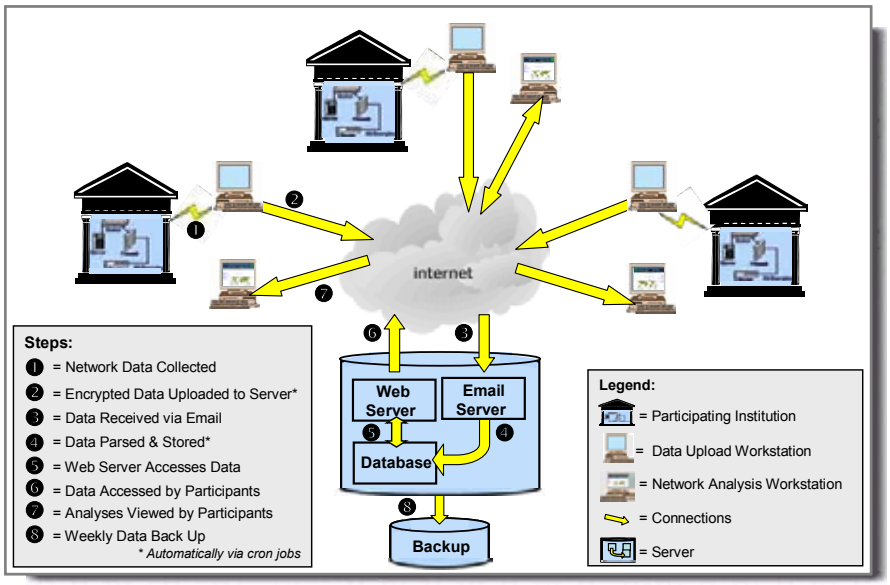
Procedures involved installing the HENA tool on participants' machines and executing the network analysis data collection, analysis, and reporting activities.

Installation. Procedures to install HENA on participants' systems involved three steps. First, each of the participants set up their machine to process This one-time activity, which required approximately one hour, involved selecting the appropriate pre-written client, installing and modifying scripts based on the pre-written client, modifying CVTWIN.INI files for script destination and time zone, and changing the IP filter rule configurations. Second, participants set up log processing and cron jobs for automatic upload every half hour. Third, the data upload, parsing, aggregation and transfer to the website were validated. Participants were assigned a unique username and password to access the user interface. At this point, the process was fully automated, with no additional effort on the participants' part.

Data Collection. Data collection for this study, which commenced on January 1, 2006, involved automated culling, parsing, and uploading of logs from the participating institutions every half-hour (see Exhibit 10 below). Firewall drop log data collected from the institution's firewall application included date/time stamps, IPs (source & destination) and, in the case of TCP and UDP, port numbers (source & destination). Intrusion Detection/Prevention (IDS/IPS) data collected included date/time stamps, IPs (source & destination), port numbers (source & destination) and alert messages. External machine logs (attackers & targets) included date/time stamps, IPs (source & destination), and port numbers (source & destination). All payload data transmitted to and from machines within the institution was excluded from data collection. The research team monitored activity to ensure the entire process was running smoothly.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Exhibit 10. HENA Network Analysis Diagram



Specific data collected for inbound and outbound attacks included type and protocol, source and destination information, and geographic location. Type of attack data was important for understanding attackers' activities, evaluating the potential vulnerability of services, identifying and monitoring security issues, and focusing resource allocation. Protocol (i.e., ICMP, TCP, UDP) attack data was used in conjunction with type of attack data to detect potential vulnerabilities and identify methods to defend against attack. Geographic location data provided insight into which countries were associated with attackers and targets. Note, however, that since location obfuscation is a common practice for avoiding detection and legal prosecution, this data provides insight only into the last leg of the inbound attack and the first leg of the outbound attack. While this data might be used to identify attackers and pursue legal prosecution, it is outside the scope of this current study. Correlating inbound and outbound attacks to identify transient attack traffic was also outside the scope of this current study.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Data analysis. Data analysis, most of which was also automated, involved querying and analyzing data at the lowest common denominator to empirically assess level of exposure and threat. Attacks were correlated across all participants with statistics such as "top 10 worldwide attackers", including their IP address, host name, number of entries implicating the attacker, and number of hosts attacked. Participants could analyze the study's data whenever they wished by accessing the user interface and monitoring aggregate and individual level data.

Materials

The Higher Education Network Analysis (HENA) tool provides a systematic, empirical approach to assessing the exposure of academic institutions' systems and their potential threats to other entities. HENA is a tailored version of DShield (www.DShield.org), the attack-correlation engine of the SANS Internet Storm Center. It is a robust, cost-effective, efficient, and scalable tool that can be used in developing an objective assessment of information security in academic institutions, helping detect and prevent attacks, and generating data-driven recommendations for policy and practice.

The HENA tool's user interface enables participants to view network analysis data at the aggregate and individual levels by clicking on the "Summary Information" or "Participant Data" tabs. Following is a brief description of both of these sections of the HENA interface.

Summary Information. The "Home" page (see Exhibit 11 below) provides several options for viewing data. For example, participants can review status and trends (i.e., survival time, SANS Internet Storm Center Status), the top ten attackers and targets, and access the ISAI and DShield home pages.

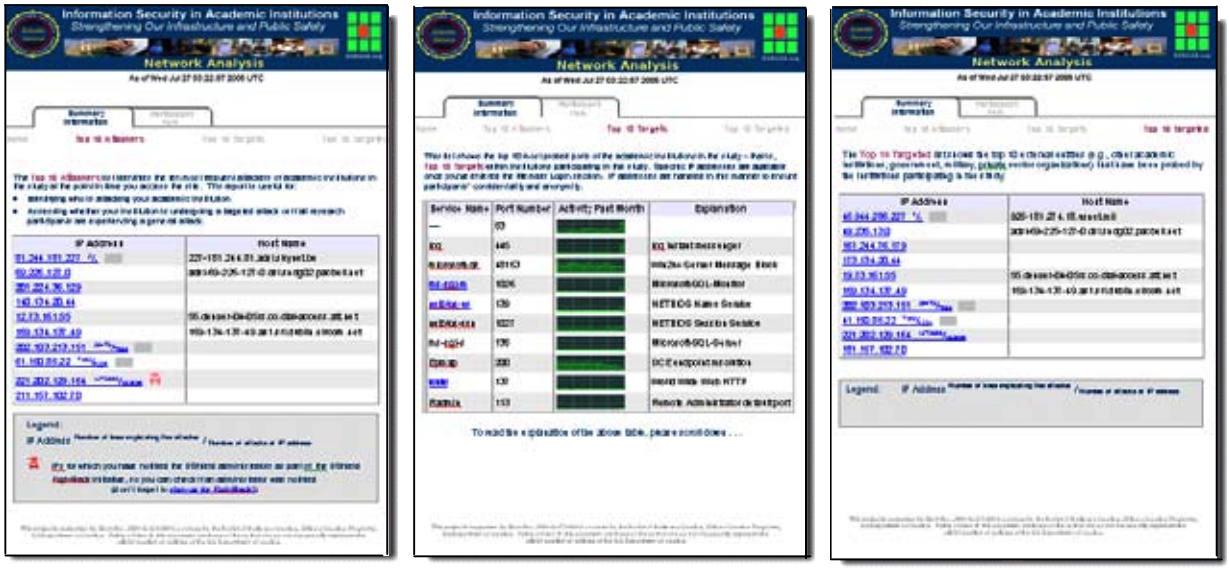
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Exhibit 11. Home Page of HENA's User Interface

Other pages in this section (see Exhibit 12 below) provide more targeted aggregate-level information. The second page of Summary Information, "Top 10 Attackers", provides information about the top ten attackers of participants in this study. This data is useful for identifying attackers of participating institutions and determining whether participants are undergoing targeted or general attacks. Participants can click through the attackers' IP addresses to learn more about attackers and report them to DShield's Fightback program. The third page of Summary Information, "Top 10 Targeted", provides aggregate and sanitized information about the participants' top ten most probed ports. Participants can click through general information about service name, port, and activity over the past month. The fourth page of Summary Information, "Top 10 Targets", provides aggregate and sanitized information about the top ten external entities (e.g., other academic institutions, military, public and private organizations) that were probed by participants' machines. Participants can click through IP addresses to learn more about targets and view the number of lines implicating the attacker.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

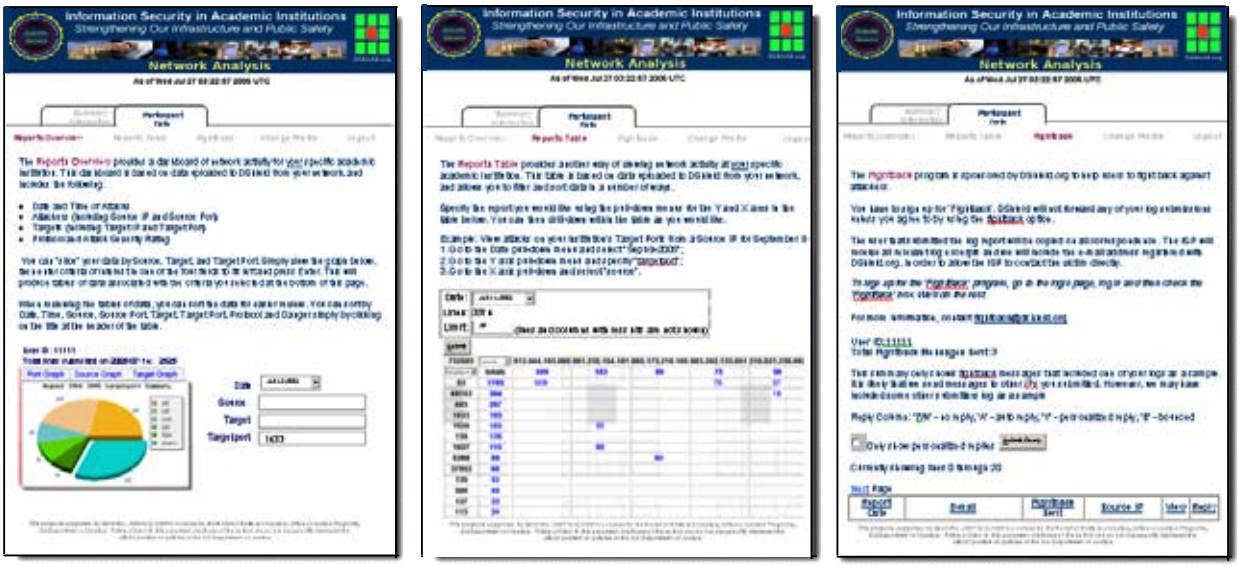
Exhibit 12. Screenshots of "Summary Information" Options



Participant Data. Each participant accesses their particular institution's data in the Participant Data portion of the user interface using the secure Member Login. The first page of Participant Data, "Reports Overview", provides a dashboard of network activity for the particular institution. It includes date and time of attacks, information about attackers and targets, and protocol and attack severity ratings. Participants can click through graphs of activity related to ports, attackers, and targets. The second page of Participant Data, "Reports Table", provides a table-based version of activity data for the particular institution. The third page of Participant Data, "Fightback", enables participants to report attackers to Fightback, a program sponsored by DShield. The final page of Participant Data, "Change Profile", enables participants to modify attributes related to their profile in the research study.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Exhibit 13. Screenshots of "Participant Data" Options



Development. As mentioned in the previous section, HENA is based on the robust technology of DShield, the attack-correlation engine that powers the SANS Institute's Internet Storm Center. Processing over 24 million records per day for contributors from the government, private, not-for-profit and higher education sectors, DShield enables these entities to share invaluable information about intrusions into their networks.

In 2005, DShield partnered with the Information Security in Academic Institutions research study (funded by National Institute of Justice Grant No. 2004-IJ-CX-0045) to create a sector-specific version of the service for academic institutions. Leveraging DShield's proven, scalable architecture, the ISAI study developed this prototype distributed intrusion detection system for academic institutions.

Development of the HENA tool involved four steps. First, four information security professionals in academic institutions were interviewed to understand the relevance of the standard version of DShield to academia. These professionals provided input as to which features should be kept, modified,

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

dropped, or added. Second, the research team modified the front-end and back-end components. They modified the front-end user interface pages, links and information (e.g., time and type of attack data, country source and target data). They modified the back-end by shifting data transmittal from email to direct upload and by creating a new database structure to suit the front-end functionality requirements. Additionally, the user interface's security was hardened using the Secure Socket Layer (SSL) protocol. Third, the research team piloted the customizations with network analysis participants and other information security and academia professionals. Fourth, the research team re-wrote aspects of the scripts and incorporated ongoing modifications.

As the research team identifies further refinements to the HENA tool's data collection and reporting features, they will continue to modify its front-end user interface and its back-end coding and database structure.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

RESULTS

Results of this research study were obtained from seventy-two (72) academic institutions participating in the ISAI survey, fifteen (15) institutions completing one-one-one semi-structured interviews, and two (2) institutions' provision of network activity. These sources of data were analyzed separately and then integrated to identify similarities and disparities in findings and to develop a comprehensive, holistic, and empirical assessment of information security in academic institutions.

Evaluation Criteria for Project Objectives

The three objectives of the project were to collect, create, and disseminate critical information about academic institutions' information security issues and approaches. Below is an explanation of the objectives and the means by which progress on each objective was tracked.

The first objective of the project was to collect quantitative and qualitative data from representative samples of information security professionals in academic institutions across the U.S. Evaluation criteria for the first objective included: 1) participation of one hundred (100) information security professionals in a survey (expected response rate 30%); 2) participation of fifteen (15) information security professionals in one-on-one semi-structured interviews (expected response rate 80%); 3) participation of two institutions in analysis of their networks (expected response rate 40%). These evaluation criteria were partially met. Specifically, the survey component of the study achieved a lower-than-expected response rate (12%), despite intensive recruitment procedures (i.e., written, telephone and email invitations and three rounds of follow-up). However, the interview component of the study achieved the expected response rate (80%), and the network analysis component achieved a higher-than-expected response rate (100%) and also involved development of Higher Education Network Analysis (HENA), a groundbreaking network analysis tool for academic institutions.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The second objective of this research study was to create a clear profile and practical roadmap for improving information security by integrating the quantitative (survey and network analysis) data and qualitative (interview) data. Evaluation criteria for the second objective included: 1) creation of a valid and reliable survey instrument; 2) development of a useful interview protocol; 3) production of quarterly, interim and final reports to the National Institute of Justice; 4) creation of a report of interview results; 5) development of a clear profile of information security in academic institutions; and 6) creation of a practical roadmap for moving forward. Each of these five evaluation criteria was successfully met.

The third objective of the project was to disseminate the project findings to constituencies in academia, law enforcement, government, public/private partnerships, security industry and the public as appropriate via written, presentation and media channels. Evaluation criteria for the third objective included: 1) creation of one white paper; 2) publication of four articles in trade journals; 3) completion of four presentations; and 4) possibly achieving media coverage. These criteria were either met or exceeded. Specifically, one white paper, four articles in trade journals, and four presentations were successfully completed. Further, the project received media coverage in over thirty news, technology, government and academic outlets (e.g., USA Today, MSN Technology and Gadgets, IEEE, CNET, DHS Daily Open Source Report, Chronicle of Higher Education, EDUCAUSE). Other countries, including Indonesia, Hungary, Italy, and Hong Kong, also featured the network analysis component of the study.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Overview of Findings

Below is an overview of the study's findings, organized according to the areas of inquiry and their associated hypotheses. For ease of reference, a summary symbol is provided to the left of each hypothesis:

☑ Hypothesis was supported by this study's findings;

☒ Hypothesis was not supported by this study's findings.

A brief explanation of findings follows each hypothesis that was *not supported* by this study's findings. Detailed findings for all hypotheses are described in the following section of this document.

Environment Hypotheses

☑ **The number of attacks on academic institutions has increased this year as compared to last year.**

☑ **Information security incidents in academic institutions involve a wide range of results, particularly unauthorized access to personally identifiable information.**

☒ **Laws and regulations have had little impact on improving information security in academic institutions over the past year.**

Overall, participants reported that laws and regulations have had a moderate to high impact on improving information security at their institutions. The most influential laws and regulations, descending order of influence, were Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach Bliley Act (GLB), Sarbanes-Oxley, and California Law SB1386. Interestingly, while GLB and Sarbanes-Oxley do not relate directly to academic institutions, they had a positive impact on improving information security in participants' institutions.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Strategy Hypotheses

- ☒ **Key information security objectives are to fulfill executive directives and to avoid negative publicity.**

  Participants' strategic objectives reflected a mix of concerns for the end-users, the institution, legal compliance, and their own professional standards. The three most frequently reported objectives were to protect end users' privacy, fulfill ethical responsibility, and fulfill legislative regulation.

- ☑ **Faculty and students have the lowest priority ratings for information security; IT staff and executives have the highest priority ratings for information security.**

  Note, however, roughly two-thirds of the top ten high-impact challenges involved cultural issues relating to senior executives and end-users.

- ☑ **Information security policies are typically sponsored at the IT Department rather than executive level.**

- ☑ **Less than half the institutions employ an Information Security Officer or person with a similar role.**

- ☒ **Over half of the institutions have conducted one or no information security assessments within the past twelve months.**

  Participants have conducted a variety of assessments over the past year; the most frequently conducted were vulnerability assessments and audits. They have also used a range of techniques to evaluate their information security over the past year; the most frequently used were network traffic flow reports, help desk calls, firewall logs, reports from staff, and incidents.

- ☑ **The budget for information security is less than 5% of the central IT budget for over three-fourths of institutions.** Note, however, that some sub-groups of participants appear to be strongly supported in terms of employees and budget. Approximately 16% of participants employ three or more full-time staff with a role dedicated solely to information security, and approximately one-third of participants have 8% or more of the central IT budget allocated to information security.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Policy Hypotheses

- ☑ Most institutions rely on a combination of informal and formal information security policies.
- ☒ Most of the institutions' end users are provided with the information security policy are required to officially agree an electronic or written version of this policy.

  Roughly two-thirds of participating institutions have provided their end users with the information security policy within the past 12 months – that is, a written or electronic version of the policy has been provided to these end user groups. However, less than half of participating institutions have required their end users' officially agreement to the information security policy within the past 12 months – that is, a written or electronic version of the policy has been provided plus explicit agreement to the policy has been required.
- ☑ Consequences for violating the information security policy are inconsistently enforced.

Information Hypotheses

- ☑ Over three-fourths of institutions share sensitive information with a variety of government agencies.
- ☒ Methods to secure sensitive information are consistently used by less than half of the participants.

  Participants use a broad range of methods to protect their sensitive information; the three most frequently used methods are firewalls, role-based access control, and physical separation.
- ☒ Less than half the academic institutions use criminal background checks or reference checks on a regular basis.

  Over half the participants conduct criminal background checks and over three-fourths use reference checks.
- ☑ Less than half the institutions have conducted an information asset classification in the past 12 months.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

People Hypotheses

- ☑ Academic institutions use a range of awareness and training methods; however, few of these methods are considered very effective.
- ☑ Less than one-fourth of institutions have mandatory awareness and training methods; however, most of these methods are considered very effective.
- ☒ Over half the institutions seek information security certifications when hiring or promoting staff.

  Slightly over half the participants do *not* seek certifications when hiring or promoting staff.

Process Hypotheses

- ☑ Automatic patch management is the most effective, but not most frequently used, method for patching computers owned and not owned by academic institutions.
- ☑ Less than one-quarter of institutions issue standardized computers; those that do so rate this practice as very effective.
- ☒ Over three-fourths of institutions have a documented IT disaster recovery plan in place.

  Just slightly over one-third of participants have a documented IT disaster recovery in place.
- ☒ Almost half the institutions have documented plans for cyberincident response and for notifying individuals that their private data has been compromised.

  Less than one quarter of participants has a documented cyberincident plan or plan for notifying individuals about private information access. However, many participants are currently considering or developing documented contingency plans or incident response plans. Interestingly, over one-third of participants have an in-house forensic analysis capability.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Technology Hypotheses

- ☑ Over three-fourths of institutions have implemented standard security techniques such as anti-virus software, firewalls and peer-to-peer monitoring and bandwidth shaping.
- ☒ More than half the institutions have implemented encryption technologies for data in transit, on the networks, and backup locations.

  However, encryption is on the horizon; it is one of the top ten technologies that participants rated as "in progress or piloting" and "considering in the next twelve months".
- ☑ Over three-fourths of institutions are not considering filtering technologies such as web, instant messaging or wireless content filtering.

Outcome Hypotheses

- ☒ Over half the institutions consider the likelihood of compromising individuals, other entities or critical infrastructure as moderate or high.

  Overall, participants seem to perceive little likelihood their institution may compromise individuals, other organizations, and critical infrastructure. Over one-half of the participants rated the likelihood that their institution may compromise individuals, other organizations, and critical infrastructure as "low" and almost one-half of them rated the likelihood as "moderate". Just one-twentieth of the participants rated the likelihood as 'high" and, interestingly, almost five percent of participants rated the likelihood as "none".
- ☑ Over half the institutions consider themselves as somewhat prepared for a major information security incident.
- ☑ Over three-fourths of institutions consider themselves more prepared now than two years ago for a major information security incident.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Profile of Information Security in Academic Institutions

A panel of experts comprised of information security experts from higher education, leading government agencies and ISAI team leaders were consulted to interpret the survey data for a profile of information security in academic institutions. All six experts were provided a spreadsheet with each item, its results, and a graphic representation of the results. First, they rated each survey item for its *impact* on information security. A rating of 3 indicated "high impact", 2 indicated "average impact", and 1 indicated "no impact". Second, the experts rated the responses to each item for *level of performance*. A rating of 5 indicated "very good", 4 indicated "good", 3 indicated "average", 2 indicated "poor", and 1 indicated "very poor". These intervals of 1- 3 and 1 - 5 were selected based on pilots with three other experts, who indicated that the task was too complex when impact was rated 1 – 5 and that the scale was not sufficiently detailed when importance was rated 1 - 3. The overall, weighted average rating for all of the survey's items was 2.6 out of 5, which corresponds to just below meeting expectations. Below is a visual depiction of the panel of experts' ratings for each of the eight components of the survey:

Exhibit 14. Summary of Participants' Information Security Profile

Component	Rating
Environment	
Strategy	
Policy	
Information	
People	
Process	
Technology	
Outcomes	

Legend: Very Good Very Poor

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Detailed Findings

Detailed findings of the participants' information security profile are organized according to eight of the components of information security in academic institutions, including: environment, strategy, information assets, policies, technology, people, processes, and outcomes. Physical environment is not addressed in this study, and it was exceedingly well explored in the recent National Summit on Campus Public Safety study. Survey results are also provided in Appendix B for ease of examination.

Environment

The environment in which academic institutions operate was assessed to understand the potential relationships between attackers' activities, results of information security incidents, the impact of laws and regulations, and academic institutions' information security policies and practices.

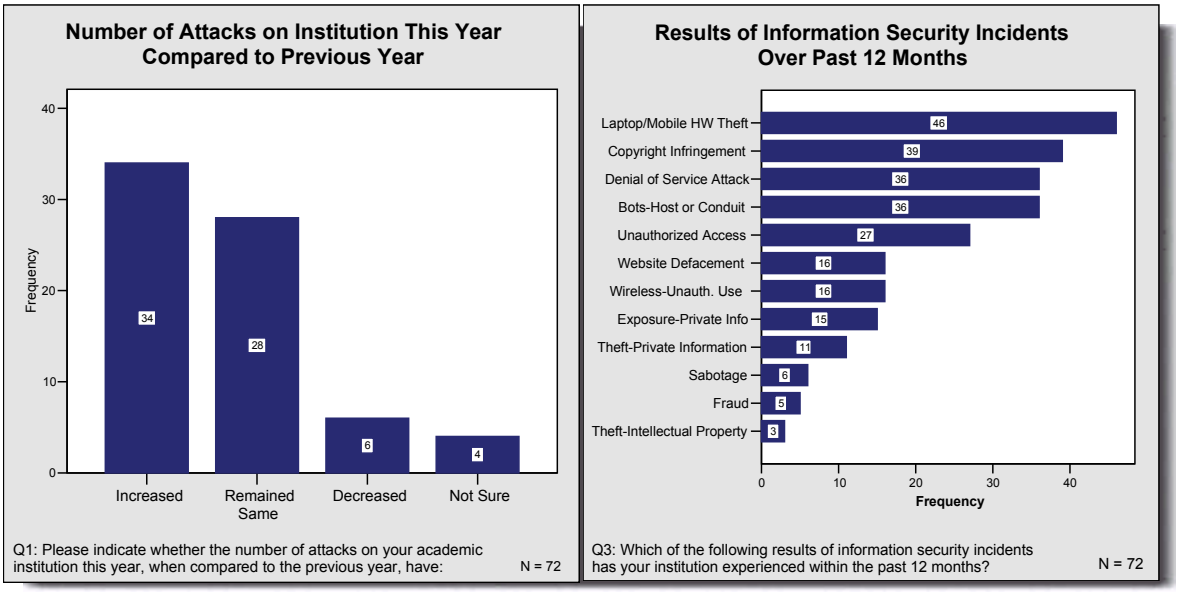
Attacks and Results of Incidents. Over three-fourths of the participating institutions reported an increased number of attacks (N = 34; 47%) or the same number of attacks (N = 28; 39%) as compared to the previous year. Six institutions (8%) reported a decreased number of attacks as compared to the previous year, and four institutions (6%) were not sure of the relative increase or decrease in attacks this year compared the previous year.

Participants reported a range of results of information security incidents at their institutions, as described in Exhibit 15 below. The most frequently cited was laptop or mobile hardware theft (N = 46; 64%), followed by copyright infringement (N = 39; 54%), denial of service attacks (N = 36; 50%), bot hosting or conduit (N = 36; 50%), unauthorized access to information, systems or network (N = 27; 38%), website defacement (N = 16; 22%), unauthorized use of wireless network (N = 16; 28%), exposure of private or sensitive information (N = 15; 21%), theft of private or sensitive information (N = 11; 15%), sabotage (N = 6; 8%), fraud (N = 5; 7%), and intellectual property theft (N = 3; 4%).

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Many of these results of incidents (e.g., copyright infringement, bot hosting or conduit, unauthorized use of wireless network) are to be expected – particularly in an academic environment - and are consistent with other studies. However, of note is the relationship between these reported results and potential compromise of the stakeholders' personally identifiable information (e.g., current and former students, staff, faculty, parents, and affiliates). Specifically, over half of the reported results (i.e., exposure of private information, theft of private information, unauthorized access to information , systems or the network, unauthorized use of the wireless network, bot hosting or conduit, fraud, and theft of laptops or mobile hardware) may directly cause exposure or loss of personally identifiable information. While some of these compromises are identified and reported, as described in the Literature Review, of concern is the number of incidents in which potential compromise is not recognized.

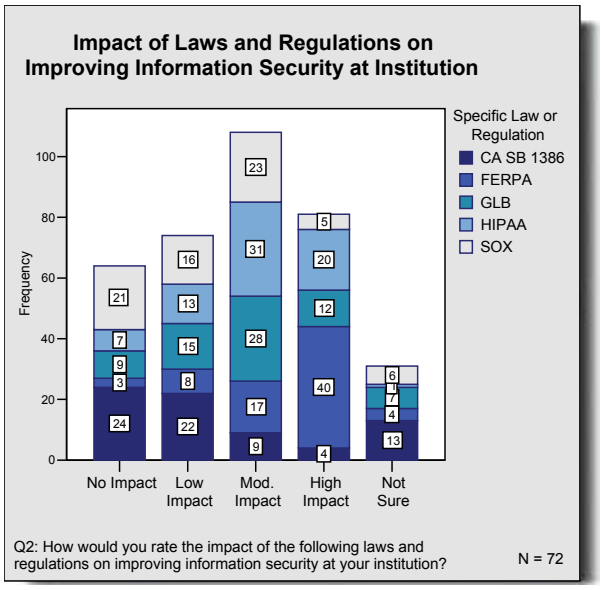
Exhibit 15. Attacks and Results of Incidents over the Past 12 Months



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Impact of laws and regulations. Overall, participants reported laws and regulations as having a moderate to high impact on improving information security at their institutions. The Family Educational Rights and Privacy Act (FERPA) had the highest impact on improving information security at participants' institutions. Over three-fourths of participants indicated that the impact of FERPA was high (N = 40; 56%) or moderate (N = 17; 24%), while the remainder of the sample indicated that FERPA had low impact (N = 8; 11%) or no impact (N = 3; 4%). The Health Insurance Portability and Accountability Act (HIPAA) had the second-highest impact on improving participants' information security. Almost three-fourths of participants indicated that HIPAA had high impact (N = 20; 28%) or moderate impact (N = 31; 43%). The Gramm-Leach Bliley Act (GLB) had the third-highest impact on improving information security; over half the participants reported that GLB had a high impact (N = 12; 17%) or moderate impact (N = 28; 39%). Sarbanes-Oxley had less of an impact on improving participants' information security than other laws and regulations, with less than half the sample rating its impact as high (N = 5; 7%) or moderate (N = 23; 32%). California Law SB1386 was rated by participants as having the least impact on improving information security at their institution; less than one-fifth of the sample rated CA SB1386 as having high impact (N = 4; 6%) or moderate impact (N = 9; 13%).

Exhibit 16. Impact of Laws and Regulations on Participants' Information Security



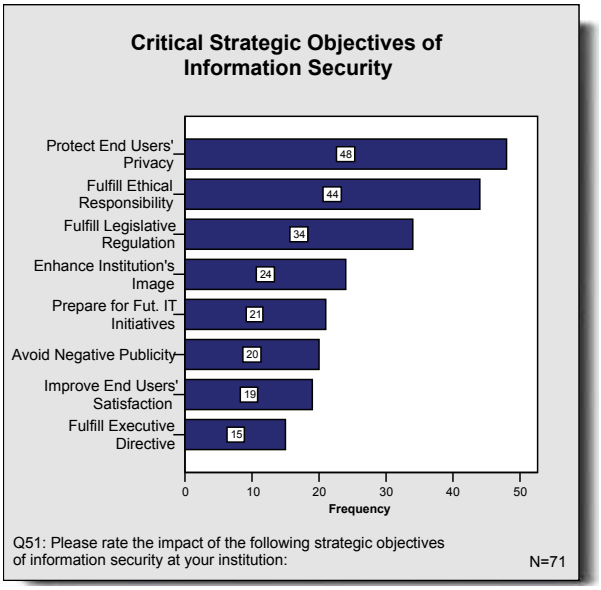
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Strategy

In this study, strategy is considered to include the strategic objectives of information security, challenges faced in attempting to maintain information security, the current priority of information security for institutional stakeholders, and resources invested in information security, such as responsibility for ensuring information security and budget allocated to information security efforts.

Strategic objectives. The three most frequently reported critical strategic objectives were to protect end users' privacy (N = 48; 68%), fulfill ethical responsibility (N = 44; 62%), and fulfill legislative regulation (N = 34; 48%). The remaining critical strategic objectives included enhance institution's image (N = 24; 34%), prepare for future IT initiatives (N = 21; 30%), avoid negative publicity (N = 20; 28%), improve end users' satisfaction (N = 19; 27%), and fulfill executive directive (N = 15; 21%). A graphical representation of strategic objectives is presented below in Exhibit 17.

Exhibit 17. Participants' Critical Strategic Objectives for Information Security



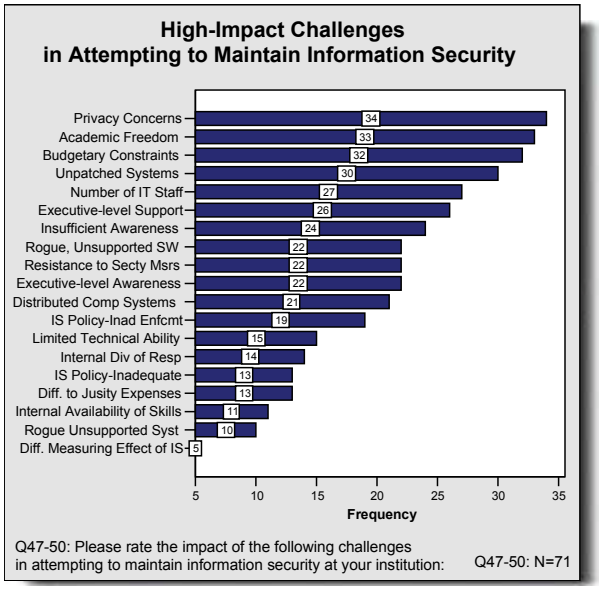
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Challenges. Participants reported a wide range of challenges to maintaining information security at their institutions. The two most widely cited high-impact challenges relate specifically to the academic environment: privacy concerns (N = 34; 48%) and academic freedom (N = 33; 47%). Additionally, of the top ten high-impact challenges, roughly two-thirds related directly to "culture" issues of senior executives and end users. Specifically, issues cited included executive-level support of initiatives (N = 26; 38%), executive-level awareness of issues (N = 22; 31%), resistance to security measures (N = 22; 31%), and insufficient awareness of information security issues (e.g., wireless threats, phishing scams; N = 24; 34%). The other top ten high-impact issues related to resourcing and the unique characteristics of academic institutions. Resource issues included budgetary constraints (N = 32; 45%) and number of IT staff (N = 27; 38%). Characteristics germane to academic institutions included un-patched systems, such as operating system and application holes (N = 30; 42%) and rogue, unsupported software, such as freeware, peer-to-peer software, and specialized applications (N = 22; 31%).

Other high-impact challenges were primarily related to policy, resources, measurement, and other characteristics typical of academic institutions. For example, policy issues included inadequate information security policy (N = 13; 18%) and inadequate enforcement of information security policy (N = 19; 27%). Resource-related issues included internal availability of skills (N = 11; 16%) and internal division of responsibilities for infosecurity (N = 14; 20%). Measurement issues involved difficulty justifying expenses or articulating a business case (N = 13; 18%) and difficulty measuring the effectiveness of initiatives (N = 5; 7%). Other issues related to characteristics typical of academic institutions included distributed computing systems, such as departmental computers (N = 21; 30%), rogue, unsupported computing systems, such as departmental computers and systems (N = 10; 14%), and limited technical ability, such as lack of knowledge in installing antivirus software (N = 15; 21%).

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Exhibit 18. Participants' Challenges in Maintaining Information Security

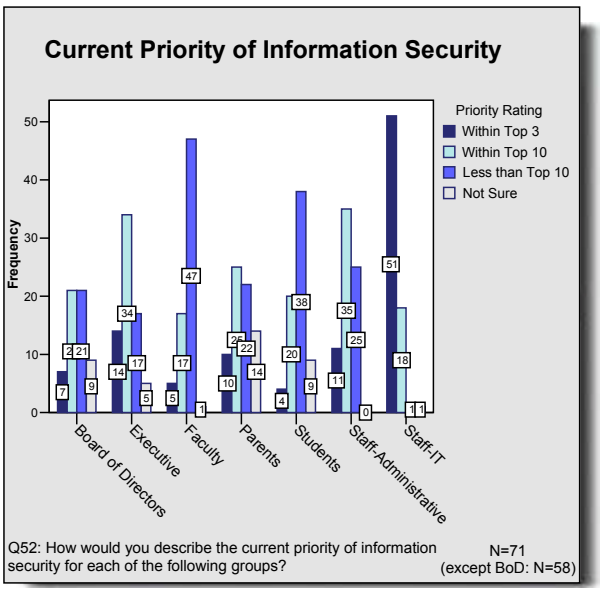


Several interesting contrasts between participants' challenges in maintaining information security and critical strategic objectives of information security exist. First, while the number one critical strategic objective is to protect end users' privacy (N = 48; 68%), the top two high-impact challenges are privacy concerns (N = 34; 48%) and academic freedom (N = 33; 47%). Second, while one of the critical strategic objectives is to fulfill executive directives (N = 15; 21%), two of the top 10 high-impact challenges are executive-level support of initiatives (N = 26; 38%), executive-level awareness of issues (N = 22; 31%). These contrasting results are addressed more fully in the Discussion section of this document.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Stakeholders' current priorities. Overall, the current priority of information security for stakeholders such as executives, students, faculty, and staff is within or less than the "top ten" priorities. Not surprisingly, IT staff rated the current priority of information security higher than other stakeholders, such as the Board of Directors, executives, faculty, administrative staff, and students. Stakeholders' rating of information security as within the "top three" current priorities include IT staff (N = 51; 72%), executives (N = 14; 20%), administrative staff (N = 11; 16%), parents (N = 10; 14%), Board of Directors (N = 7; 12%), faculty (N = 5; 7%), and students (N = 4; 6%). Consideration of stakeholders' ratings as within the "top ten" priorities provides a slightly different perspective. Specifically, ratings shifted to the following order: IT staff (N = 69; 97%); executives (N = 48; 68%); administrative staff (N = 46; 65%); parents (N = 35; 49%); Board of Directors (N = 28; 48%); students (N = 24; 34%); and faculty (N = 22; 31%). Note that Board of Director ratings may slightly higher than indicated in these results, as one version of the on-line survey skipped this item for eleven respondents.

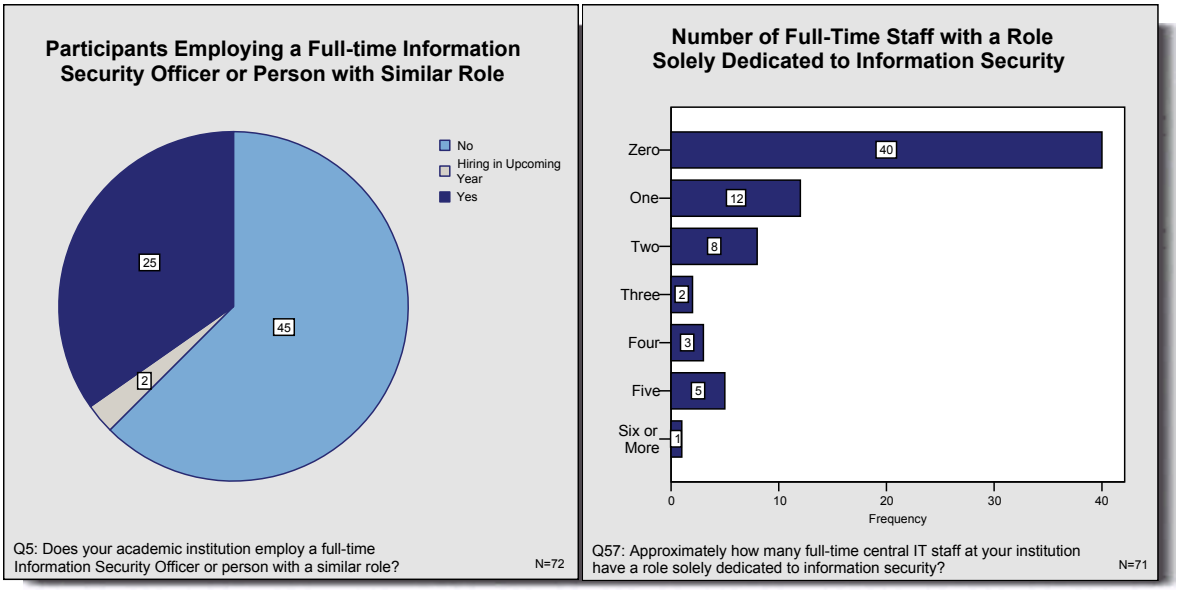
Exhibit 19. Current priority of information security for stakeholders



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Responsibility and staffing. Responsibility for information security of the participating academic institutions seems to lack full-time support and clear accountability. Over half the academic institutions participating in the survey (N = 45; 63%) do not employ a full-time Information Security Officer or person with a similar role (see Exhibit 20 below). Twenty-five of the participants (35%) currently employ a full-time information security professional and two participants (3%) will be hiring an Information Security Officer in the upcoming year. The number of full-time staff dedicated solely to information security (also see Exhibit 20 below) is similar to the findings described above. Specifically, over half of the participants have zero full-time staff members dedicated to information security (N = 40; 56%). Twelve institutions (17%) have one full-time information security staff member and eight institutions (11%) have two full-time information security staff. Two institutions (3%) employee three full-time information security staff, three institutions (4%) have four full-time staff, five institutions (7%) have five staff, and one institution (1%) employs six or more full-time staff dedicated solely to information security.

Exhibit 20. Full-time Staff Responsible for Information Security

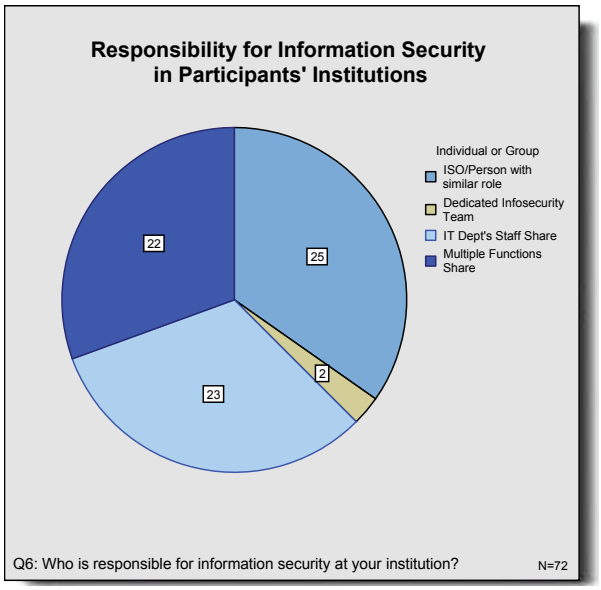


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Institutions participating in the survey cited a range of individuals or groups responsible for information security in their institutions. Approximately one-third of participants have one individual responsible for information security: twenty-five institutions (35%) have an Information Security Officer or person with a similar role that is responsible for information security.

A dedicated information security team is responsible for information security at two institutions (3%). Responsibility is hared between staff or departments for over half of the participants: the IT Department's staff share responsibility at twenty-three institutions (32%) and multiple functions share responsibility for information security at twenty-two institutions (31%).

Exhibit 21. Responsibility for Information Security



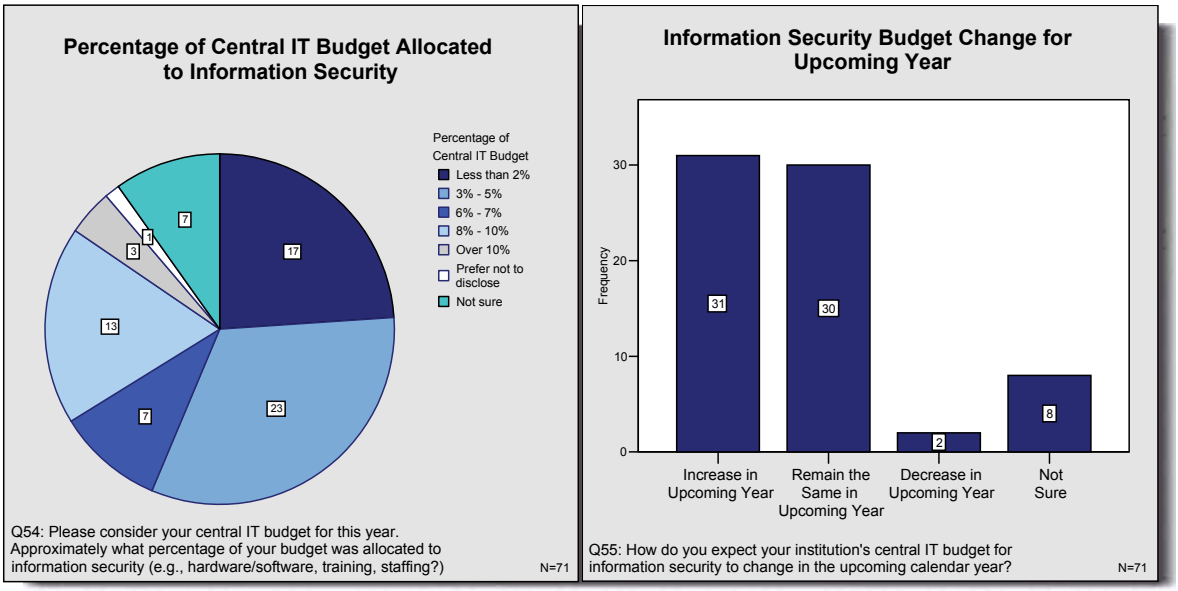
Budget for information security. Participants' budgets for information security ranged from less than 2% to over 10% of their central IT budgets. Over half of the participants have 5% or less of their central IT budget allocated to information security. Specifically, twenty three participants (32%) reported their information security budget as 3% - 5% of their central IT budget and seventeen

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

participants (24%) reported 2% or less of their central IT budgets are allocated to information security. Almost one-third of participants had between 6% and 10% of their central budgets allocated to information security. Specifically, thirteen institutions (18%) had 8% - 10% allocated to information security and seven institutions (10%) had 6% - 7% allocated to information security. Interestingly, three institutions (4%) had over 10% of their central IT budget allocated to information security. Seven participants (10%) indicated that they were "not sure" and one participant (1%) declined to disclose this information.

Over three-fourths of the participating institutions' central IT budgets will increase or remain the same in the upcoming year. Specifically, the information security budget for thirty-one participants (44%) will increase in the upcoming year and thirty institutions' (42%) budgets will remain the same. The information security budgets for two institutions (3%) will decrease in the upcoming year and eight participants (11%) were not sure of the change in central IT's budget for information security in the upcoming year.

Exhibit 22. Budget for Information Security



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

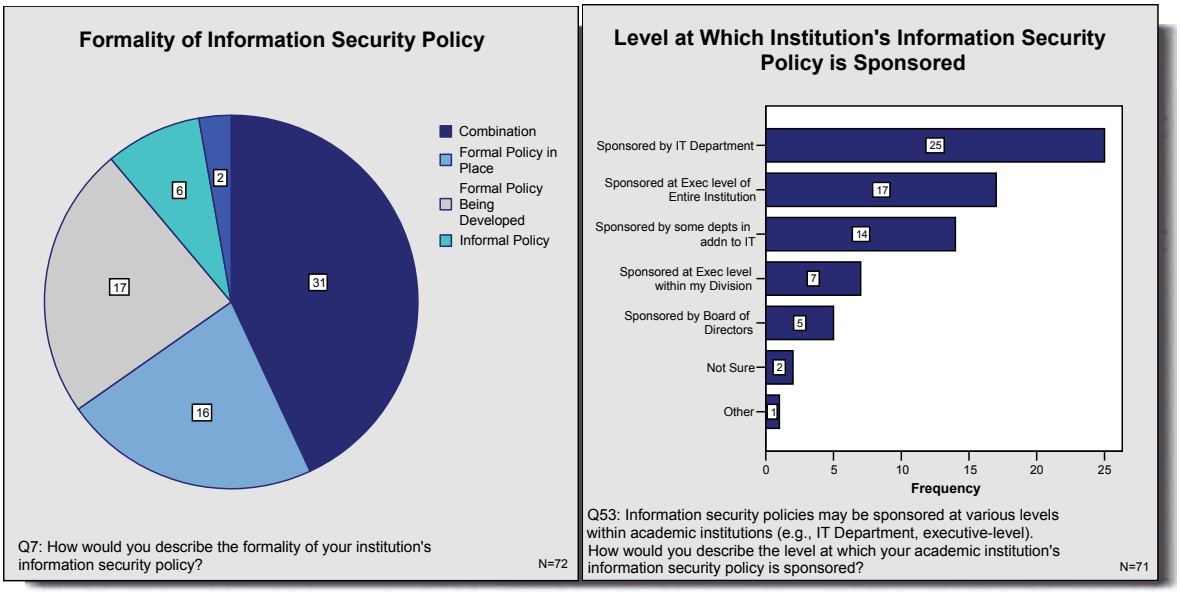
Policy

Policy addresses the aggregate of directives, regulations, rules, and practices that prescribes how each institution manages, protects, and distributes information. Key characteristics include formality, institutional support, consequences, enforcement, provision to and agreement by end users.

Formality and sponsorship. Participants' information security policies are at various stages of development. The most frequently cited are a combination of formal and informal policy (N = 31; 43%). Less than one-quarter of participants have a formal policy in place (N = 16; 22%) or are developing a formal policy (N = 17; 24%). Six institutions (8%) have an informal policy and two institutions (3%) have no information security policy in place.

Participants' information security policies tend to be sponsored either by the IT department (N = 25; 35%) or, interestingly, at the executive level. Over one-third of participants' information security policies are sponsored at the executive level of the entire institution (N = 17; 24%), by the Board of Directors (N = 5; 7%), or within the division (N = 7; 10%). Fourteen institutions (20%) have their policy sponsored by some departments in addition to the IT department.

Exhibit 23. Formality and Sponsorship Levels of Policy



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

End users and the policy. Roughly two-thirds of participating institutions have provided end users with the information security policy within the past 12 months – that is, a written or electronic version of the policy has been provided to these end user groups (versus simply posting the policy on the institution's website). Specifically, fifty-one participants (71%) reported that they provide the information security policy to staff, forty-nine participants (68%) provide the policy to students, forty-eight (67%) provide it to faculty, and twenty-six (36%) provide the information security policy to affiliates such as contractors, visitors, library users, and alumni.

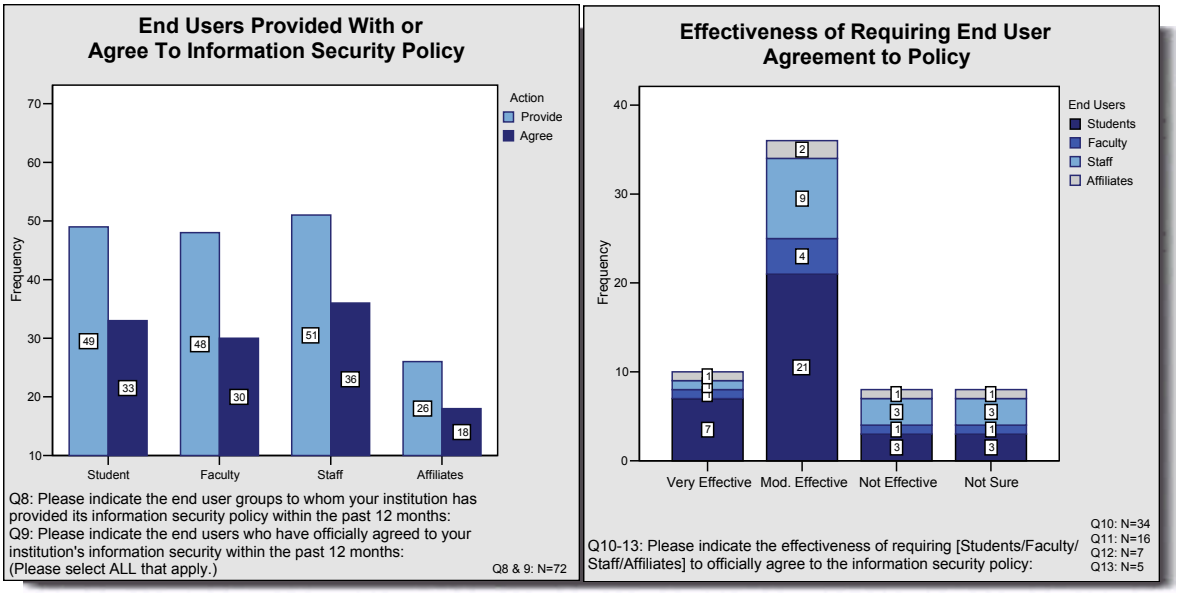
However, less than half of the participating institutions report that they have required their end users' official agreement to the information security policy – that is, a written or electronic version of the policy has been provided plus explicit agreement to the policy has been required within the past 12 months. Specifically, thirty-six participants (50%) require staff to officially agree to the information security policy, thirty-three participants (46%) require students to officially agree to the policy, thirty (42%) require faculty to officially agree to it, and just eighteen (25%) require affiliates to officially agree to the information security policy.

Survey findings indicate that requiring official agreement to the information security policy is most effective with students: seven participants (20%) rate it as "very effective" and twenty-one institutions (62%) rated it as "moderately effective", while three institutions (9%) rated it as "not effective". However, findings indicate that requiring official agreement to the information security policy is not as effective with staff, affiliates or faculty as it is with students. Specifically, the effectiveness of requiring staff to officially agree was primarily rated as "moderately effective" (N = 9; 56%) or "not effective" (N = 3; 19%), while just one participant indicated it was "very effective" (N = 1; 5%). The effectiveness

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

of requiring faculty to officially agree to the policy was rated as primarily "moderately effective" (N = 4; 57%), followed by "very effective" (N = 1; 14%) and "not effective" (N = 1; 14%). The effectiveness of requiring affiliates to officially agree was similarly rated as "moderately effective" (N = 2; 40%), "very effective" (N = 1; 20%) and "not effective" (N = 1; 20%). Ratings for "not sure" for students, staff, faculty, and affiliates respectively, three (88%), three (19%), one (14%), and one (20%).

Exhibit 28. End Users' Provision and/or Agreement to Information Security Policy

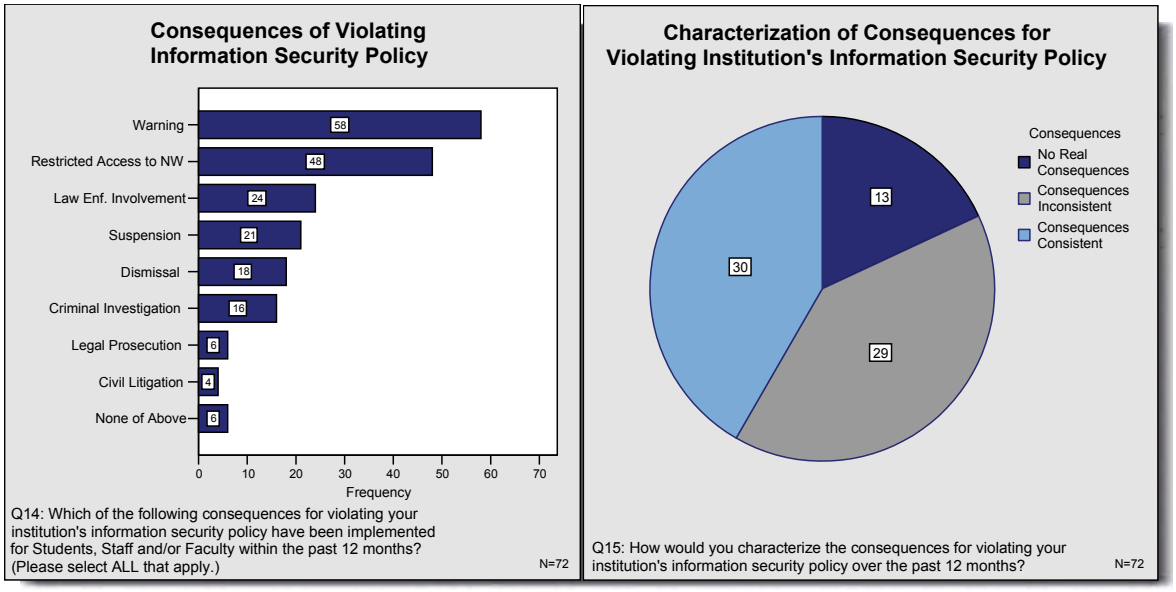


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Consequences and enforcement. Violations of the information security policy over the past twelve months involve a range of internal and external consequences. The two most frequently cited consequences included warning (N = 58; 81%) and restricted access to the network (N = 48; 67%). Interestingly, the third most frequently cited consequence was law enforcement involvement (N = 24; 33%). This was followed by suspension (N = 21; 29%), dismissal (N = 18; 25%), criminal investigation (N = 16; 22%), and civil litigation (N = 4; 6%). Six institutions (8%) stated that none of the above consequences has been implemented in the past twelve months.

Participants also provided information about the consistency of consequences for violating their institution's information security policy. Over half of the participants indicated that consequences are inconsistent (N = 29; 40%) or there are no real consequences (N = 13; 18%). Less than half of the participants stated that consequences have been consistent (N = 30; 42%). These results indicate that, although information security policies with consequences may be in place, inconsistencies in the actual implementation of consequences for violating the information security policy still exist.

Exhibit 24. Consequences and Enforcement of Violating Information Security Policy



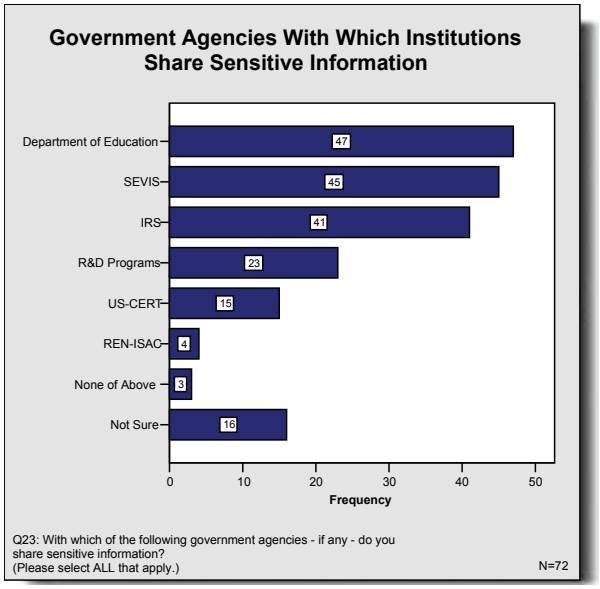
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information

Many academic institutions deal with "sensitive information" – that is, personally identifiable information about students, faculty, or staff (e.g., social security number, date of birth, medical data) and non-public information (e.g., technical, medical, government-related research data). A critical but often overlooked component of information security programs is classification of the actual information and its associated systems. This study briefly addresses information classification by reviewing issues related to creating, processing, or sharing sensitive information.

Sharing Sensitive Information. Participants share sensitive information with a variety of government agencies. The most frequently cited government agency is the Department of Education (N = 47; 65%), followed by the Student and Exchange Visitor Information System (SEVIS; N = 45; 62%), and the Internal Revenue Service (N = 41; 57%). They also share sensitive information with US-CERT (N = 15; 21%) and the REN-ISAC (N = 4; 6%). Three participating institutions (4%) share sensitive information with none of these agencies and sixteen (22%) responded that they are not sure of which government agencies with which their institutions share sensitive information.

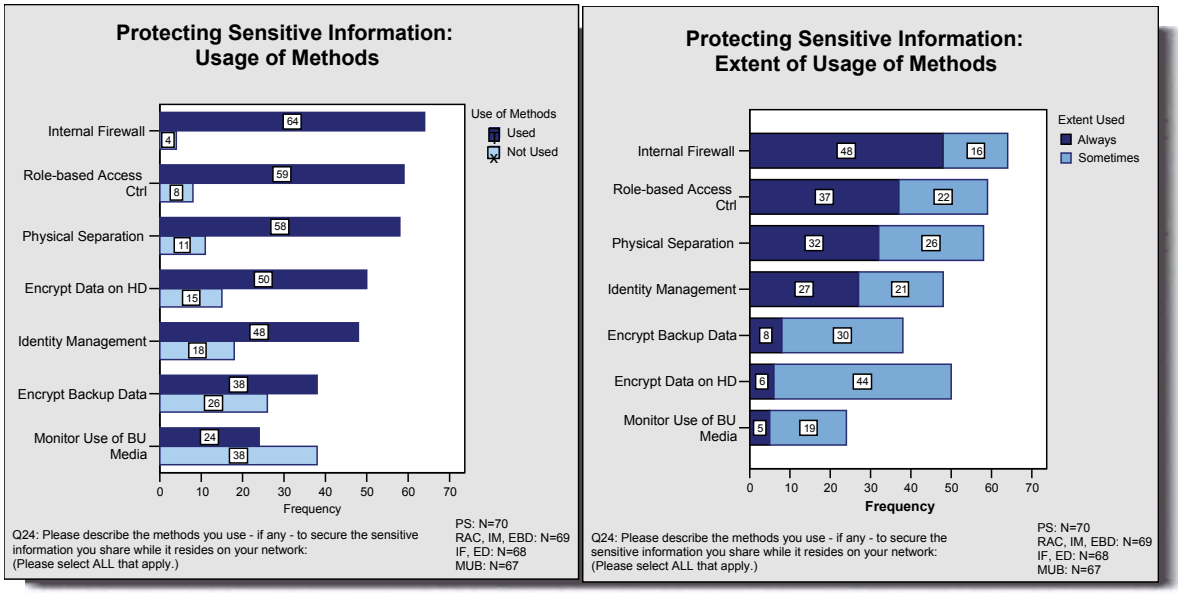
Exhibit 25. Agencies with which Institutions Share Sensitive Information



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Methods to protect sensitive information. Institutions participating in the survey indicated a broad usage of methods to protect sensitive information. Internal firewalls were the most frequently used method to protect sensitive information (N = 64; 94%), followed by role-based access control (N = 59; 86%), and physical separation (N = 58; 83%). Two of the three most frequently used methods to protect sensitive information involved software and hardware separation: firewalls were used by sixty-four participants (94%) and physical separation was used by fifty-eight participants (83%). User access methods, such as role-based access control (N = 59; 86%) and identity management (N = 48; 69%), were used by participants, as were encryption methods such as encrypting data on hard drives (N = 50; 69%) and encrypting data for off-site storage (N = 38; 63%). Monitoring use of backup media (e.g., thumb drives/USBs, CDs) was used by twenty-four (36%) of the participating institutions.

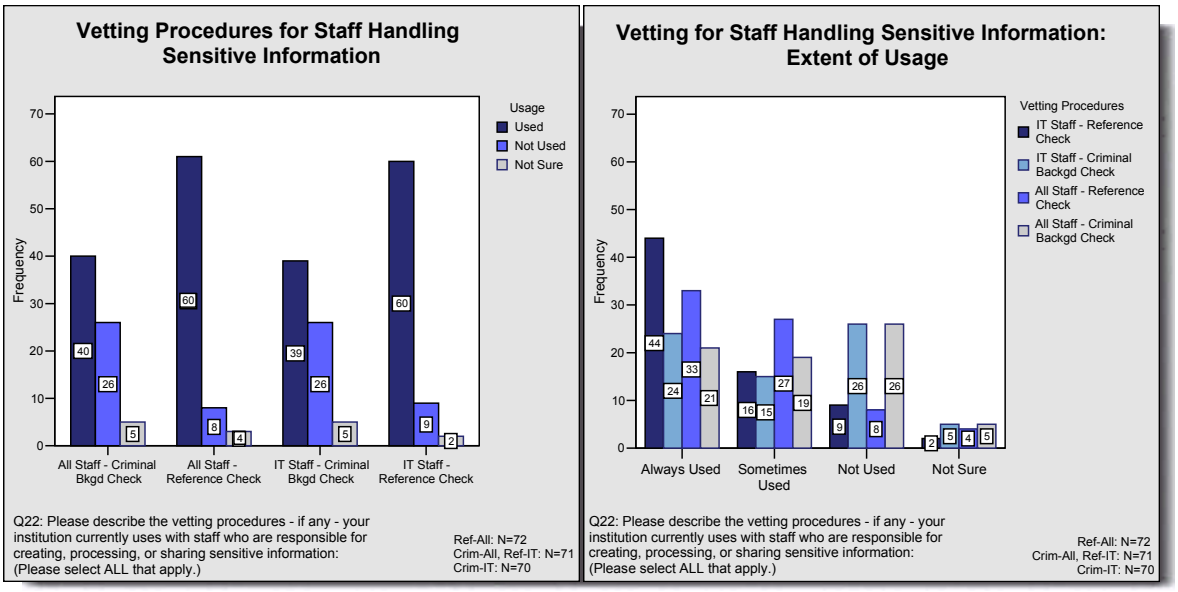
Exhibit 26. Use of Methods to Protect Sensitive Information



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Vetting procedures for staff handling sensitive information. Vetting procedures are part of the personnel security requirements that ensure individuals occupying positions of responsibility within academic institutions (including third-party service providers) are trustworthy and meet established security criteria for their duties. Over three-fourths of participants use reference checks to vet staff handling sensitive information: sixty institutions (83%) indicated they conduct reference checks for both IT staff and all staff. Over half of the participating institutions use criminal background checks: forty institutions (55%) conduct criminal background checks on all staff and thirty-nine (54%) institutions conduct criminal background checks on IT staff.

Exhibit 27. Personnel Security for Sensitive Information



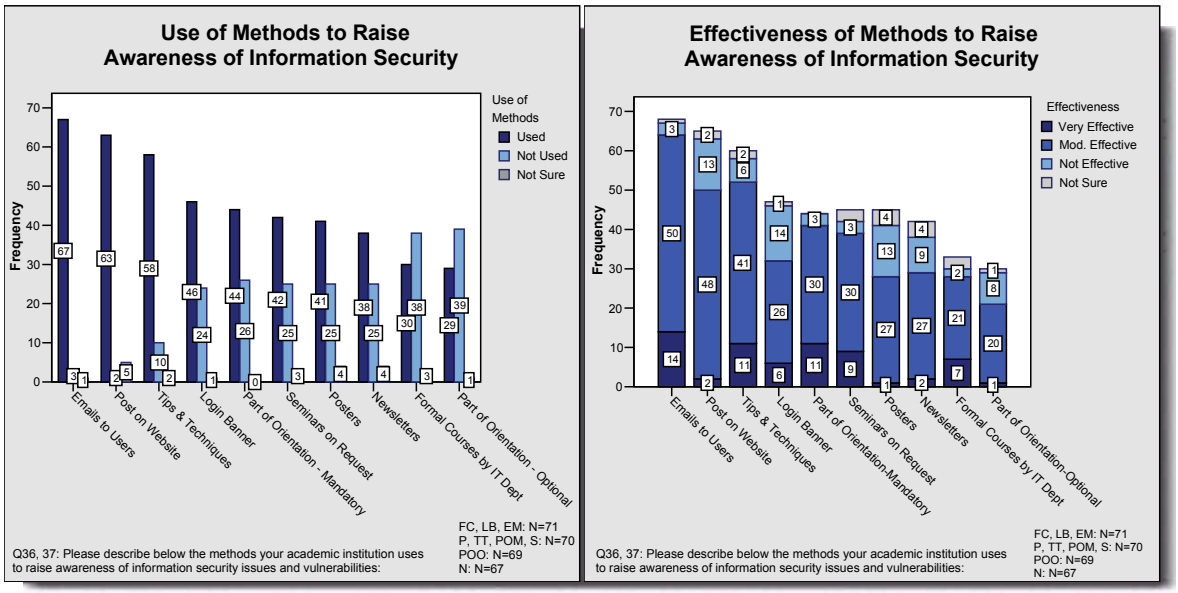
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

People

In this study, "people" are defined as the executives, faculty, staff, students, and affiliates that use (i.e., create, access, store, share) or are responsible for the institution's information or information systems. "Awareness and training" involves ensuring that users are aware of the security risks associated with their activities (including applicable laws, policies, and procedures) and that they are adequately trained to carry out their activities without posing a threat to the institution's information security.

Methods to raise awareness. Participants use a relatively wide range of methods to raise awareness of information security in their institutions. Emails to users (N = 50; 70%), postings on the website (N = 48; 69%) and tips and techniques (N = 41; 59%) were most widely used, followed by use of a login banner (N = 26; 37%), posters (N = 27; 39%), seminars on request (N = 30; 43%), mandatory part of orientation (N = 30; 43%), newsletters (N = 27; 40%), formal courses offered by the IT Department (N = 21; 30%), and optional part of orientation (N = 20; 29%). The three methods with the highest percentage of "very effective" ratings were emails to end users (N = 14; 20%), tips and techniques (N = 11; 16%), and mandatory part of orientation (N = 11; 16%). Note, however, that methods rated as very effective which are difficult to implement, such as mandatory part of orientation and formal courses offered by IT department (N = 7; 10%) seem to be less-used.

Exhibit 29. Use and Effectiveness of Methods to Raise Awareness of Information Security

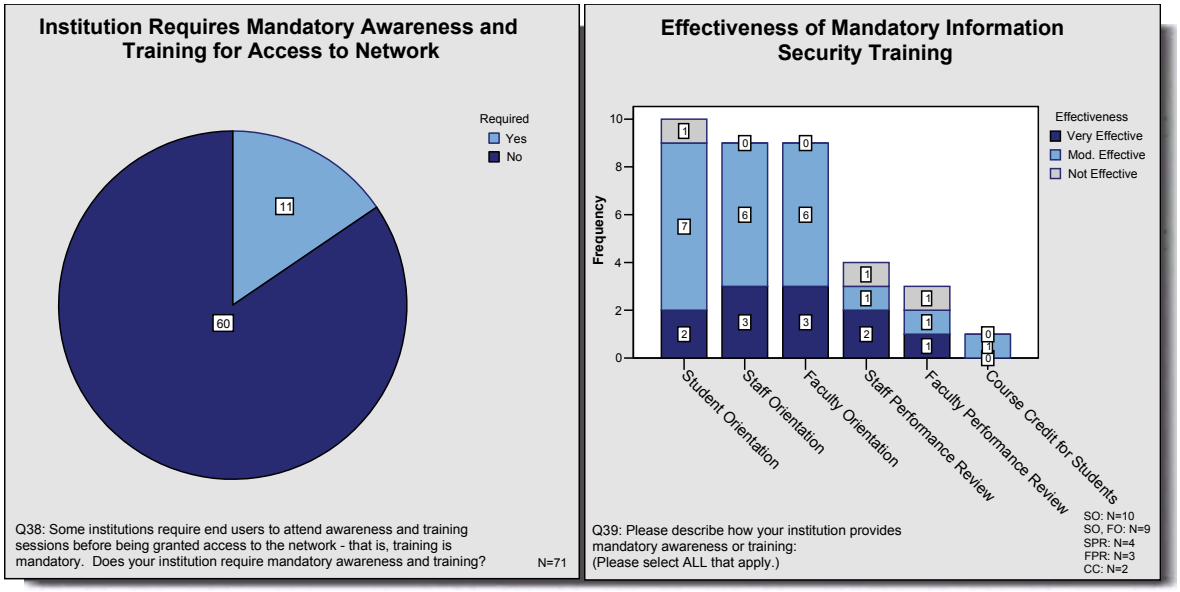


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Mandatory awareness and training. Almost ninety percent of institutions participating in the survey (N = 60; 85%) do not require end users to attend mandatory awareness and training sessions before being granted access to the network. Of the eleven (16%) institutions that do require mandatory awareness and training to access the network, the most frequently implemented method is student orientation (N = 10; 62%), followed by faculty orientation (N = 9; 56%), staff performance review (N = 4; 25%), faculty performance review (N = 3; 19%), and course credit for students (N = 2; 12%).

As with methods used for training and awareness, the most effective methods are not necessarily the most frequently used; note, however, that the number of responses to mandatory training and awareness is quite small so these results should be considered only as trend indicators. Following is a list of the effectiveness ratings for the mandatory security training methods: mandatory part of staff orientation (N = 3; 33%); mandatory part of faculty orientation (N = 3; 33%); mandatory part of staff performance review (N = 2; 50%); mandatory part of faculty performance review (N = 1; 33%); and mandatory part of student orientation (N = 2; 20%).

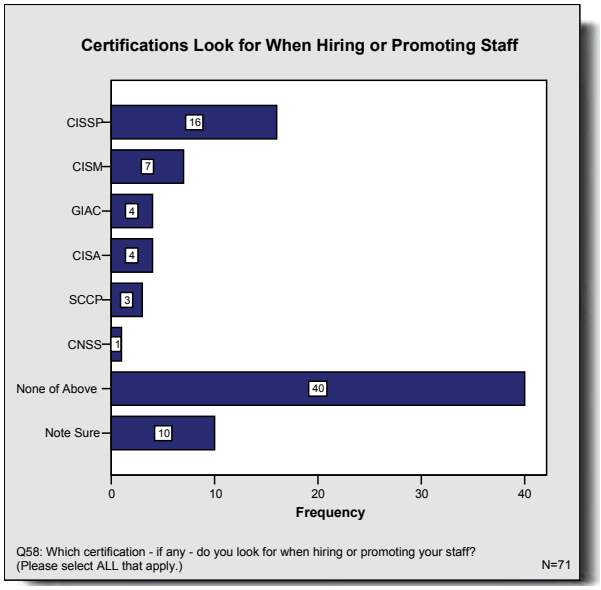
Exhibit 30. Mandatory Awareness and Training



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Certifications sought when hiring or promoting staff. When hiring or promoting staff, over half of the participants (N = 40; 56%) indicated that they do not seek any certifications when hiring or promoting staff. Almost one-quarter of the participants seek the CISSP certification (N = 16; 23%) over other accreditations such as the CISM (N = 7; 10%), GIAC (N = 4; 6%), CISA (N = 4; 6%), SCCP (N = 3; 4%), or CNSS (N = 1; 1%). Ten participants (14%) responded "not sure" to this question. This result may be because these certifications are not critical to success of newly hired or promoted staff or it may reflect the dearth of skilled professionals with these qualifications.

Exhibit 31. Certifications Sought When Hiring or Promoting Information Security Staff



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Practices

For purposes of this study, "practices" are defined as academic institutions' information security controls - that is, the safeguards or countermeasures - that protect the confidentiality, integrity, and availability of each institution's information and systems. These practices may involve management, operational, and procedural activities that span the entire institution or are specific to the IT Department's functioning. In this study, information security controls such as assessments and evaluations, patch management, contingency planning and incident response are considered as practices.

Assessments and Evaluations

As part of an effective information security program, institutions must periodically assess their information security controls and determine their effectiveness. They must also develop and implement plans of action to remediate ineffective controls and/or to reduce information and system vulnerabilities. This study addresses information security assessments and evaluations by considering assessments within the past 12 months, techniques used to evaluate information security, and methods to justify information security expenditures.

Assessments conducted within past 12 months. Participants in the study have conducted a variety of assessments over the past year. The most frequently cited were vulnerability assessments (N = 40; 56%) and audits (N = 37; 51%). Other assessments relatively widely used by participants included risk assessments (N = 28; 39%), penetration testing (N = 26; 36%), and application-level testing (N = 24; 33%). Information asset classification, surprisingly, was the least frequently used assessment (N = 18; 25%), and eight participants (11%) have used none of the above assessments within the past 12 months.

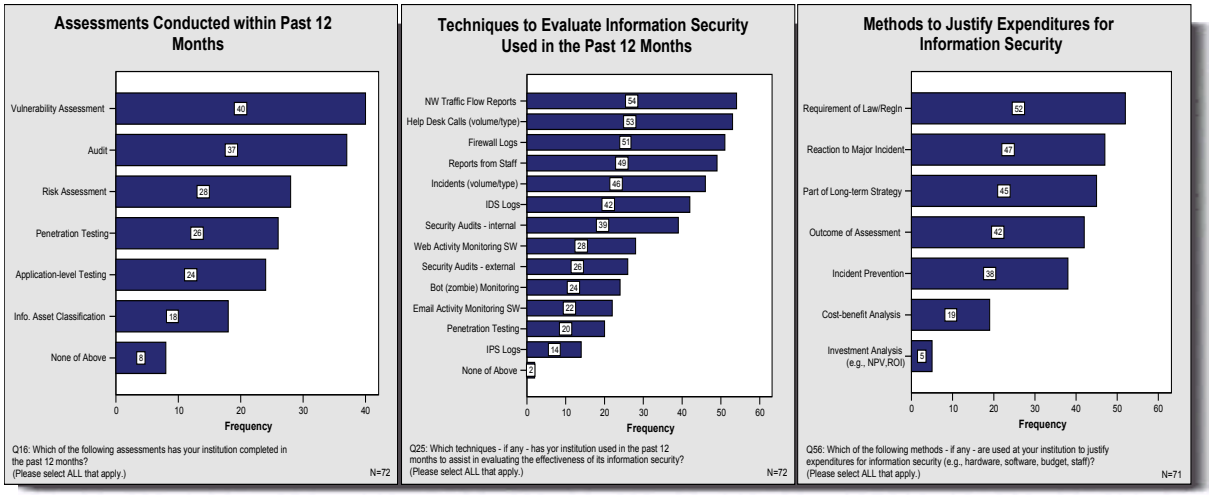
Techniques used in past 12 months to evaluate information security. Participating institutions have also used a range of techniques to evaluate information security in the past year. The seven most frequently used techniques included network traffic flow reports (N = 54; 75%), help desk calls – both

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

volume and type (N = 53; 74%), firewall logs (N = 51; 71%), reports from staff (N = 49; 68%), incidents – both volume and type (N = 46; 64%), intrusion detection system logs (N = 42; 58%), and internal security audits (N = 39; 54%). Other techniques used within the past 12 months included web activity monitoring software (N = 28; 39%), external security audits (N = 26; 36%), bot (zombie) monitoring (N = 24; 33%), email activity monitoring software (N = 22; 31%), penetration testing (N = 20; 28%), and intrusion prevention logs (N = 14; 19%). Two participants (3%) have used none of the above techniques in the past 12 months.

Methods to justify expenditures for information security. Participants also used a variety of methods to justify expenditures for information security. The two most frequently used methods to justify expenditures for information security (e.g., hardware, software, budget, staff) included requirement of law or regulation (N = 52; 73%) and reaction to major incident (N = 47; 66%). Other methods used to justify expenditures included part of long-term strategy (N = 45; 63%), outcome of assessment (N = 42; 59%), incident prevention (N = 38; 54%), cost-benefit analysis (N = 19; 27%), and investment analysis (e.g., NPV, ROI) (N = 5; 7%).

Exhibit 32. Information Security Metrics



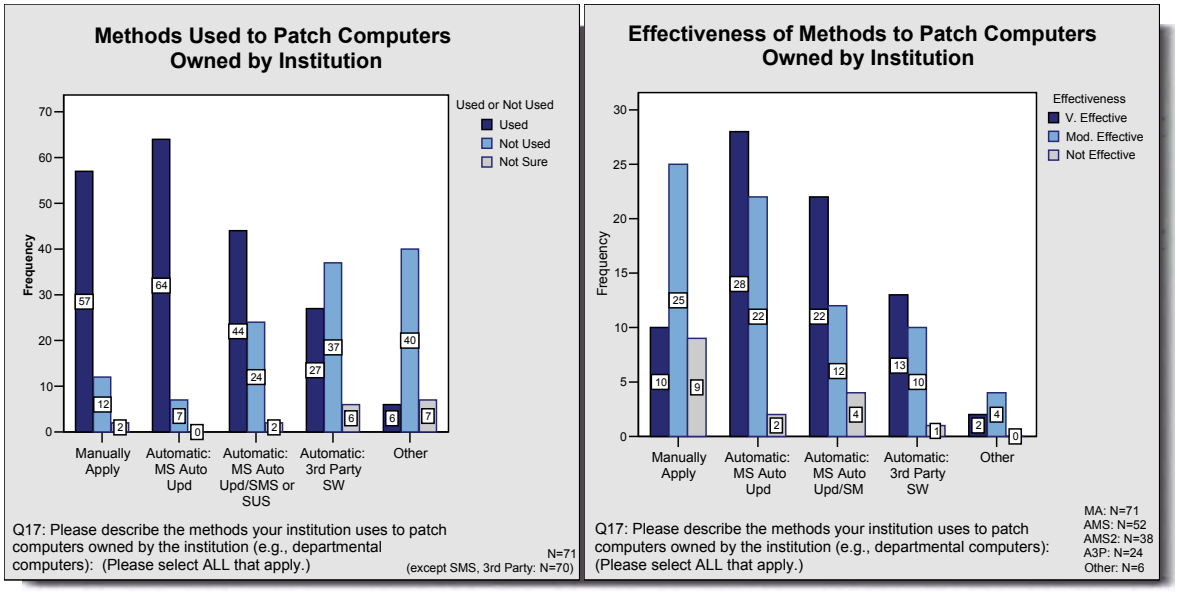
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Patch Management

Computers owned by the institution. Overall, most of the institutions that participated in the survey use at least one patch management method for computers owned by the institution. The most frequently cited method used to patch computers owned by the institution is MS AutoUpdate (N = 64; 90%), closely followed by manual application of patches (N = 57; 80%). Forty-four institutions (63%) use MS AutoUpdate-SMS or SUS. Twenty-seven institutions (39%) use automatic third party software, and six institutions (11%) use other methods of patch management.

Effectiveness of patch management methods for computers owned by the institution evidences a slightly different pattern than actual usage of methods. Specifically, the most frequently cited "very effective" method is MS AutoUpdate (N = 28; 54%), which does correspond with extent of usage. However, MS AutoUpdate-SMS or SUS is rated as the second-most effective (N = 22; 58%) and automatic third party software is rated as the third-most effective (N = 13; 54%); manual application, is rated as "very effective" by less than one-fourth of the institutions (N = 10; 23%).

Exhibit 33. Methods Used to Patch Computers Owned by Institution

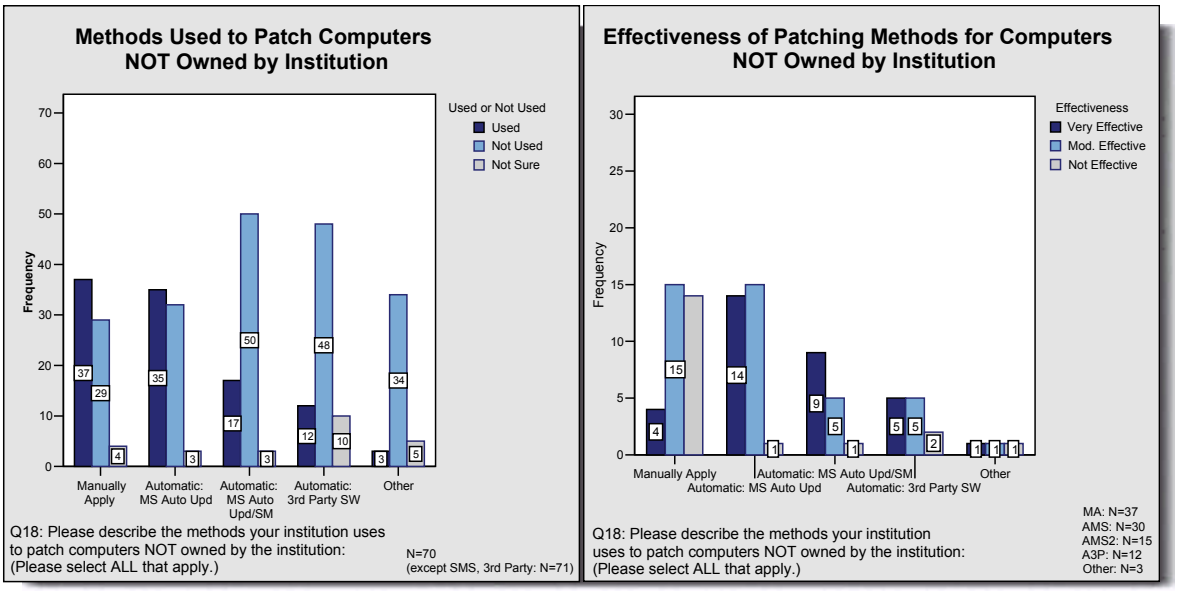


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Computers not owned by the institution. Results for patch management of computers not owned by the institutions are rather dissimilar from patch management of computers owned by the institutions. First, overall usage of patch management for computers not owned by the institutions is lower. Second, the most frequently cited method to patch computers not owned by the institutions is manual application (N = 37; 53%), followed very closely by MS AutoUpdate (N = 35; 50%). AutoUpdate-SMS or SUS is used by seventeen institutions (24%), automatic third party software is used by thirteen institutions (18%), and other methods of patch management are used by three institutions (7%).

Despite the differences in usage of methods for patching computers owned by the institution versus computers not owned by the institution, effectiveness ratings are quite similar. Specifically, the most frequently cited "very effective" method is MS AutoUpdate (N = 14; 47 %), followed by MS AutoUpdate-SMS or SUS (N = 9; 56%), automatic third party software (N = 5; 42%), manual application (N = 4; 12%), and other (N = 1; 33%).

Exhibit 34. Methods Used to Patch Computers Owned by Institution

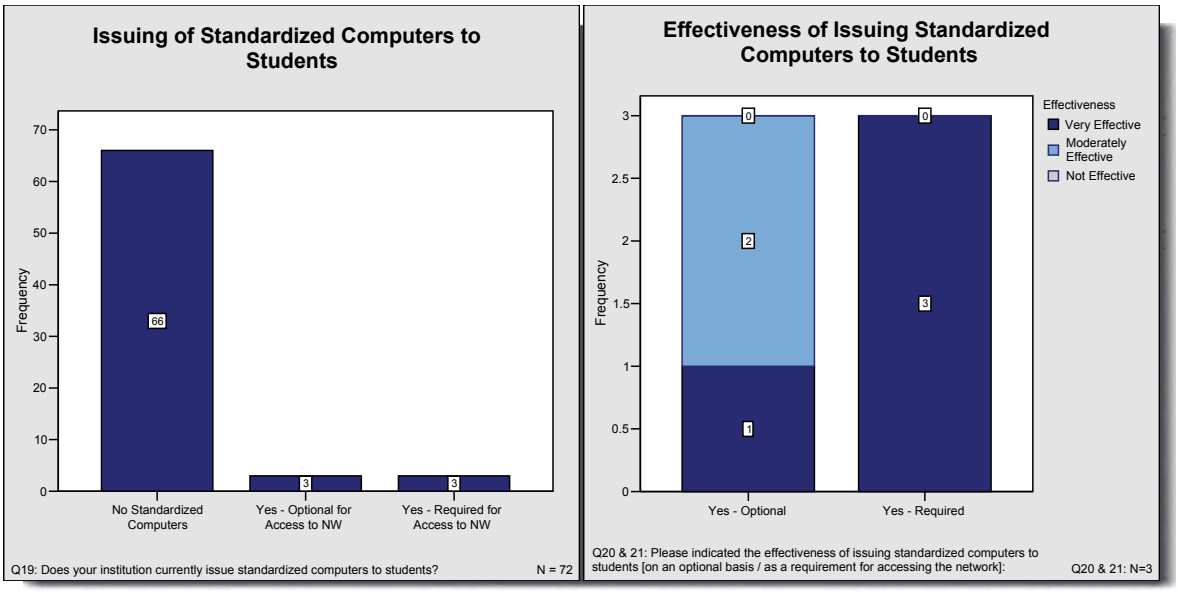


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Standardized Computers

Survey results for issuing of standardized computers to students provide some insight into the complexities faced by information security professionals in academic institutions. The majority of participating institutions (N = 66; 92%) do not issue standardized computers to students. Three institutions (4%) issue standardized computers to students on an optional basis, and three institutions (4%) issue standardized computers to students on a mandatory basis. Of the three institutions that issue standardized computers on an optional basis, one (33%) rated this practice as "very effective". Of the three institutions that issue standardized computers on a mandatory basis, all three (100%) rated this practice as "very effective".

Exhibit 35. Issuing of Standardized Computers



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Contingency Planning and Incident Response

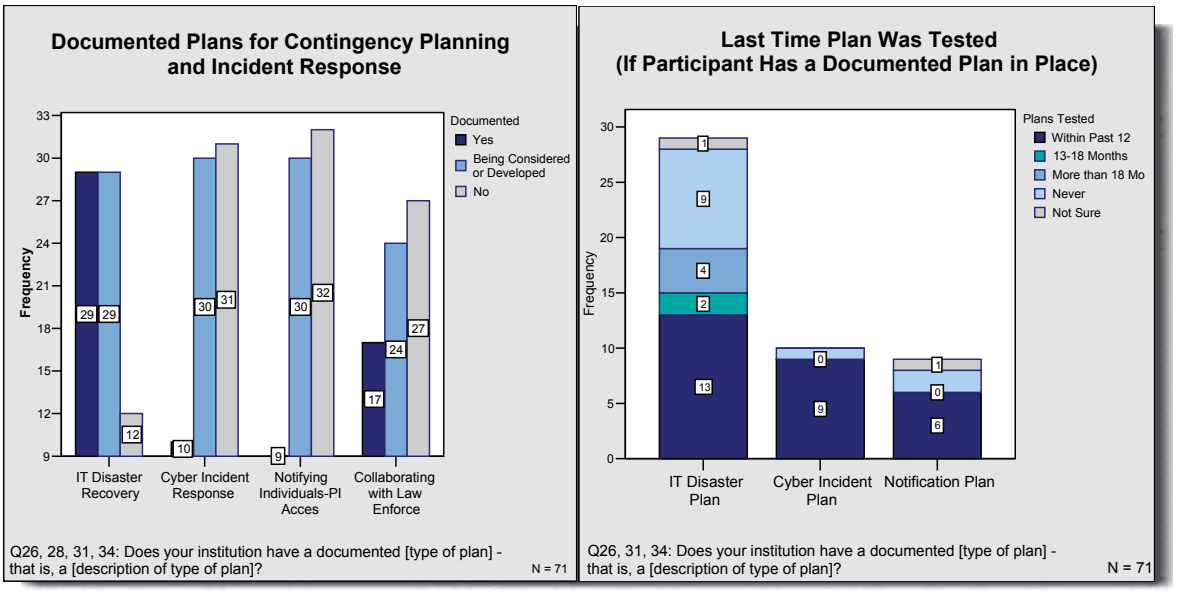
Contingency planning and incident response are critical to mitigating the impact of information security incidents. "Contingency planning" is intended to ensure the availability of critical information resources and continuity of operations in an emergency situation. It involves establishing, maintaining, and effectively implementing plans for emergency response, backup operations, and post-disaster recovery of information systems. "Disaster recovery plans" are considered as plans for supporting operations during and after an incident or disaster. Sources of incidents or disasters may be natural (e.g., flood, fire), human (e.g., malicious code, terrorist attack), or environmental (communications, power failure). "Incident response" involves establishing an operational incident handling capability, including adequate preparation, detection, analysis, containment, recovery, and user response activities. It also involves tracking, documenting, and reporting incidents to appropriate institutional officials and/or authorities.

Overall, participating institutions tend not to have documented contingency planning or incident response plans in place (see Exhibit 36 below). Less than half of the participants (N = 29; 41%) have a documented IT disaster recovery plan in place, and less than one quarter of the participants have a documented cyberincident plan (N = 10; 14%) or a documented plan for notifying individuals about private information access (N = 9; 13%). However, many participants are currently considering or developing documented contingency plans or incident response plans. Nearly half of the participants are considering or developing a documented IT disaster recovery plan (N = 29; 41%), documented cyberincident response plan (N = 30; 42%), and documented plan for notifying individuals about access to private information (N = 30; 42%). Of note is that almost one-quarter of participants (N = 17; 24%) already have a documented plan for collaborating with law enforcement and almost one-third (N = 24; 34%) are considering or developing a documented plan for collaborating with law enforcement.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The last time participants tested their documented plans seems to vary by type of plan (refer to Exhibit 36, right-hand panel). For example, the majority of documented cyberincident and notification plans have been tested within the past twelve months (N = 9; 90% and N = 8; 73%, respectively). On the other hand, less than half of the participants have tested their documented IT disaster plans within the past twelve months (N = 12; 45%), less than one-twentieth have tested this plan between the past thirteen to 18 months or more ((N = 2; 0.7% and N = 4; 1%, respectively), and almost one-third of participants (N = 9; 31%) have never tested this plan. This difference in participants' testing of their documented plans may be related to the establishment of "Y2K" disaster plans for the new millennium. Also of note is the number of institutions that have implemented their cyberincident plan: eight participants (89%) have implemented their cyberincident plan within the past twelve months and one (11%) has implemented it within the past 13 – 18 months.

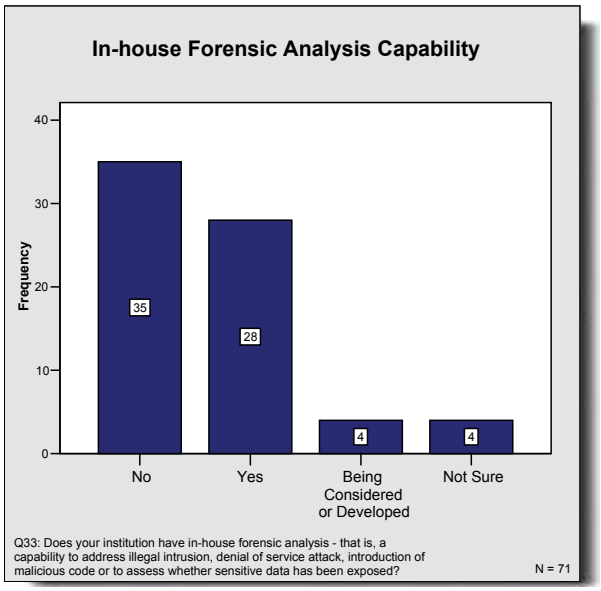
Exhibit 36. Documented Contingency Planning and Incident Response Plans



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Interestingly, a relatively large proportion of participating institutions have an in-house forensic analysis capability - that is, a capability to address illegal intrusion, denial of service attack, introduction of malicious code or to assess whether sensitive data has been exposed. Almost XX of participants currently have an in-house forensic analysis capability (N = 28; 39%) and four participants (6%) are considering or developing this capability.

Exhibit 37. In-house Forensic Analysis Capability

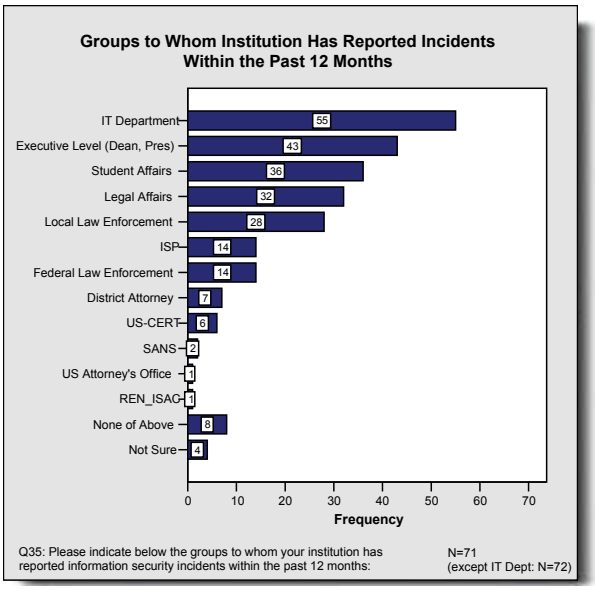


Groups to whom have reported incidents. Participants have reported information incidents to a variety of groups within the past 12 months. Most of these groups have been part of their own institution; for example, the four groups to whom participants have most frequently reported information security incidents within the past 12 months include their IT department (N = 55; 76%), the executive level (e.g., Dean, President; N = 43; 61%), Student affairs (N = 36; 51%), and Legal affairs (N = 32; 45%). Interestingly, twenty-eight of the participants (39%) reported incidents to local law enforcement within the past 12 months, while fourteen participants (20%) have reported information

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

security incidents to their Internet Service Provider. Some participants have reached out to federal law enforcement (N = 14; 20%), the District Attorney (N = 7; 10%), and U.S. Attorney's Office (N = 1; 1%). Disappointingly few institutions have reported information security incidents over the past 12 months to agencies such as REN-ISAC (N = 1; 1%), SANS (N = 2; 3%), and US-CERT (N = 6; 9%). Eight participants (11%) have not reported information security incidents to any of the aforementioned groups over the past 12 months, and four participants (6%) indicated they are "not sure" of groups to whom they have reported information security incidents over the past 12 months.

Exhibit 38. Groups to Whom Participants Report Information Security Incidents



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

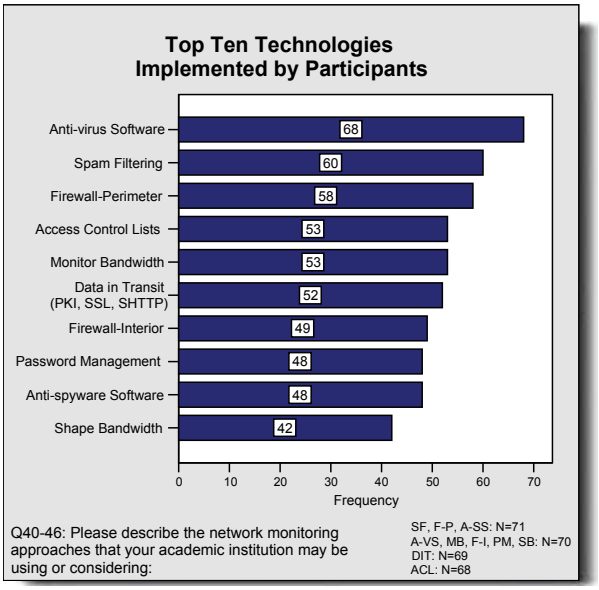
Technology

Institutions participating in this study indicated that they use a variety of technology solutions in securing their networks and information. Participants rated their use of technology solutions as "implemented", "in progress", "considering in twelve months", and "not considering". "Implemented" means the technology solution has been implemented across the entire institution or implemented in some areas with no plans for additional implementation in the future. "In Progress" means the technology solution is being implemented or has been implemented in some areas with plans for additional implementation in the future. "Considering in 12 months" means the technology solution is being considered for implementation in the upcoming twelve months, and "not considering" means the solution is not being considered for implementation.

Technologies Implemented by Participants

Summary of "Top Ten" Implemented Technologies. The ten technologies most frequently implemented by participants represent a mix of network monitoring, identity management, peer-to-peer, filtering and encryption technologies.

Exhibit 39. "Top Ten " Implemented Technologies



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

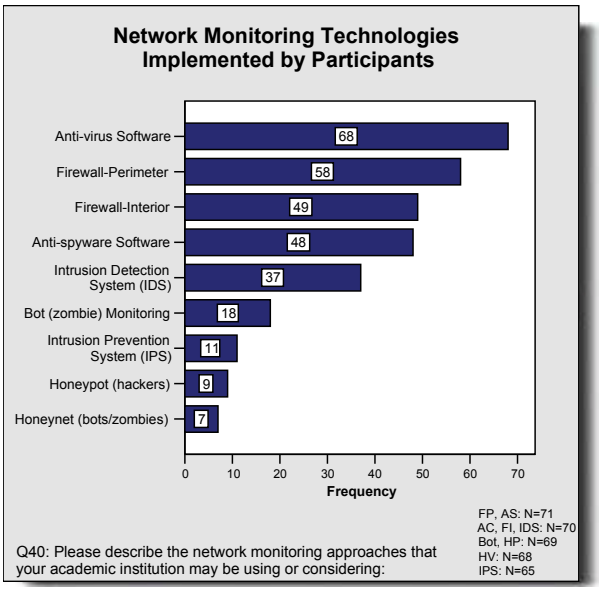
The three most frequently implemented technologies include anti-virus software (N = 68; 97%), spam filtering (N = 66; 85%), and perimeter firewalls (N = 58; 82%). Other "top ten" technologies include access control lists (N = 53; 78%), encryption for data in transit (e.g., PKI, SSL, SHTPP; N = 52; 75%), monitoring bandwidth for peer-to-peer (N = 53; 76%), interior firewalls (N = 49; 70%), anti-spyware software (N = 48; 69%), password management (N = 48; 69%), and shaping bandwidth (N = 42; 60%).

While understanding which technologies the participants have most frequently implemented (i.e., the "top ten" list) is useful, a more granular perspective of implemented technologies provides greater insight into participants' actual state of affairs. This information provides an understanding of participants' "baseline" of technologies they have implemented, and may be considered in conjunction with data regarding their technologies rated as "in progress or being piloted", "being considered", and "not being considered", all of which are provided in this section of the document. Accordingly, following is a summary of the technologies that have been implemented by participants, organized according to seven categories: network monitoring; identity management; peer-to-peer networking; filtering; wireless; encryption; and instant messaging.

Network monitoring. A variety of network monitoring techniques have been implemented by participants. The most commonly implemented techniques were anti-virus software (N = 68; 97%), firewalls at the perimeter (N = 58; 82%) and the interior (N = 49; 70%), anti-spyware (N = 48; 68%) and intrusion detection systems (N = 37; 53%). Other implemented technologies include bot (zombie) monitoring (N = 18; 26%), intrusion prevention systems (N = 11; 17%), honeypots for hackers (N = 9; 13%) and honeynets for bots and zombies (N = 7; 10%).

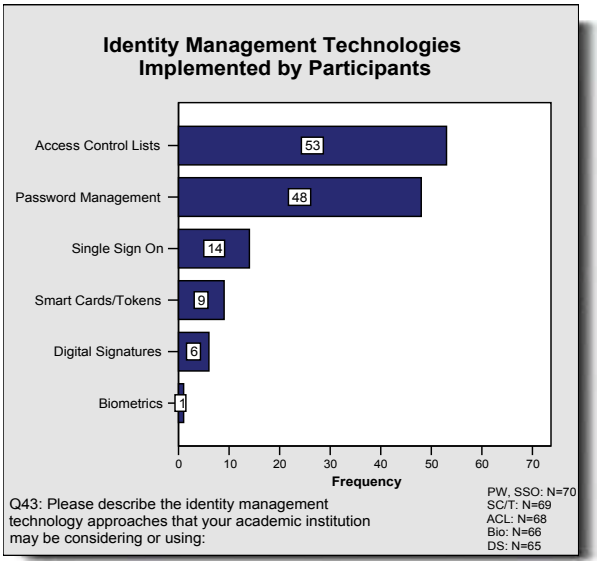
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Exhibit 40. Network Monitoring Technologies



Identity management. Identity management technologies most commonly implemented by participants include access control lists (N = 53; 78%) and password management (N = 48; 69%). Additional implementations include single sign on (N = 14; 20%), smart cards/tokens (N = 9; 13%), digital signatures (N = 6; 9%) and biometrics (N = 1; 2%).

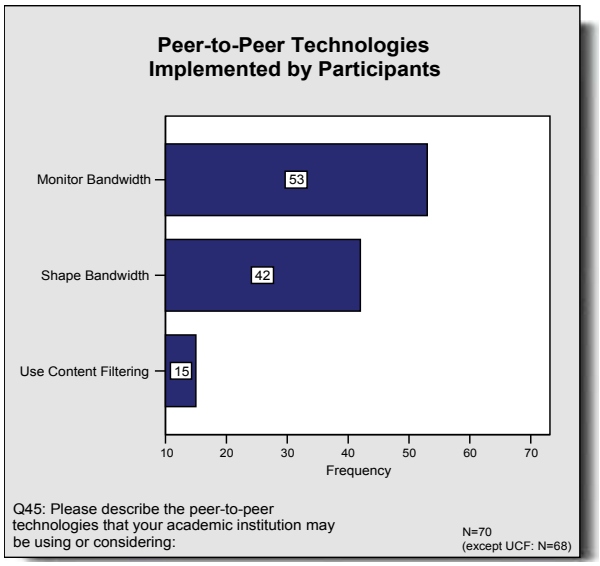
Exhibit 41. Identity Management Technologies



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

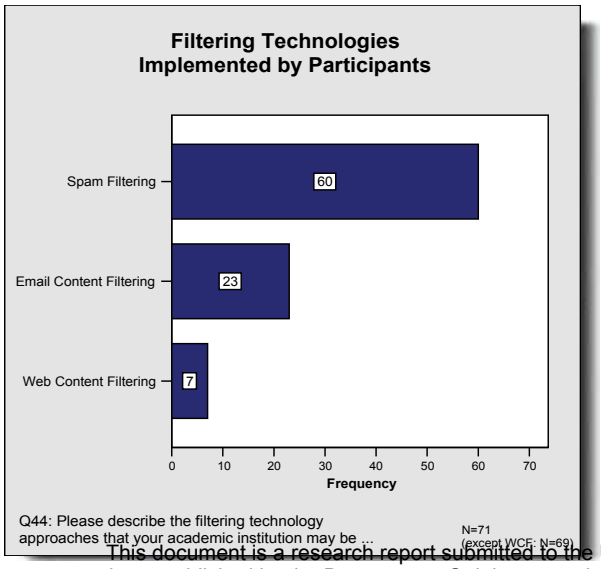
Peer-to-peer technologies and Filtering. Peer-to-peer technologies include monitoring (N = 53; 76%) and shaping (N = 42; 60%) bandwidth. Content filtering has been less implemented (N = 15; 22%).

Exhibit 42. Peer-to-peer Technologies



Filtering. The type and prevalence of filtering technologies implemented by participating institutions reflect academia's values of academic freedom and privacy. While sixty institutions (85%) have implemented spam filtering, twenty-three institutions (32%) have implemented email content filtering and just seven institutions (10%) have implemented web content filtering.

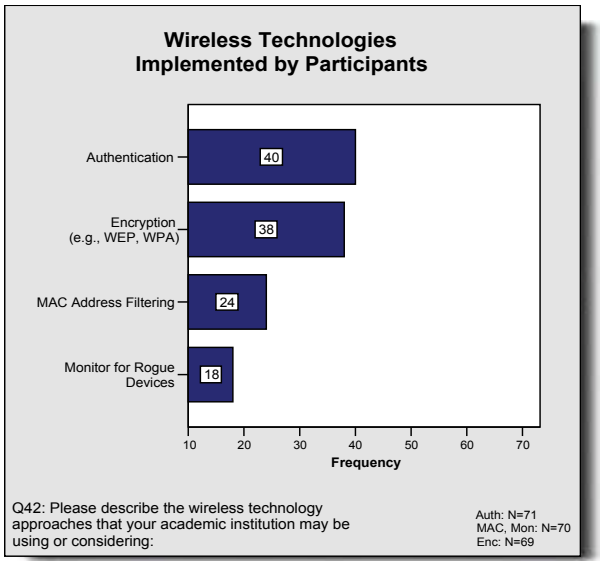
Exhibit 43. Filtering Technologies



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

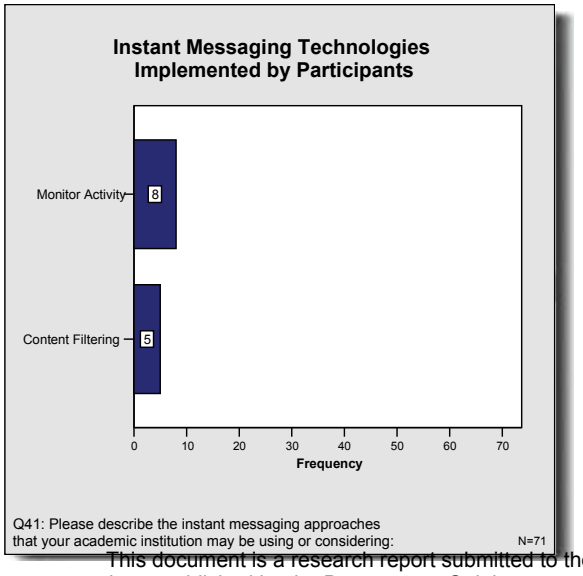
Wireless. Wireless technologies implemented most frequently include authentication (N = 40; 56%) and encryption (N = 38; 55%). Additionally, participating institutions have implemented MAC address filtering (N = 24; 34%) and monitoring for rogue devices (N = 18; 26%).

Exhibit 44. Wireless Technologies



Instant messaging. Instant messaging techniques have been implemented by few of the participating institutions. Eight institutions (11%) have implemented monitoring of activity and just five institutions (7%) have implemented content filtering of instant messaging activity.

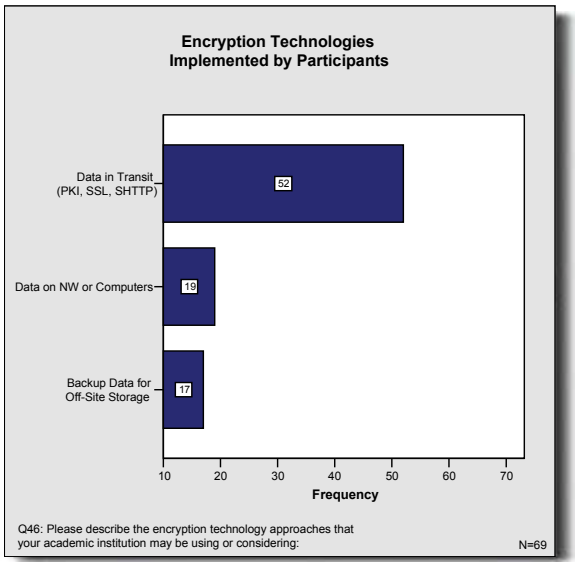
Exhibit 46. Instant Messaging Technologies



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Encryption. Encryption technologies implemented by participants vary widely. Technology for encryption of data in transit (e.g., PKI, SSL, SHTTP) has been implemented by over half the participants (N = 52; 75%). However, this implementation is much less for encryption for data on the network or computers (N = 19; 28%). Further, back up of data for off-site storage has been implanted by less than one-fifth of the participants (N = 17; 25%).

Exhibit 45. Encryption Technologies

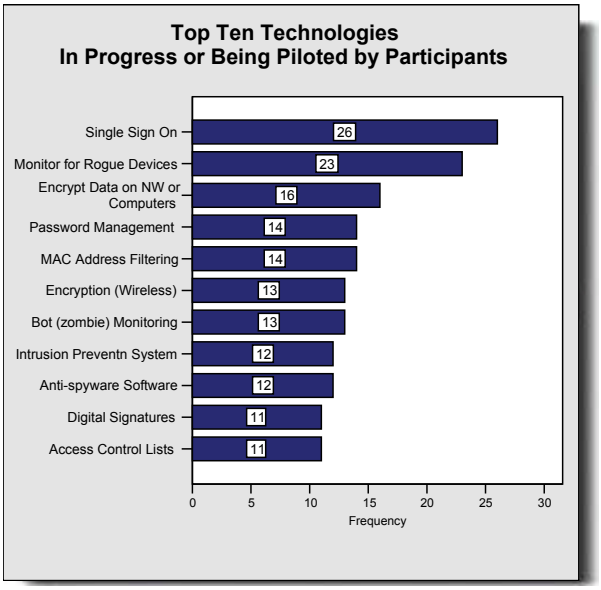


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Technologies in Progress or Being Piloted

The ten technologies most frequently cited by participants as "in progress" or "being piloted" relate to identity management, wireless access, network monitoring, and encryption (see Exhibit 47 below). The three most frequently cited technologies in progress or being piloted include single sign on (N = 26; 37%), monitoring for rogue wireless devices (N = 23; 33%), and encrypting data on the network or computers (N = 16; 23%). Other technologies cited as "in progress" or "being piloted" include password management (N = 14; 20%), MAC address filters for wireless access (N = 14; 20%), bot (zombie) monitoring (N = 13; 19%), encryption for wireless access (N = 13; 19%), intrusion prevention system (N = 12; 18%), anti-spyware software (N = 12; 17%), digital signatures (N = 11; 17%), and access control lists (N = 11; 16%).

Exhibit 47. Technologies in Progress or Being Piloted

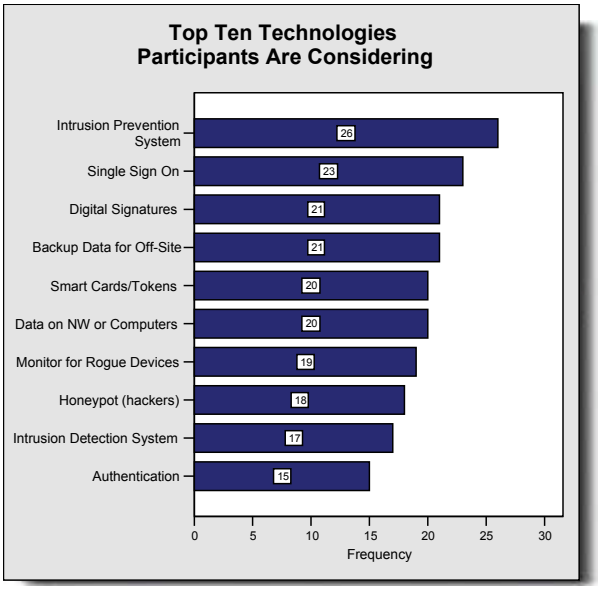


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Technologies Being Considered

The ten technologies that participants most frequently rated as "considering in the next twelve months" related to identity management, network monitoring, encryption, and wireless access (refer to Exhibit 48 below). The three technologies most frequently cited as being considered include intrusion prevention systems (N = 26; 40%), single sign on (N = 23; 33%), and digital signatures (N = 21; 32%). Other technologies that participants cited as "considering in the next twelve months" included encryption of backup data for off-site storage (N = 21; 30%) and data on network or computers (N = 20; 29%), smart cards/tokens (N = 20; 29%), monitoring for rogue wireless devices (N = 19; 27%), honeypots for hackers (N = 18; 26%), intrusion detection systems (N = 17; 24%), and authentication (N = 15; 21%).

Exhibit 48. Technologies Participants Are Considering

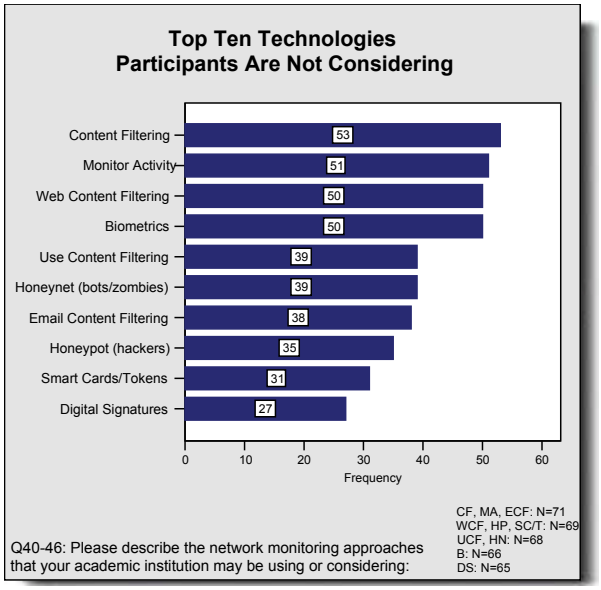


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Technologies Not Being Considered

The ten technologies that participants most frequently cited as "not considering" were related to filtering, identity management, instant messaging, and network monitoring (see Exhibit 49 below). These results reflect the cultural values of academic freedom and privacy as well as actual security needs. The technologies most frequently cited as not being considered include instant message content filtering (N = 53; 75%), monitoring instant messaging activity (N = 51; 72%), web content filtering (N = 50; 73%), and biometrics (N = 50; 73%). Other technologies that participants cited as "not considering" include peer-to-peer content filtering (N = 39; 57%), honeynets for bots and zombies (N = 39; 57%), email content filtering (N = 38; 54%), honeypots for hackers (N = 35; 51%), smart cards/tokens (N = 31; 45%), and digital signatures (N = 27; 42%).

Exhibit 49. Technologies Participants Are Not Considering



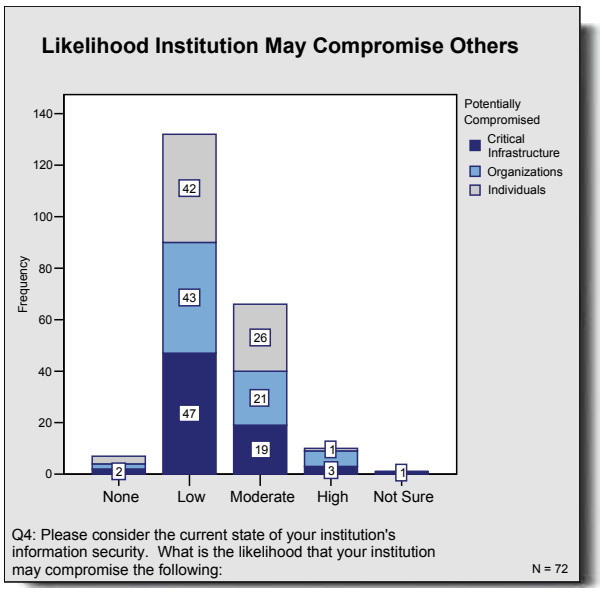
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Outcomes

In this study, outcomes are considered as results of the interaction between threats, vulnerabilities, consequences and control measures. The survey component of this study focused on three outcomes: likelihood the institution may compromise others, current preparedness for a major information security incident, and level of preparedness compared to two years ago. The network analysis component focused on outcomes as the actual inbound and outbound attack activities on participants' networks.

Likelihood institution may compromise others. Over one-half of the survey participants rated the likelihood that their institution may compromise individuals, other organizations, and critical infrastructure as "low" (N = 42; 19%%, N = 43; 20%, and N = 47; 22%, respectively). Almost one-third of the participants rated the likelihood that their institution may compromise individuals, organizations, and critical infrastructure as "moderate" (N = 26; 12%, N = 21; 10%, and N = 19; 9%, respectively). Just one-twentieth of participants rated the likelihood of compromise to individuals, organizations, and critical infrastructure as "high" (N = 1; 0.5%, N = 6; 3%, and N = 3; 1%, respectively). Interestingly, almost five percent of participants rated the likelihood that their institution may compromise individuals, organizations, and critical infrastructure as "none" (N = 3; 1%, N = 2; 1%, N = 2; 1%, respectively).

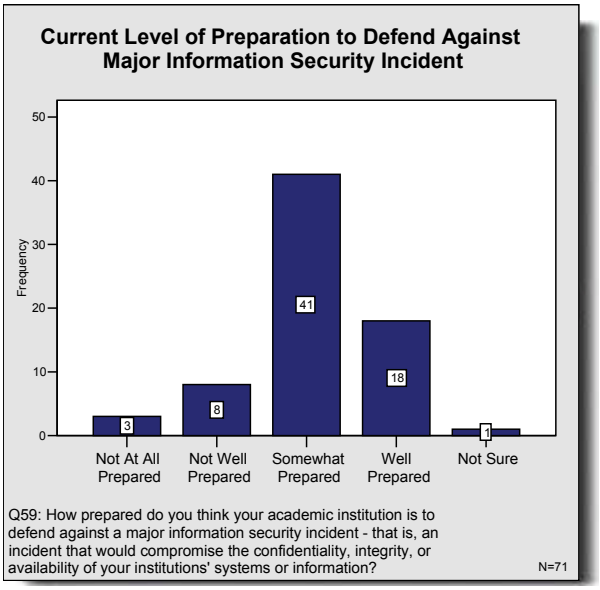
Exhibit 50. Likelihood Institution May Compromise Others



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Prepared for a major incident. Over three-fourths (82%) of the survey participants consider their institutions either "somewhat prepared" (N = 41; 57%) or "well prepared" (N = 18; 25%) to defend against a major information security incident – that is, an incident that would compromise the confidentiality, integrity, or availability of their institution's systems or information. Eight participants (11%) consider their institution "not well prepared" and three participants (4%) consider their institution "not at all prepared" to defend against a major information security incident. One participant (1%) indicated that he/she is "not sure" of the institution's preparedness to defend against a major information security incident.

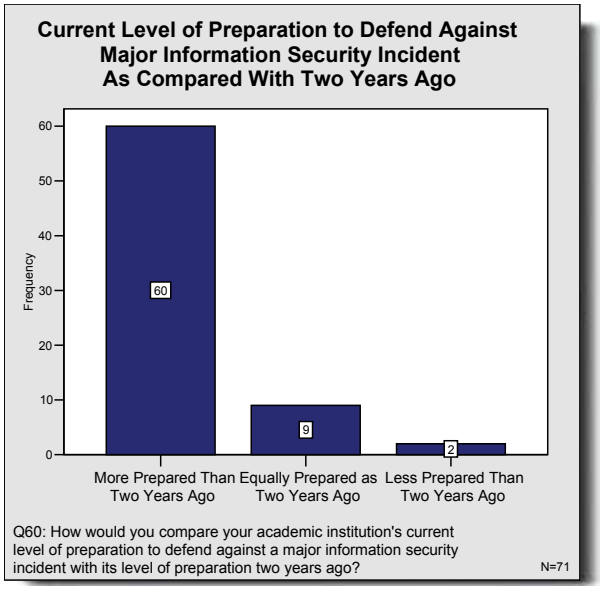
Exhibit 51. Current Preparation for a Major Information Security Incident



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Current level of preparation compared with two years ago. Over three-fourths of survey participants (N = 60; 83%) indicated that their institution is "more prepared than two years ago" to defend against a major information security incident. Nine participants (13%) indicated that their institution is "equally prepared as two years ago" and two participants (3%) indicated their institution is "less prepared than two years ago".

Exhibit 52. Preparation for Major Incident Compared with Two Years Ago



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Empirical Analysis of Network Activity

Network activity data from two academic institutions was collected for six months using the Higher Education Network Analysis (HENA) tool. Both inbound attacks (attacks on participants from other entities) and outbound attacks (attacks from participants on other entities) were tracked from January 1, 2006 to June 30, 2006. Data collected include type and protocol of attack, source and destination information, and geographic location. Note that, in the context of this report, "attacks" are defined as the incidents that are detected as violations of participants' firewall or intrusion detection/intrusion prevention rule sets. They reflect attempted rather than successful attacks, and do not reflect incidents that may have occurred and were not detected by the participants' network monitoring systems.

Number of attacks

Almost two million attacks (N = 1,827,481) were identified for the two participating institutions over the four months of data collection. The vast majority of these attacks (N = 1,752,367; 96%) were inbound; less than one-hundred thousand (N = 75,114; 4%) of these attacks were outbound.

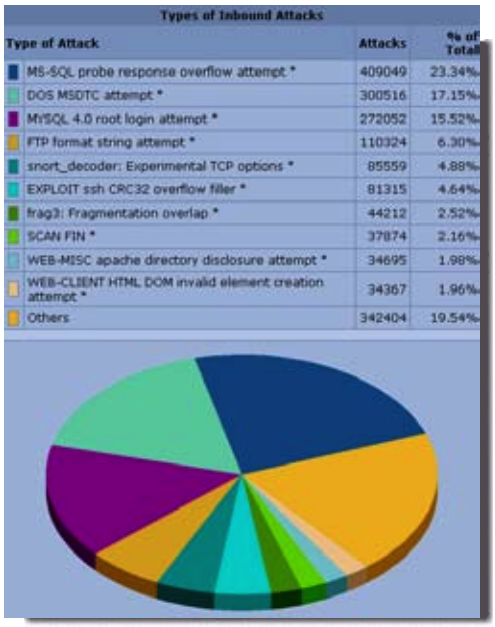
Types of attacks

A variety of attack types were employed for both inbound and outbound attacks. The following paragraphs characterize the types of inbound and outbound attacks and any relevant trends.

Inbound attacks. The types of inbound attacks (see Exhibit 53) reflect attempted database attacks, reconnaissance efforts, and Internet vandalism. The three most frequently identified types of attacks were *MS-SQL probe response overflow* (N = 409,049; 23%), *DOS MSDTC attempt* (N = 300,516; 17%, and *MYSQL 4.0 root login* (N = 272,052; 15%). These three most frequently identified inbound attacks, as well as other findings of note, are described in more detail in the subsequent paragraphs.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Exhibit 53. Types of Incoming Attacks



Types of Inbound Attacks		
Type of Attack	Attacks	% of Total
MS-SQL probe response overflow attempt *	409049	23.34%
DOS MSDTC attempt *	300516	17.15%
MySQL 4.0 root login attempt *	272052	15.52%
FTP format string attempt *	110324	6.30%
snort_decoder: Experimental TCP options *	85559	4.88%
EXPLOIT ssh CRC32 overflow filler *	81315	4.64%
frag3: Fragmentation overlap *	44212	2.52%
SCAN FIN *	37874	2.16%
WEB-MISC apache directory disclosure attempt *	34695	1.98%
WEB-CLIENT HTML DOM invalid element creation attempt *	34367	1.96%
Others	342404	19.54%

Attacks against database services represent over one-third of the inbound attacks. For example, *MS-SQL probe response overflow* may indicate Denial of Service (DoS) attempts, in which the attacker intended to stop the functioning of the participants' database services or to cease the operations of the participants' machines undergoing the attack. Another, potentially more serious class of this attack is a buffer overflow, in which the attacker was attempting to exploit the participants' database services to run arbitrary code and, possibly, to create "jump-off" points for other attacks. Password attacks, such as the *MYSQL 4.0 root login*, indicate the attacker believed (or hoped) the participants' targeted database servers had weak passwords. The attacker probably sought access to personally identifiable information/intellectual property or wished to modify existing data for some intent.

Reconnaissance attacks indicate that the attacker was looking for information about the structure and operation of the participants' web servers. *WEB-MISC apache directory disclosure* is an example of these attacks that could, in some cases, also lead to compromise of the system's integrity. The *Snort_decoder: Experimental TCP options* attacks could indicate that the attacker was trying to

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

determine whether a Snort network monitoring device was tracking and logging network activity, attempting to hide data in experimental TCP fields to avoid traffic capturing mechanisms, or simply trying out some experimental TCP options. *SCAN FIN* attempts indicate the attacker was gathering information about the participants' firewall rules, or possibly trying to get around the firewall.

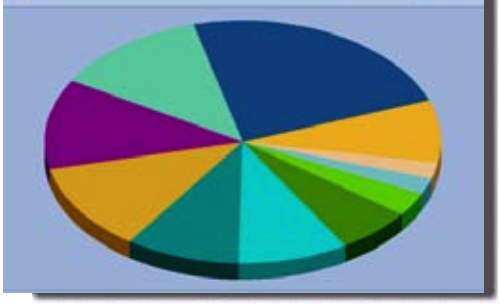
Several other types of attacks indicate further attempts to test the integrity of the participants' networks. *DOS MSDTC attempt* and *Frag3: Fragmentation overtap* were not intended to access data, but rather to bring down a particular machine or service, incur loss (i.e., data integrity, functionality, reputation, money), or practice hacking techniques. The *exploit ssh CRC32 overflow filler* is rather dangerous; if executed successfully it can lead to complete control of the machine.

Outbound attacks. The outbound attack types (see Exhibit 54 below) were related to denial of service attempts, reconnaissance efforts, and a Sober virus outbreak. The three most frequently identified types of outbound attacks were *http_inspect: BARE BYTE UNICODE ENCODING* (N = 14,903; 23%), *spp_rpc_decode: Incomplete RPC segment* (N = 7,970; 12%), and *spp_rpc_decode: Multiple Records in one packet* (N = 7,622; 12%).

Exhibit 54. Types of Outbound Attacks

Types of Outbound Attacks

Type of Attack	Attacks	% of Total
http_inspect: BARE BYTE UNICODE ENCODING *	14903	23.48%
spp_rpc_decode: Incomplete RPC segment *	7970	12.55%
spp_rpc_decode: Multiple Records in one packet *	7622	12.01%
http_inspect: DOUBLE DECODING ATTACK *	7466	11.76%
http_inspect: OVERSIZE REQUEST-URI DIRECTORY *	5934	9.35%
VIRUS OUTBOUND bad file attachment *	5697	8.97%
BAD-TRAFFIC IP Proto 103 PIM *	3920	6.17%
frag3: Fragmentation overlap *	1954	3.08%
ATTACK-RESPONSES Invalid URL *	1379	2.17%
http_inspect: IIS UNICODE CODEPOINT ENCODING *	1346	2.12%
Others	5292	8.34%



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Denial of service attacks indicate attempts emanating from (or through) the participating institutions' networks to bring down a specific target's computer. For example, the successful execution of *spp_rpc_decode: Incomplete RPC segment* would have been crashing the target machine due to memory exhaustion (the target would have been waiting for completion from each connection). Successful execution of the *spp_rpc_decode: Multiple records in one packet* attacks would have been similar to a buffer overflow attack.

Attacks on other organizations' web servers were also frequently identified outbound attacks. The *http_inspect: BARE BYTE UNICODE ENCODING* attempt is an attack on Microsoft's web server software. The *http_inspect: OVERSIZE REQUEST-URI DIRECTORY* attempt is not an attack against a specific web server, but against all associated servers.

Reconnaissance attacks indicate that an attacker (either within one of the participating institutions or using a participant's network as a "jumping off" point) was probing directory listings on the targets' machines. Examples of these attacks include *ATTACK-RESPONSES directory listing* and *ATTACK-RESPONSES id check returned userid*. The attempted *ATTACK RESPONSES – Invalid URL* may indicate a false positive (i.e., the end user mis-typed the URL of a page that does not exist) or reconnaissance efforts.

Protocol of attacks

Five protocols associated with inbound and outbound attacks were identified in the network analysis: Transmission Control Protocol (TCP); User Datagram Protocol (UDP); Internet Control Message Protocol (ICMP); Generic Routing Encapsulation (GRE); and Protocol-Independent Multicast (PIM). TCP enables two hosts to establish a connection and exchange data streams, guarantees data delivery, and ensures that packets are delivered in the order they were sent. UDP is a connectionless

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

protocol that, unlike TCP, provides very few error recovery services; it is used primarily for broadcasting messages over a network. ICMP supports packets containing error, control, and informational messages (e.g., ICMP echo requests, as used by the PING command). ICMP attacks (N = 15,806; .9%) indicate that the institution's edge router is sending back a message refusing to process the attempted attack. GRE is typically used for VPN connections.

Both inbound and outbound attacks primarily involved TCP protocol (N = 1,213,656; 72% and N = 55,775; 90% respectively). The UDP protocol was used in slightly over one-quarter of inbound attacks (N = 449,598; 27%) and less than five percent of outbound attacks (N = 2,019; 3%). The ICMP protocol attacks accounted for less than one percent of inbound attacks (N = 15,806; 0.9%) and just over one percent of outbound attacks (N = 659; 1%). Attacks using the GRE protocol were identified for no inbound attacks and one outbound attack (0.01%).

Exhibit 55. Protocol of Inbound and Outbound Attacks

Inbound Attacks per Protocol		
Protocol	Number	% of Total
TCP	1,213,656	72%
UDP	449,598	27%
ICMP	15,806	0.9%
PIM	947	0.1%
Outbound Attacks per Protocol		
Protocol	Number	% of Total
TCP	55,775	90%
PIM	3,720	9%
UDP	2,019	3%
ICMP	659	1%
GRE	1	0.1%

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Countries associated with attacks

Information about specific countries associated with attacks was obtained by IP address lookups using MaxMind location resolution services, which the research team integrated into the HENA tool. Two hundred and sixty (260) different countries were associated with attacks identified in the network analysis.

Inbound attacks. One hundred seventy three (173) countries were involved in inbound attacks on the participating institutions. The country most frequently associated with attacks on the two participating institutions was the United States (N = 647,770; 37%), followed by the Republic of Korea (N = 288,307; 16%) and China (N = 216, 738; 12%). The ten countries with the highest frequency of attacks on participants are listed in Exhibit 56 below:

Exhibit 56. Top 10 Countries Associated with Inbound Attacks

Who's Attacking Us – Top Ten Countries		
Country	Attacks	% of Total
United States	647,770	37%
Korea, Republic of	288,307	16%
China	216,738	12%
Netherlands	137,254	8%
Canada	76,043	4%
Taiwan, Province of China	53,376	3%
United Kingdom	42,737	2%
Germany	33,461	2%
Japan	25,497	1%
Sweden	24,809	1%

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Note that the frequency of attacks from the Netherlands is significantly skewed due to a one-day barrage on one of the institutions comprised of over 106,000 attacks originating from one IP address.

A pictorial illustration of the ten countries most frequently involved in inbound attacks on the two participants is provided in Exhibit 57 below:

Exhibit 57. Top 10 Countries Associated with Inbound Attacks

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Outbound attacks. Eighty-seven (87) different countries were involved in outbound attacks from the participating institutions. The country associated with the most frequent targets of the participants was the United States (N = 40,019; 63%), followed by Denmark (N = 6,551; 10%), and Malaysia (N = 4,152; 7%). The ten countries associated with the most frequently attacked targets are below:

Exhibit 58. Top 10 Countries Targeted in Outbound Attacks

Who We're Attacking – Top Ten Countries		
Country	Attacks	% of Total
United States	40,019	64%
Denmark	6,441	10%
Malaysia	4,152	7%
Germany	3,098	45%
Switzerland	1,317	2%
Unknown	1,287	2%
China	1,261	2%
United Kingdom	581	0.9%
Korea, Republic of	424	0.7%
France	414	0.7%

A pictorial illustration of the ten countries associated with the most frequent targeted attacks is provided below, in Exhibit 59.

Exhibit 59. Top 10 Countries Targeted in Outbound Attacks

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Top 10 Individual Inbound Attackers

The "Top 10 Individual Inbound Attackers" of institutions participating in the network analysis were defined by the IP addresses from which the ten most frequently identified inbound attacks originated. These Top 10 Individual Attackers accounted for over one-third of the inbound attacks (N = 653,572; 36%) over the four-month data collection period. Countries in which these top ten attackers were located included the Republic of Korea (N = 266,726; 16%), China (N = 233,615; 8%), United States (N = 87,187; 5%), Canada (N = 26,312; 2%), Taiwan (N = 22,656; 1%), and Sweden (N = 10,721; 0.6%). The actual origination point was not identifiable for seven of the ten top attackers, as their IP addresses traced back to Internet Service Providers (ISPs). However, three attacks that were identifiable originated from academic institutions. Specifically, these three attacks emanated from a university in Taiwan, and Education Center in Korea, and a private university located in the Southern United States.

Exhibit 60. Top 10 Individual Inbound Attackers

Top 10 Individual Inbound Attackers			
IP	Country	Attacks	% of Total
61.109.245.140	Korea, Republic of	258,787	15%
218.4.139.234	China	118,293	7%
87.210.66.109	Netherlands	106,355	6%
160.81.236.74	United States	76,113	4%
69.156.167.63	Canada	26,312	2%
163.13.158.113	Taiwan, Province of China	22,656	1%
60.213.54.117	China	15,322	0.9%
152.3.138.2	United States	11,074	0.7%
83.253.2.63	Sweden	10,721	0.6%
211.46.55.231	Korea, Republic of	7,939	0.5%

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Top 10 Individual Outbound Targets

The "Top 10 Individual Outbound Targets" are defined by the IP addresses for the ten most frequently identified targets of outbound attacks emanating from the participating institutions. These Top 10 Individual Targets accounted for almost one-third of the outbound attacks (N = 24,837; 33%) over the four-month data collection period. Countries in which top ten targets were located included United States (N = 11,206; 18%), Denmark (N = 6,408; 10%), Malaysia (N = 4,133; 7%) and Germany (N = 1,870; 3%). Over half of the top ten targeted IP addresses resolved to Internet Service Providers (ISPs) and therefore could not be identified. The four IP addresses resolving to specific targets indicated attack attempts on companies based in the U.S.

Exhibit 61. Top 10 Individual Outbound Targets

Top 10 Individual Outbound Targets			
IP	Country	Attacks	% of Total
83.90.144.3	Denmark	5,394	9%
218.111.18.4	Malaysia	4,133	7%
144.232.187.198	United States	3,720	6%
72.37.157.36	United States	2,851	45%
24.9.242.131	United States	2,313	4%
85.14.217.41	Germany	1,870	3%
80.219.125.74	Switzerland	1,220	2%
209.208.193.226	United States	1,168	2%
209.10.215.36	United States	1,154	2%
80.166.149.180	Denmark	1,014	2%

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Linking HENA Network Analysis Results to Action

Actions associated with participants' HENA network analysis results can be considered at several levels. The following pages describe examples of these actions, based on the data obtained in this study. Note that the information security professionals that have chosen to participate in the study have full discretion as to whether and how they would like to intervene; the researchers only provide suggestions for improving information security based on the empirical data.

At the aggregate level of analysis, the study's findings indicate several "quick and dirty" actions. First, the Top 10 Individual Inbound Attackers, which account for over one-third of the inbound attacks, should be blocked or dropped. Most of these IP addresses have been on the Top 10 list for a large duration of the study, with no attempts to terminate their attacks. Second, the Top 10 Individual Outbound Targets, which comprise almost one-third of the outbound attacks, should be notified that they are being targeted in attacks, and the information security professional should check IP addresses to identify which machine within the institution is perpetrating the attacks. Logs should be kept and, depending on the nature and severity of attacks, a forensic specialist or local law enforcement may wish to ensure any evidence is intact prior to approaching the individual.

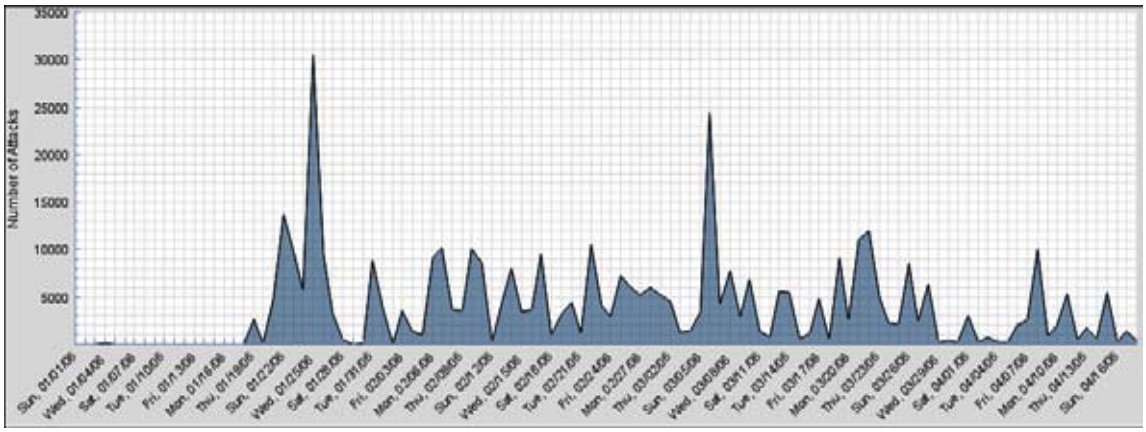
At the more detailed level of analysis, a number of actions should be taken to address specific threats. Note that their potential impact on information assets and systems should be prioritized so the limited time of the information security professional is not wasted. Many of the types of attacks have associated controls that are relatively easy to implement. When presenting data on types of attacks, the HENA tool provides a graphical representation of the duration and frequency of the attack as well as a link to descriptions of each attack available through Snort®, an open source network intrusion prevention and detection system using a rule-driven language that combines the signature, protocol and anomaly based inspection methods.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Example #1: MS-SQL probe response overflow attempt

The aggregate data indicates that this attack has occurred almost half a million times (N = 409,010; 24%) during the four months the data has been collected. Viewing more detailed information provided by HENA (see below), it is evident that these attacks have been occurring for almost three months and do not represent a sudden onslaught on the participants' networks.

Exhibit 62. HENA Output for Attack Example #1



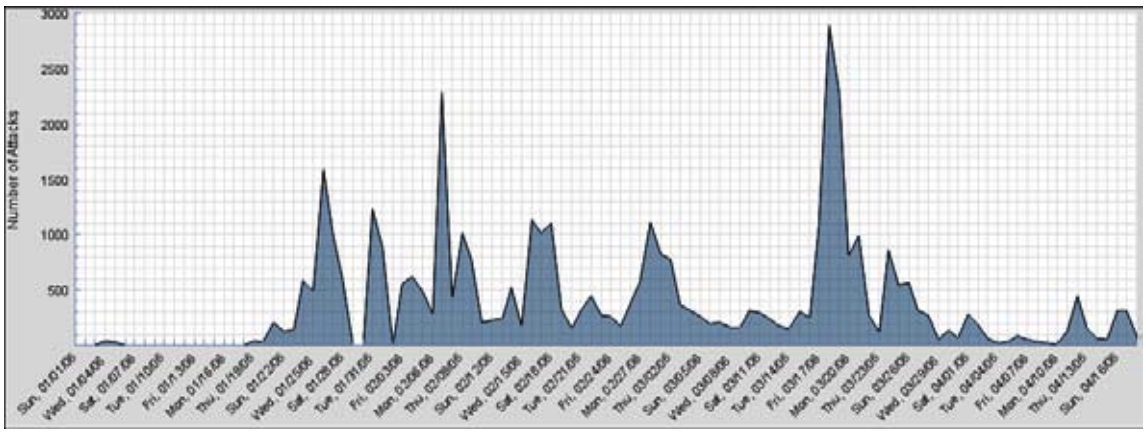
Clicking through to the description of the attack, its impact is rated as "Serious. Execution of arbitrary code is possible. Denial of Service (DoS)". Essentially, this attack occurs when the perpetrator is attempting to exploit a well-known vulnerability in Microsoft Windows Data Access Components. The attacker may spoof the response from an SQL server to exploit the vulnerability, execute arbitrary code and successfully complete a Denial of Service attack. Fortunately, this vulnerability is very easily remediated, as described in the attack definition. The information security professional can apply the appropriate vendor supplied patches and service packs, use a packet filtering firewall to block access to port 1434 for UDP traffic, or use IPsec to block incoming requests on UDP port 1434 on the SQL server.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Example #2: SCAN FIN Attack

The aggregate data indicates that this attack has occurred 37,874 times over the past several months, and represents 2% of incoming attacks. Viewing more detailed information about the attack (see below), one learns that it has been occurring on a somewhat steady basis for the past several months.

Exhibit 63. HENA Output for Attack Example #2



Clicking through to the description of the attack, one is informed that it is "intermediate" ease of implementation. Successful execution means that information regarding firewall rule sets, open/closed ports, ACLs, and possibly even OS type may be disclosed. This technique can also be used to bypass certain firewalls or traffic filtering/shaping devices. Essentially, this type of attack is used in reconnaissance, during which the perpetrator is gathering information leading up to another, more directed attack. Again, while having this type of ongoing attack with no remediation is not certainly optimal, several remediation steps exist. The information security professionals can determine if this particular port would have responded as being open or closed. If open, they would watch for more attacks on this particular service or from the remote machine that sent the packet. If closed, they would simply watch for more traffic from this host. It is strongly suggested that filtering this type of traffic at the ingress points of the network is considered.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The more detailed level of analysis also provides insights into potentially serious threats to the institution's information assets and associated systems, as well as public safety and security. The information security professional can skim through HENA's output to identify attacks of potential concern and then learn more about them as appropriate. While empirically tracking transnational criminal activity is not explicitly in this study's scope, a significant number of potential transnational criminals have probed the participants' networks. The table below presents examples of incidents obtained from one participant's log files on a Sunday evening:

Exhibit 64. Log Files From a Sunday Evening

Incident	Source	Example of Output
An attempt from China to access a Trojan program	An account in Beijing, China – CNCGROUP Heilongjiang province network.	[1:2182:8] BACKDOOR typot trojan traffic [Classification: A Network Trojan was detected] [Priority: 1] 01/04-21:11:31.055317 218.9.29.154 :2237 -> 128.***.**.***:20295 TCP
An attempt from Canada to exploit a Microsoft database in the university	An account in Halifax, Canada – Andara High Speed Internet c/o Halifax Cablevision LTC	[1:2329:6] MS-SQL probe response overflow attempt [Classification: Attempted User Privilege Gain] [Priority: 1] 01/04-21:13:20.447244 24.222.143.144:61858 -> 128.***.*.***:62088 UDP
An attempt from Vietnam to exploit a buffer overflow in the popular sendmail mail server	An account in Hanoi, Vietnam -- Vietnam Posts and Telecommunications Corp (VNPT)	[1:2183:6] SMTP Content-Transfer-Encoding overflow attempt[Classification: Attempted Administrator Privilege Gain] [Priority: 1] 01/04-19:18:45.496708 22.255.121.142: 1652 -> 128.***.*.**:25 TCP
Multiple attempts from Korea to gain access to university's system. Probably following a buffer overflow attack	An account in Seoul, Korea - Network Management Center	[1:1390:5] SHELLCODE x86 inc ebx NOOP [Classification: Executable code was detected] [Priority: 1]01/04-17:54:28.412981 222.122.74.26:23601 -> 128.***.**.***:4397TCP
An attempt *from* a university in the Northeast to hack *into* a Russian Website	An account within University X	[1:2436:5] WEB-CLIENT Microsoft wmf metafile access Classification: Attempted User Privilege Gain] [Priority: 1] 01/04-17:38:53.524107 128.***.***.***:2936 -> 81.9.5.9:80TCP

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The results of this study's network analysis, accomplished using the Higher Education Network Analysis (HENA) tool developed in this study, represent the first attempt to empirically assess actual network activity in academic institutions. The importance of using a measurement technique such as HENA to identify individual institutions' potential vulnerabilities and threats, as well as to characterize these vulnerabilities and threats for academia as a sector, is addressed in the Discussion section of this document.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

DISCUSSION

This study represents one of the first empirical assessments of the impact of information security in academic institutions on public safety and security. As illicit activity via the Internet accelerates and perpetrators move from better-protected private and government entities to softer targets, academic institutions face a barrage of attacks (e.g., data theft, malicious software infections, compromise of network services, infiltration of other entities). Adverse impacts of information security incidents include compromised private data and intellectual property, substantial financial losses, and potential threats to critical infrastructure, public safety and national security.

To address these issues, an empirical assessment of information security in academic institutions was conducted using a combination of survey, interview, and network analysis research methods. Based on these findings, a data-based profile of information security in academic institutions was created and a roadmap of recommendations for policy and practice has been developed. This section of the document describes the recommended roadmap for improving information security, addresses the contributions and limitations of this study, and explores ideas for future research.

Roadmap for Improving Information Security in Academic Institutions

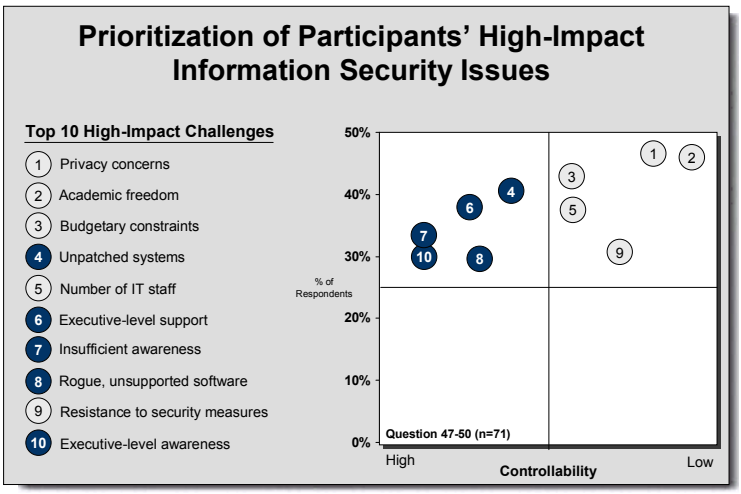
A number of data-based and focused approaches to improving information security in academic institutions can be derived from this study's findings. These approaches may be considered as a "roadmap", or set of activities designed to reduce the incidence and impact of information security incidents in academic institutions. This roadmap highlights critical issues, prioritizes improvement opportunities, lists effective and ineffective approaches, and provides a means to evaluate and balance the costs of security with the value of assets protected. It is designed to leverage participants' strengths and remediate their weaknesses in a proactive, integrated, multi-faceted way.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Participants in this study have a number of strengths to leverage, particularly the dedication of their information security professionals, use of techniques to evaluate information security, collaborative relationships with a variety of parties for addressing cyberincidents, and the range of technologies implemented for network monitoring, identity management, and peer-to-peer networks.

Participants face several challenges in maintaining information security at their institutions. A prioritized approach to addressing these challenges is recommended (see Exhibit 65 below), since some issues can be readily addressed and others involve long-term efforts for improvement. For example, awareness of the ramifications of information security incidents can be changed; the underlying values of academic freedom and privacy are more difficult to modify. The participants' high-impact challenges that are also controllable revolve around improving existing practices, boosting awareness, and tightening information security policies. Fortunately, these three challenges are inter-related, so improvement in one area will facilitate improvement in the others.

Exhibit 65. Participants' Information Security Issues



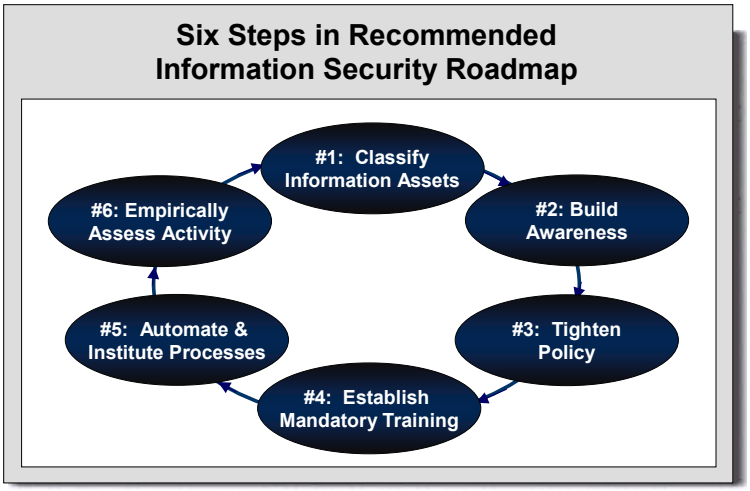
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The information security roadmap focuses on challenges that are high-impact and under the control of information security professionals. It provides practical recommendations, based on findings of this study and other relevant research, to enhance information security in academic institutions. The roadmap (see Exhibit 66 below) is based on a risk management approach, which ensures the institution's most critical information assets and associated systems are adequately protected. This approach maximizes both resource allocation and protection of information assets and systems. Six inter-related steps are recommended for participants in achieving a baseline level of information security:

1. Locate and classify information assets;
2. Build awareness;
3. Tighten security policy;
4. Establish mandatory training;
5. Automate and institute processes; and
6. Empirically assess activity.

Each of these steps is described in the following pages.

Exhibit 66. Information Security Roadmap



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Recommendation #1: Classify Information Assets

Asset classification involves locating information assets and their associated systems, then classsifying them as high, moderate, or low impact with respect to the impact of maintaining their confidentiality, integrity, and availability. This step is important in the academic setting, where resources are limited and valuable data and systems may be scattered throughout multiple departments, campuses, states, and even countries. Asset classification helps the information security professional focus resources and ensure the institution's most critical information assets and systems have adequate protection.

Locating and classifying information assets and associated systems may be an overwhelming task in academia's decentralized environment, and this study's findings indicate it is often overlooked. For example, survey participants completed a variety of assessments (e.g., vulnerability assessment, penetration testing) in the past 12 months, and almost half stated they had completed a risk assessment. However, only one-quarter of participants in the survey completed an information classification within the past 12 months.

Actions. Classifying information assets and associated systems involves three steps:

1. Locate and identify information assets and associated systems;
2. Classify their impact as high, moderate, or low with regard to maintaining confidentiality, integrity, and availability (see Exhibit 67 below);
3. Document these assets to build senior administration's awareness and to identify appropriate information security controls.

Outcomes. Outcomes of adopting a risk management approach include: 1) information assets and their associated systems are located and identified; 2) an initial classification of these assets has been completed; and 3) the first cut at an information asset database has been created.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Tip#1. Results of the asset classification – particularly when documented as an asset database - can be used to build awareness and buy-in with senior administration. When the institution's senior administrators can clearly understand the locations and value of their information assets and associated systems, they are far more likely to provide support and resources such as funding and staff.

Tip #2. Leverage the plethora of high-quality, free information about classifying information assets. For example, NIST (www.nist.org) and EDUCAUSE (www.educause.edu/security) provide excellent, free resources for information asset classification.

Tip #3. This process can be iterative. For example, an initial sweep will identify assets across campus and will help build senior administration's awareness. This awareness can be channeled to encourage cooperation from individuals across the campus for a more detailed assessment. These results can, in turn, further build senior administration's buy-in and support.

Exhibit 67. Framework for Information Asset Classification

Classifying Information Assets

	Confidentiality	Integrity	Availability
Low	The loss of confidentiality could be expected to have a limited adverse effect on operations, assets, or individuals.	The loss of integrity could be expected to have a limited adverse effect on operations, assets, or individuals.	The loss of availability could be expected to have a limited adverse effect on operations, assets, or individuals.
Moderate	The loss of confidentiality could be expected to have a serious adverse effect on operations, assets, or individuals.	The loss of integrity could be expected to have a serious adverse effect on operations, assets, or individuals.	The loss of availability could be expected to have a serious adverse effect on operations, assets, or individuals.
High	The loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.	The loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.	The loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets, or individuals.

Source: NIST FIPS Publication 199

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Recommendation #2: Build Awareness

Information security is relevant to the institution's diverse end users – including faculty, students, staff, affiliates *and* senior administration – for different reasons. However, the overarching goal of building awareness for all of these end users is simply that (a) they are aware of how they may affect information security and (b) they know how to respond if they suspect an incident.

Building awareness of information security can be a difficult activity in the academic environment with high student turnover, both full-time and part-time end users, multiple campuses, and a range of access methods. This study's findings confirm end users' lack of priority for information security: roughly two-thirds of senior administration and administrative staff and just one-third of faculty and students currently consider information security as within their top ten priorities. Further, four of the respondents' top ten high-impact challenges concerned issues such as senior administration's support of initiatives and awareness of issues, end users' resistance to security measures, and insufficient awareness of information security issues.

Actions. Building awareness involves four steps:

1. Obtain senior administration's support by educating them on key issues and ramifications;
2. Ensure faculty understands the integrity of their research and reputation may be on the line;
3. Collaborate with staff to ensure how their roles may impact information security is addressed;
4. Teach students simple methods to improve infosecurity and provide outlets for experimentation.

Outcomes. Outcomes of building awareness include: 1) increasing senior-level support and securing an appointed champion (if not full-time staff member) for information security; 2) increasing faculty awareness of the potential benefits to securing their research and data and thereby, hopefully, reducing their resistance to security measures; 3) further improving staff awareness and practices; and 4) increasing students' understanding of ramifications of their actions for the entire campus's security.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Tip#1. Setting up a quarantined network for faculty and students is an excellent way for end users to conduct their research, information sharing, and experimentation activities without compromising the institution's networks. It may also help shift the culture as end users recognize that information security and academic freedom are not mutually exclusive objectives.

Tip #2. Use a robust, defensible standard that ties into awareness-building efforts. This will enhance credibility and establish a shared language between end users and the information security professional. Two practical, easy-to-understand, and very robust standards are NIST 800-53 and ISO17799 (see Exhibit 68 below). NIST 800-53, created in 2005 by the National Institute of Standards and Technology, is an emerging framework used within the federal government. It provides detailed guidelines for selecting and specifying security controls for information systems and is generally considered to be the cutting-edge approach to information security. ISO 17799 is a comprehensive set of controls comprising best practices in information security. This internationally recognized generic information security standard consists of ten discrete sections, each focusing upon a specific aspect of infosecurity. Additionally, EDUCAUSE provides a high-quality risk assessment framework developed specifically for the academic community (see www.educause.edu/security).

Exhibit 68. Two Recommended Frameworks for Building Awareness

Information Security Program

Links in the Security Chain:
Management, Operational, and Technical Controls

- ✓ Risk assessment
- ✓ Security planning
- ✓ Security policies and procedures
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Security awareness and training
- ✓ Physical security
- ✓ Personnel security
- ✓ Certification, accreditation, and security assessments
- ✓ Access control mechanisms
- ✓ Identification & authentication methods (biometrics, tokens, passwords)
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls & network security methods
- ✓ Intrusion detection systems
- ✓ Security configuration settings
- ✓ Anti-viral software
- ✓ Smart cards

Source: NIST FIPS 200

Ten Domains of
Information Security Code of Practice

". . . intended to provide a common basis for developing organizational security standards and effective security management practice."

- ✓ Security Policy
- ✓ Organizational Security
- ✓ Asset Classification and Control
- ✓ Personnel Security
- ✓ Physical and Environmental Security
- ✓ Communications & Operations Management
- ✓ Access Control
- ✓ Systems Development & Maintenance
- ✓ Business Continuity Management
- ✓ Auditing and Compliance

Source: ISO 17799

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Tip#3. Seek out each end user group's answer to WIIFM ("What's In It For Me?"). Senior administrators are ultimately responsible for information security at their institutions and need to provide support and sponsorship for success. The institution's reputation can be readily enhanced or tarnished by incidents and responses to incidents, so information security will increasingly be a source of competitive advantage – or disadvantage – for academic institutions. Senior administrators' support of a top-down approach can be enhanced when they are aware of the information assets and associated systems located across the campus (per Step 1: Classify Information Assets). Their sense of urgency can be augmented when they are informed of the the ramificiations of incidents involving these assets and associated systems. Faculty's information security-related concerns typically revolve around the integrity of their research and maintaining their reputation. Thus they need to be educated on the potentially deleterious effects of their lack of support before they will (with the facilitation of senior administration support, tighter policy and consequences, and mandatory training) modify their behavior. Once senior administration and faculty recognize the positive and negative impacts of information security on their primary goals, they will begin to support information security objectives. Once students recognize the senior administration and faculty's emphasis on these issues, understand consequences of violating the policy, and are provided with alternative outlets for their computing and networking activities, they will start to fall into line as well, and culture change will be initiated.

Tip #4. Use resources such as the EDUCAUSE Cybersecurity Resource Center, a replete library of academic institutions' training materials. Leverage resources from the government and private sectors.

Tip #5. Send relevant output from www.privacyrights.org, a website that lists organizations with compromised information, to senior administration to highlight the large proportion of academic institutions that are routinely hacked.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Recommendation #3: Tighten Policy

A straightforward, consistently enforced information security policy ensures end users are aware of – and act in accordance with – the institution's desired rules and practices. An policy that is realistic, enforceable, and measurable provides end users with a clear understanding of which activities they should and should not conduct. Consequences for violating this policy that are meaningul and consistently enforced provide incentive for end users' compliance. Tightening the policy is particularly effective in when implemented conjuntion with informing end users of of critical information assets and systems, boosting awareness of key issues, and conducting training on addressing these issues.

Developing, ratifying, distributing, and enforcing the information security policy is a complex task in the academic environment. Academia's unique characteristics (e.g., culture of openness and academic freedom, a variety of powerful stakeholders with divergent perspectics, long lead-time requirements for change, high end user turnover, varying views on appropriate disciplining for students, faculty, staff and senior administration) make tightening the information security policy particularly difficult. These complexities are reflected in this study's findings. For example, almost half of the survey participants reported a mixed use of formal and informal information security policy and less than one quarter have a formal policy in place. Roughly two-thirds of participating institutions have provided their end users with the information security policy within the past 12 months; further, less than half have required their end users' official agreement to the information security policy within the past 12 months. Additionally, while violations of the information security policy involve a range of internal and external consequences, over half of the participants indicated that consequences have been either inconsistent or there are no real consequence. Fortunately, remediation of these issues will significantly improve academic institutions' information security posture.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Actions. Four steps are involved in tightening the information security policy:

1. Develop and ratify the information security policy -- at senior administration level.
2. Obtain agreement on consequences for violating the information security policy (address consequences regarding both frequency and severity of violations)
3. Require *all* end users – faculty, senior administrators, staff, students, affiliates – to read *and agree to* the information security policy and its consequences *prior* to granting access to the network.
4. Obtain agreement from all enduser every semester *prior* to granting access to the network.

Outcomes. Outcomes of tightening the information security policy include: 1) the policy is agreed upon at the senior administrative level; 2) the policy is documented; 3) faculty, students, staff, affiliates *and* senior administration are provided with and agree to the policy and its consequences.

Tip #1: When developing and ratifying the policy, use best practice and templates whenever possible. Since obtaining agreement at the senior administration level may be the most difficult aspect of this step in the raodmap, using best practice examples and well-known templates will keep your policy defensible in the face of stakeholders' competing interests. Review the information security policies of other academic institutions as well as not-for-profit, government, and private sector organizations. Take advantage of knowledge and tools developed by experts in information security and academia. For example, EDUCAUSE has developed the Information Security Governance Assessment Tool, a free, high-quality self-assessment designed specifically for academic institutions (see www.educause.edu/security) and also provides very useful courses in policy development.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Tip #2. Once the policy has been ratified at the senior administration level, provide two weeks for input to the policy from all end user groups. Integrate this feedback as appropriate for the final policy, then provide a thank you and feedback to each contributor. If an end user's suggestion was not incorporated, include information about why the suggestion not incorporated. Obtaining input from all end users will help reduce the resistance that will inevitably occur when all end users are asked to sign agreement to the policy.

Tip #3. If this is the first time the institution has adopted a formal information security policy, use this to advantage. Acknowledge the issues to date – everyone is aware of them even if they have not been formally acknowledged. End users may be quite interested in providing input to a new policy; leverage this opportunity, as their involvement in the process will reduce overall resistance. Since this is a new initiative, use this situation to require *all* end users' agreement to the policy – even faculty and senior administration – as this will send a signal throughout the institution. This is an excellent opportunity to set good precedent. Note that senior administration's support is critical at this stage, so ensure buy-in has been sufficiently established.

Tip #4. Implement consequences of violating the information security policy fairly and consistently – otherwise the effect of all other efforts will be mitigated if not wasted.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Recommendation #4: Establish Mandatory Training

Mandatory training ensures that end users are aware of the security risks associated with their activities and they are sufficiently trained to carry out these activities without posing a threat to the institution's information security. Training end users in how to appropriately handle information and associated systems is critical to achieving results from other activities, such as boosting awareness, tightening policy, using institutionalized practices, and assessing outcomes. End users need to know which activities are appropriate and also *how* to conduct these activities.

Ensuring that end users are aware of – and sufficiently skilled to act upon – the desired behaviors is a difficult task in academic institutions. Challenges such as high end user turnover, diverse access methods, divergent computer usage goals, and high-risk activities are exacerbated by the culture of openness and experimentation. These issues are reflected in the survey results: almost ninety percent of participants do not require end users to attend mandatory awareness and training sessions before being granted access to the network. However, the eleven participants that do require mandatory awareness and training rate over ninety percent of these methods as either moderately or very effective. The implications of insufficient training ripple through the institution, as evidenced by participants' ranking of insufficient awareness and insufficient technical ability as four of the top ten high-impact challenges.

Actions: An efficient and effective mandatory training program involves five steps:

1. Identify baseline training requirements for all end users (e.g., basic network usage, simple secure practices installing and maintaining antivirus and antispymare software,) and obtain senior administration's buy-in to these training requirements.
2. Design a simple, short overview session for *all* end users (including faculty and senior administration) that is a requirement for accessing the network.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

3. Develop role-based training according to end users' activities and relationships to the institution's information assets and associated systems.
4. Develop a refresher/update course for end users that have completed the overview session; this should be required every semester for access to the network.
5. Ensure mandatory training is completed by *every* end user prior to accessing the network and that refresher/update training is completed every semester.

Outcomes. Outcomes of establishing mandatory training are: 1) end users know basic steps to improve information security; 2) end users know basic steps of what *not* to do regarding information security; 3) end users are aware of the consequences of compromising information security; 4) end users are aware of who to call if they suspect a compromise

Exhibit 69. Example of Student Residence Hall Training

USE OF STUDENT RESIDENCE HALL COMPUTING NETWORKS

Do:
- ✓ Comply with the Student Instructional Computing Responsible Use Code, Conduct Code, and other related college policies
- ✓ Accept responsibility for your content, including complying with federal and state laws
- ✓ Follow specified computing naming conventions to avoid network conflicts
- ✓ Be responsible for activities conducted to or from your network connection

Don't:
- ✗ Assign your computer a non-college-owned domain name
- ✗ Use your computer for commercial purposes
- ✗ Overload the network
- ✗ Conduct illegal activities

Consequences (in order of increasing severity):
- ⊗ Disconnection of your computer from the network
- ⊗ College disciplinary action
- ⊗ Criminal prosecution

Source: SANS Institute, 2002

Tip#1. The overview training should be mandatory for all end users, including senior administration, faculty, staff, students and affiliates. This investment of 15 minutes once per end user is critical to not just establishing a shared understanding of the institution's security needs but also to support the changing culture. Senior administration's buy-in and support, which should have been

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

achieved by this point, will be useful in obtaining additional resources if needed and overcoming resistance to the training. This overview should reinforce the information security policy and consequences for violating the policy.

Tip#2. Adhere to the KISS ("Keep It Simple Smartie") principle. Focus precisely on what is required to achieve and maintain the baseline level of information security. Use relevant examples and "war stories" to hilight key issues. Maximize outcomes by establishing a feedback mechanism for end users' suggestions to improve or simplify activities or the training. simplify or make easier for end users.

Tip#3. Do not reinvent the wheel. Numerous information security training resources have been developed, many of which are free. Review materials from leading institutions such as SANS, CERT, EDUCAUSE, and DISA. EDUCAUSE's recent cybersecurity awareness competition yielded a number of high-impact, free videos that appeal to students (see Exhibit 70 below). Other engaging electronic training options, such as Easyl, are developing apace and should be explored.

Exhibit 70. Screenshots from Free EDUCAUSE Training Videos

Tip#4. The first time the overview training course is designed and implemented will be overwhelming. However, once the IT staff become acclimated to administering the training and end users adjust to the requirements of mandatory training, it will become a routine process.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Recommendation #5: Automate and Institutionalize Processes

Information security processes that protect the confidentiality, integrity, and availability of the institution's information and systems may involve management, operational, and/or procedural actvities. Appropriately automated and institutionalized processes streamline key information security activities, define end users' required behavior, and address issues in a standardized and timely manner.

Automating and institutionalizing processes in academia can be very difficult. In the decentralized environment, processes may not be aligned at an institutional level because each academic and administrative department, division, or campus has developed its own processes over time. End users access the system via multiple access methods, often using their own computers, many of which are differently configured. This study's finding highlight the difficulty information security professionals encounter with regard to automated and institutionalized process. For example, patch management methods for computers owned by the institutions and not owned by the institutions varied markedly in extent of usage and effectiveness. Less than a quarter of survey participants have a documented cyberincident plan or plan for notifying individuals about private information access. Over ninety percent of participants do not issue standardized computers, yet all institutions that do so rate this practice as "very effective".

Actions. Four steps are involved in automating and institutionalizing processes:

1. Identify key processes for achieving the institution's desired baseline level of information security.
2. Inform senior administration of the issues and their repercussions and, using a collaborative process, develop a prioritized list of policies to automate/institutionalize with rough timeframes.
3. Identify required resources (e.g., financial, staffing, consulting, hardware, software) and sources of information, using best practice when possible.
4. Ensure ongoing communication and progress reporting to senior administration and end users.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Outcomes. Outcomes of the activities involved in automating and institutionalizing processes include: 1) a prioritized list of processes to be automated and/or institutionalized - which has support from senior administration; 2) targeted sources of information and best practice to maximize effectiveness and minimize extra work or re-work; 3) a roll-out plan based on prioritized the list and necessary resources (e.g., financial, staffing, hardware or software requirements). This includes a plan for regular progress reporting to senior administration.

Tip #1. Make sure the processes are layered to cover different aspects of IT infrastructure. For example, review virus update software and processes, intrusion detection or prevention systems, access control and identity management, audits, content filtering at gateway, server and desktop levels for closing bad sites, patch management, encryption of backup data, contingency planning, and incident response planning. Include PDAs, USBs, and mobile clients. For every analysis and solution, consider implications for the Internet, extranet, intranet, and internal mission-critical systems.

Tip #2. Leverage technology to automate PC cleaning and updates as much as possible. For example, Bradford Network's Campus Manager tracks computers using their media access control (MAC) address, then students who initiate connection within the institution's network are directed to a virtual LAN, where they can install appropriate software. Perfigo, Cisco, and Clean Access may be useful. The website www.patchmanagement.org is a very useful and free resource.

Tip #3. Consider quarantining students, faculty and staff from access to the campus network until they have installed (and updated) antivirus and antispyware software and updated their operating system patches. This standardized process is particularly effective when senior administration supports it and the policy has been tightened so end users have a clear understanding of consequences of their actions.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Tip #4. Document plans for disaster recovery and incident management. Use best practice and existing resources - many sources are excellent and free (e.g., NIST, EDUCAUSE). Using best-practice templates will maximize quality, minimize re-work, and provide defensible positions when discussing these plans with senior administration and other end users. Then tailor plans for the particular institution's needs based on outcomes of the information classification and a risk management approach.

Tip #5. Prepare for resistance! End users, particularly in the academic culture that tends to oppose security measures, will balk at changes in security that influence their daily behaviors. In communications with end users, point out that automating and institutionalizing processes will better protect their private data and intellectual property and will also reduce their time and effort once they adjust to the new activities. Standardizing and automating processes is an excellent way of achieving long-term as well as short-term gains when the information security professional is armed with a clear understanding the information assets and associated systems, strong executive support, a tight policy, and end users who are aware of key issues.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Recommendation #6: Empirically Assess Activity

Empirically assessing activity involves evaluating the institutions information security controls, processes, and outcomes to determine their effectiveness and methods for improvement. Empirical assessments that clearly indicate remediation actions for the controls, processes, or outcomes are particularly useful.

Given the variety of stakeholders, end users, access methods, computers, and networks, academic institutions often have the opportunity to integrate disparate assessments from across the decentralized structure to develop a holistic view of the institution. For example, survey participants have conducted a variety of assessments over the past year; the most frequently conducted were vulnerability assessments and audits. They have also used a range of techniques to evaluate their information security over the past year; the most frequently used were network traffic flow reports, help desk calls, firewall logs, reports from staff, and incidents. Similarly, methods to justify information security expenditures were also broadly used. The two most frequently cited methods were requirement of law or regulation and reaction to major incident. Additionally, the Higher Education Network Analysis (HENA) tool developed in this study provides clear direction for controls that can be modified, implemented, or removed to improve information security.

Actions. Five steps are involved in empirically assessing activity:

1. Prioritize the most important controls, processes, and measures to be assessed, based on asset classification, boosting awareness, tightened policy, and institutionalized practices.
2. Determine the gap between current and desired assessments.
3. Identify how to close the gaps by reviewing current policies and practices, comparing to targets, conducting peer benchmarking, and then developing a remediation plan.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

4. Follow up and compare metrics annually. Report outcomes of these comparisons to senior administration and end users.
5. Refine the process to achieve continuous improvement. The environment and institution are dynamic, so the controls, processes and outcomes must be continually re-evaluated.

Outcomes. Outcomes of empirically assessing activity include: 1) prioritized list of controls, processes and measures to be assessed; 2) plans for how to close the gaps between current and desired measurement activities; 3) an ongoing, meaningful, actionable assessment of activities and their impact on the institution's information security.

Tip #1. Focus on what is necessary - less is better. When selecting security metrics, ensure that they: a) yield quantifiable information; b) are readily obtainable; c) are part of a repeatable process; and d) are useful for tracking performance and directing resources. Examples of metrics with these characteristics include the number of security incidents over a given period, the percentage of data repositories with defined owners and classifications, and the percentage of systems that comply with the institution's password policies.

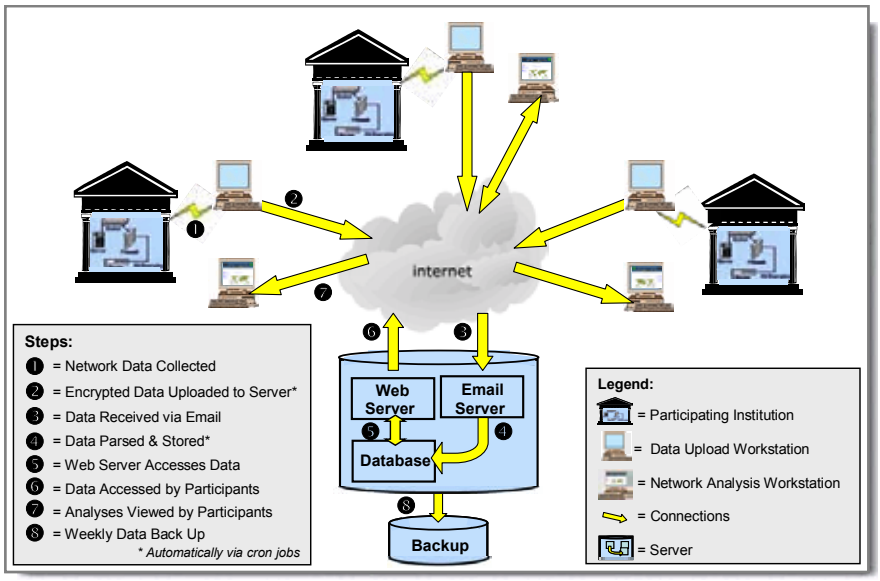
Tip #2. Get buy-in for the metrics from senior administration. This process will demonstrate the information security professional's concern for senior administrators' decision making and resource allocation procedures and will facilitate dealing with resistance from faculty, students, and staff.

Tip #3. All feedback from a well-conducted empirical assessment is useful. If initial results of the assessments are not good, clearly state the reasons and propose options for improving performance when meeting with senior administration. If initial results are good, highlight contributions from senior administration as well as the information security team, establish means to maintain good outcomes for these processes, and focus the next set of priorities.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Tip #4: Take advantage of the Higher Education Network Analysis (HENA) tool developed in this study. This free tool empirically assesses each institution's level of exposure and potential threat and provides anonymized data about other participating institutions' level of exposure and potential threat. The information security professional can also use this tool to identify/block attackers and can identify problem computers at the campus, all with minimal effort for installation and data upload.

Exhibit 71. HENA Network Analysis Diagram



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Tailoring the Roadmap for Each Institution

Based on each institution's specific information security profile, the information security professional will focus on certain areas as appropriate. Plans and actions should be based on a list of issues prioritized according to level of impact, ease of control, feasibility, and senior administration support. Steps include:

1. Assess current practices and policies.
2. Compare to targets.
3. Develop a tailored roadmap based on the gap between current and desired states.

Key issues for the particular institution and emerging concerns for the higher education sector (e.g., wireless, instant messaging, encrypting backup materials, handling laptops, PDAs, and USBs with sensitive data) should be considered. Value propositions to address with senior management are: (a) how effectively resources have been utilized to date; (b) how effectively resource will be used in the tailored roadmap; and (c) the perceived utility of justifying and approving future investments.

Exhibit 72. Tailoring the Roadmap for Each Institution

So What Should The Proactive Information Security Professional Do Now? There are Four Key Steps...

Take Stock
- What initiatives are underway or in plan? And how are they tracking?
- What are the consequences of this study for the current initiatives?
- How clear and compelling is the executive point of view on information security?
- What other resource commitments have you made?

Fix The Basics
- Are you currently able to protect your critical assets and systems?
- Do you need to implement or improve controls to achieve your desired baseline level?
- Are you able to measure progress and report internally and externally?
- Do you have the required core competencies and capabilities in place for your baseline level?

Scan for Opportunities
- Low-hanging fruit: What issues have high impact and are relatively easy to address?
- Mid-range goals: Can you leverage the above activities to address high-impact issues that are not so easy to address?
- Long-term goals: Identify long-term needs, link them to your strategy and work with executives
- What other latent or untapped capabilities do you have?

Select and Act
- Develop the business cases
- Evaluate each initiative relative to the full portfolio (realign your portfolio regularly)
- Collaborate with your executives to ensure their buy-in and support
- Select the appropriate controls, plan and implement

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Contributions of the Study

This study contributes to policy, practice and theory at the national, state, local, and individual institutional levels in four ways, as described in the following paragraphs.

First, this study represents the initial attempt to assess the link between information security incidents, approaches, policy, and practice in academic institutions and as they relate to the broader picture. This systematic assessment of issues, approaches, and network activity enables an objective, empirically-based understanding of the effectiveness of current policies and practices as well as levels of exposure and threat. Using this information, participants are able to develop data-based, focused remediation approaches for improving information security. Information security professionals in academic institutions may use these findings to justify increased budgets for information security in order to properly defend their networks or to gauge future investments in campus network security - based on quantified issues and vulnerabilities. Since this study's sanitized and anonymized databases will be available to the public through the National Institute of Justice, this project may be useful to other researchers for studies requiring empirical data regarding information security or by other entities interested in objectively understanding the network activity of academic institutions.

Second, this study furthers the definition of illicit Internet activity metrics, a critical research area. As illicit activities and crimes conducted via the Internet continue to grow exponentially, development of "hard" metrics that are comparable across academic institutions and other sectors are increasingly important. This study incorporates more traditional metrics concerning the effectiveness of controls and processes, obtained through the survey and interview components of this study, with hard metrics provided by the Higher Education Network Analysis (HENA) tool, developed in the network analysis component of the study. These hard metrics – for both inbound and outbound attacks - include frequency, protocol, and type of attack, as well as country affiliation and detailed information

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

regarding the top ten attackers and targets. These hard metrics offer direct insights into improving controls and processes, and this study provides the first application of these metrics to the academic community.

Third, this study supplies government and law enforcement agencies with an objective profile of issues and remediation approaches that are proactive, cost-effective, and facilitate information sharing. For example, the National Science Foundation (NSF) is currently working with its large facilities to develop guidelines for information security; this study may facilitate their endeavors by providing unique insights that have not been obtained previously. Law enforcement agencies that are collaborating with academic institutions to address cyberintrusions may use these findings in conjunction with their efforts to promote proactive partnering between academic institutions and law enforcement agencies. For example, the FBI may leverage its strong groundwork in working with academic institutions, established through the recent investigation of the well-publicized Stakkato incident, to build relationships with organizations supporting academic institutions as well as the institutions themselves.

Fourth, this study raises several interesting policy-related opportunities at the federal, state, and local levels. For example, an approach that bridges the gap between several federal mandates (e.g., President's National Strategy to Secure Cyberspace, DHS's National Infrastructure Protection Plan, NIST's FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems) and academia involves establishing a minimum baseline of information security for academic institutions. This baseline could serve as an incentive for obtaining research funding, in a model similar to the NSA NIETP/NSF relationship, or as a requirement for accreditation and operational funding, in a manner similar to the Department of Education's Title IV status. In either case, inter-agency collaboration and

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

shared provision of funds to assist academic institutions achieve this baseline requirement are strongly encouraged. At the state policy level, the assessment techniques developed in this study could be used in shaping state-level legislation based on empirical data (e.g., Ohio, California laws). They could also be used by state-level politicians to evaluate the current state of information security of institutions in their jurisdiction and to solicit appropriate resources from the government and private sectors. At the local level, a proactive campaign by local law enforcement on "hot topics" would be beneficial; for example, the New York Police Department successfully raised awareness at local colleges and universities about identity theft through presentations and posters. It is also recommended that, in most cases, collaboration between academia's information security professionals and local law enforcement could be enhanced.

Finally, this study provides several valuable directions for future research, including extending the research to a national focus, international crime and justice issues, and other industries. These areas of research are described in the following section of this document.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Future Research

Future research studies should focus on quantifying the threat that academic institutions pose to public safety and security, assessing the types and volume of illicit and transnational criminal activity occurring in academic institutions, and empirically determining the impact of information security policies and practices on academic institutions' information security posture. Additionally, a very promising area of future research involves empirically assessing the actual network activity of academic institutions to understand impacts on critical infrastructure and linkages to transnational crime.

Note that these research studies should involve collaboration between key players in the academic sector (e.g., EDUCAUSE, REN-ISAC, NSA's NIETP), government agencies (e.g., NIJ, FBI, MS-ISAC, US-CERT) and other entities (e.g., SANS, InfraGard, DShield). In this way, key issues can be identified and stakeholders that are best equipped to address them could be mobilized.

Quantifying the threat to public safety and security. Quantifying the threat that academic institutions may or may not pose to public safety and security would help leaders in the academic, government, and private sectors determine appropriate policy and practices. For example, if research findings demonstrate that academic institutions are, in fact, a disproportionate threat, then security campus networks may become a national and international cybersecurity priority at policy and practice levels. Conversely, if findings indicate that academic institutions are not a disproportionate threat, leaders in these sectors could focus their efforts on other crucial areas. In either case, findings from this type of research would be extremely informative for improving academic institutions' information security profile via additional knowledge of network activity.

These types of studies may be relatively easily conducted using the Higher Education Network Analysis (HENA) tool developed in this research study. HENA provides an ideal mechanism for

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

conducting research studies empirically assessing network activities because it is non-intrusive, free, robust, scalable, and has extensive comparison data (its basis is the SANS Internet Storm Center's DShield technology, which processes over 24 million records per day for contributors from the government, private, not-for-profit and higher education sectors).

Assessing illicit and transnational criminal activity in academic institutions. Illicit and transnational criminal activities (e.g., identify theft, denial-of-service attacks, fraud, and infiltration of government and private organizations) are increasingly propagated by computers infected by malicious software, creating a thriving black market for organized criminals, foreign nationals, and terrorists. While academia's networks are generally considered more vulnerable to these activities than other sectors, little empirical research has addressed this issue.

Empirically assessing academic institutions' current level of activity can be readily accomplished by combining technologies that empirically assess different components of illicit activity and transnational crime. For example, a valuable study would involve combining the HENA tool (developed in this study to identify inbound and outbound attacks that violate organizations' rules), the Worminator (developed at Columbia University to track stealth probes into and originating from organizations), and LNDAT (developed at the University of Albany to detect computers infected with bots and nodes from which attacks are emanating). Integrating these three technologies into a robust platform would provide data for the frequency of attacks on and from academic institutions, stealth attacks into and out of academic institutions, and botnet activity within and emanating from academic institutions. Outcomes of this type of research would determine types and levels of transnational criminal activity in academic institutions and could be compared with data from non-academic organizations to ascertain whether academic institutions are disproportionately vulnerable to transnational criminal activity.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Empirically determining the impact of policies and practices. Another area of future research involves empirically determining the impact of policies and practices on information security in academic institutions. Objectives would include: 1) empirically assessing attacks to and emanating from academic institutions; 2) objectively measuring the impact of implementing security controls on network activity; 3) identifying barriers and facilitators to implementing security controls in an academic environment; and 4) providing clear direction for next steps in security policy and best practices.

This type of research would best be accomplished through a study including six to ten academic institutions. Participants would provide ongoing network activity measures via the HENA tool and complete a self-assessment of security controls at the beginning and end of the study using the methodology from NIST's SP800-53A. To assess the actual impact of implementing security controls on network activity, half of the participants would implement security controls while half would not. Data would then be analyzed to determine whether significant differences exist between the two groups.

Findings from this type of research would advance the practice and knowledge of academic institutions and provide useful information to relevant government agencies. For example, government agencies that provide large-scale research funds to academic institutions (e.g., NSF, DoD, NSA) may use these findings as input to developing an accreditation process that ties the effectiveness of an institution's information security to funding opportunities. Thus, academic institutions may be required to demonstrate a baseline level of information security (i.e., a level of security due diligence) to be eligible for funding. Federal agencies that are required to comply with the NIST Federal Information Security Management Act (FISMA) standards may use these studies' insights into the barriers and facilitators for implementation when addressing security controls for their own initiatives.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Law enforcement agencies concerned with cybercrime may use outcomes from these types of studies to shape their policy in preventing and mitigating the effects of cyberattacks in academic institutions. Outcomes of this area of research would also be valuable for academic institutions. For example, academic institutions would be provided with rich management, operational and technical information security data that directly translates to focused and efficient practices.

Other research areas. Two very promising areas of future research involve the Higher Education Network Analysis (HENA) tool developed in this research study. The first area involves refining the HENA tool's data collection and reporting features to develop almost real-time reporting capabilities, correlate inbound and outbound attacks to identify transient traffic, and provide detailed information about inbound and outbound attacks by month, week, and day.

The second area involves leveraging the HENA tool as a cost-effective, real-time platform at the national, state, or local level. For example, at the national level, it may function similarly to a Department of Homeland Security Information Sharing and Analysis Center (DHS ISAC). Specifically, HENA could be integrated into the current Research and Education Networking Information Sharing and Analysis Center (REN-ISAC), provide the basis for a Higher Education Information Sharing and Analysis Center (HE-ISAC), or be used by another agency seeking similar functionality. State-and local-level governmental agencies may also find HENA useful for assessing network activity of academic institutions within their jurisdiction. Academic institutions would benefit from all of these potential applications. Additionally, the public would benefit through academic institutions' improved security of information systems containing private data and intellectual property. This may, in turn, reduce academic institutions' potential threat to critical infrastructure, public safety, and national security.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

In conclusion, as illicit activity via the Internet burgeons and perpetrators move from better-protected private and government entities to softer targets, academic institutions may represent a disproportionate threat to public safety. This concern is compounded by the increasing inter-connectedness between academic, government, military, private sector, and critical infrastructure entities. Academic institutions, along with home broadband users, are generally perceived as the weakest link in America's information security chain due to their profligate bandwidth use and lax security – a perfect digital haven for cybercrimes and an ideal incubator for illicit Internet activities. These concerns need to be addressed with empirical research and data-based recommendations for policy and practice. All of our systems are connected and problems in one sector directly affect others. If academic institutions are the weakest link, what are the risks associated with other sectors that need to interoperate with higher education? Unless we diagnose the unique vulnerabilities that exist in higher education and research laboratories and realign how those networks interoperate and share information securely, our systems will remain insecure and public safety and homeland security will suffer as a result.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

END NOTES

Thornburgh, N., "The Invasion of the Chinese Cyberspies," *Time Magazine*, August, 29, 2005, http://www.time.com/time/magazine/printout/0,8816,1098961,00.html

Goth, Greg, "Higher-Ed Networks Begin Circling the Wagons," *IEEE Distributed Systems Online,* (6:12), December, 2005, http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/mags/ds/&toc=comp/mags/ds/2005/12/oztoc.xml

McAfee, Virtual Criminology Report: North American Study into Organized Crime and the Internet, McAfee, July, 2005, www.mcafeesecurity.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf

Staff Reporter, "Students infecting university system with viruses", *Washingtonpost.com*, September 4, 2003.

Sieberg, D., "Hacker infiltrated government computers,"*CNN.com*, May 10, 2005., http://www.cnn.com/2005/TECH/05/10/govt.computer.hacker/

Multi-State Information Sharing and Analysis Center (MS-ISAC), *What You Need To Know About Botnets!*, MS-ISAC, November 2004, http://whitepapers.silicon.com/0,39024759,60125590p-39001181q,00.htm

Schevitz, Tanya, "Colleges leaking confidential data Students compromised by Internet intrusions," *San Francisco Chronicle*, April 5, 2004, http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/04/05/MNGGP60LNV1.DTL

Evers, Joris, "University of Colorado servers hacked," *CNETNews.com*, July 22, 2005, http://news.com.com/University+of+Colorado+servers+hacked/2110-7349_3800712.html?part=rss&tag=5800712&subj=news

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Haruwitz, Ralph, "Computer records on 197,000 people breached at UT," *Statesman.com,* April 24, 2006, http://www.statesman.com/news/content/news/stories/local/04/24utcomputers.html

Foster, Andrea L., "Colleges Brace for the Next Worm," *The Chronicle of Higher Education,* March 19, 2003, http://chronicle.com/weekly/v50/i28/28a02901.htm

Burd, Steffani, and Scott Cherkin, "The Impact of Information Security in Academic Institutions on Public Safety and Security", presented to the ASIS International Organization, New York, June 6, 2005.

Campbell, Donald T., and Julian C. Stanley, *Experimental and Quasi-Experimental Designs for Research,* Boston: Houghton Mifflin, 1963.

Department of Education (DOE), *National Center for Education Statistics (NCES) Integrated Postsecondary Education Data System (IPEDS)*, Home Page http://nces.ed.gov/ipeds/

Federal Bureau of Investigation, and Computer Security Institute (FBI/CSI), *FBI/CSI Computer Crime and Security Survey,* FBI/CSI, 2005, www.usdoj.gov/criminal/cybercrime/FBI2005.pdf

EDUCAUSE Center for Applied Research (ECAR), *Study on IT Security in Higher Education*, EDUCAUSE, 2005, http://www.educause.edu/2005CurrentIssuesResources/6323

Cronbach, Lee, "Coefficient alpha and the internal structure of tests," *Pschiatrika* 16 (1951): 297-334.

DShield.org, *Distributed Intrusion Detection System*, DShield.org Home Page, www.dshield.org

United States Department of Justice's Office of Community Oriented Policing Services (COPS), *National Summit on Campus Public Safety, Strategies for Colleges and Universities in a Homeland Security Environment*, United States Department of Justice, July 2005, http://www.cops.usdoj.gov/mime/open.pdf?Item=1561

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SNORT, Open Source Snort Intrusion Detection and Prevention System Home Page, SNORT, http://www.snort.org/

National Institute of Standards and Technology (NIST), *Federal Information Processing Standards Publication: Minimum Security Requirements for Federal Information and Information Systems (FIPS 200)*, NIST, July 2005, http://csrc.nist.gov/publications/drafts/FIPS-200-ipd-07-13-2005.pdf

National Institute of Standards and Technology (NIST), *Draft Special Publication 800-53A: Guide for Assessing the Security Controls in Federal Information Systems*, NIST, July 15, 2005, http://csrc.nist.gov/publications/drafts/sp800-53A-ipd.pdf

National Institute of Standards and Technology (NIST), *Federal Information Processing Standards Publication: Standards for Security Categorization of Federal Information and Information Systems. (FIPS PUB 199)*, NIST, Feb, 2004, www.csrc.nist.gov/publications/ fips/fips199/FIPS-PUB-199-final.pdf

International Organization for Standardization (ISO), *International Standard 17799,* ISO, http://www.iso.org/iso/en/aboutiso/introduction/index.html

Various Authors, EDUCAUSE, Internet2, The National Cyber Security Alliance (NCSA), *Computer Security Awareness Videos - Contest Winners*, EDUCAUSE, 2006, http://www.educause.edu/SecurityVideoContest/7103

United States National Infrastructure Advisory Council, *National Strategy to Secure Cyberspace*, U.S. National Infrastructure Advisory Council, February 14, 2003, http://www.whitehouse.gov/pcipb

United States Department of Homeland Security (U.S. DHS), *National Infrastructure Protection Plan,* U.S. DHS, November 2, 2005, http://www.fas.org/irp/agency/dhs/nipp110205.pdf

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

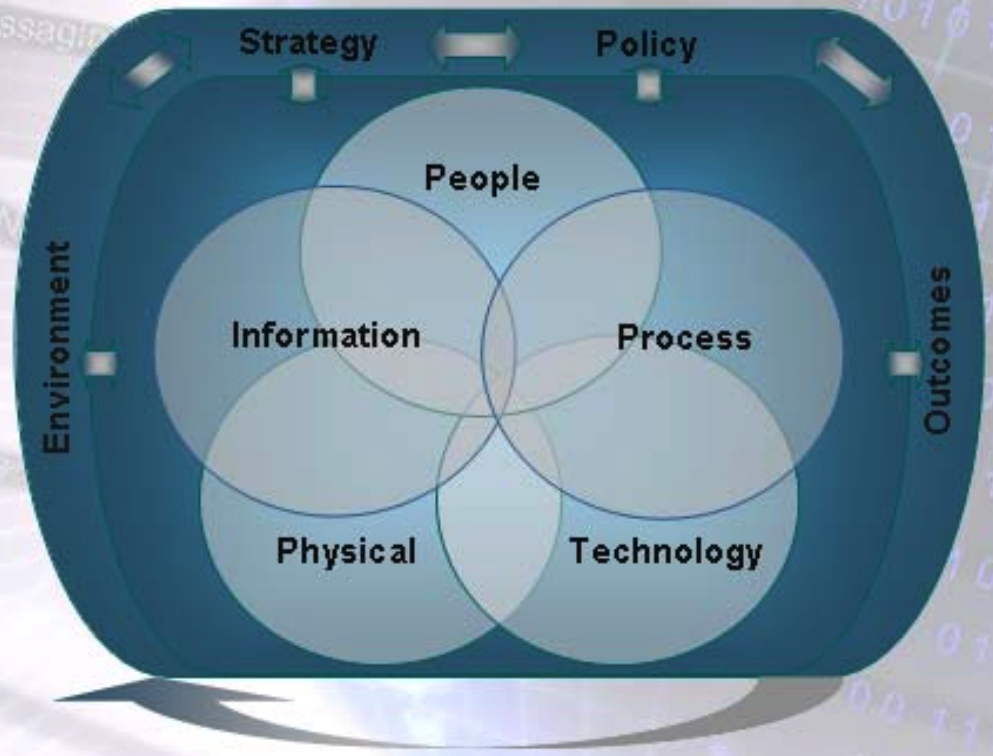
APPENDIX A:
GENERAL REFERENCE MATERIALS

- ISAI Model
- Research Methodology Process
- Project Overview
- Definition of Key Terms

This project was supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions (ISAI) Model



Model Characteristics

- Integrated vs. Fragmented
- Appropriate vs. Unbalanced
- Descriptive and Prescriptive
- Proactive vs. Reactive
- Balanced Costs and Benefits

Burd, S. & Cherkin, S. (2004)

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Research Methodology Process (RMP)

Plan

Balance Between Data Precision and Cost

An iterative process in which the study's objectives, research design, sampling plan and logistics are clearly articulated.

All aspects of planning are addressed in a collaborative manner with NIJ and team.

This process ensures:

- right balance of precision and cost
- focused and flexible approach
- robust design that yields accurate and generalizable data

Execute

Focused and Flexible

A rigorous data collection process featuring:

- standardized procedures
- cutting-edge data collection tools
- fully-trained resources
- touch points with NIJ

This process will minimize errors in data collection in a cost-effective manner and ensure accurate, reliable, and valid data.

Analyse

Robust and Generalizable

A systematic approach to ensure the data is clean, valid, and analyzed to address academic institutions' objectives.

The outcome is achieving our agreed-upon data analysis needs and forming the basis for attaining further insights.

Insight

Delivering Insight

This step draws conclusions from the analysis and extracts insights from the study findings.

Additional analyses based on data collectors' insights ensure that academic institutions receive maximal benefit from the project.

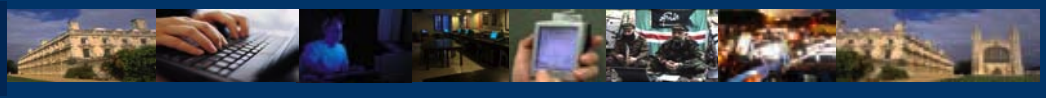
Results of the research are presented in a white paper and symposium key academic institutions and press releases will be generated.

Burd, S. (2001)

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions

Strengthening Our Infrastructure and Public Safety



PROJECT OVERVIEW

Academic institutions face unique information security threats and increasingly frequent and severe breaches. Incidents such as information theft, data tampering, viruses, worms, and terrorist activity constitute significant threats to public safety and national security.

The clash between academia's open culture and current needs for security, the anonymity and diversity of IT users, and students' high-risk activities (e.g., peer-to-peer networking, wireless, instant messaging) are establishing academic institutions as a weak link in America's chain of infrastructure security.

The purpose of this research project is to address these issues by providing objective data, recommendations for policy, and a roadmap for implementation. Project goals include:

- Identify and quantify the unique information security issues of academic institutions;
- Create an empirically based profile of threats and vulnerabilities;
- Determine the balance of costs with assets to be protected;
- Create a roadmap for implementation; and
- Distribute project results and insights to universities, government, industry and the public.

Research data will be collected from academic institutions across the United States. Approximately one hundred participants will complete a web-based survey, fifteen additional participants will complete one-on-one semi-structured interviews, and three universities' networks will be monitored for network analysis. Outcomes include an information security profile of academic institutions, recommendations for policy, a roadmap for implementation, and publications for all stakeholders. Project close date is May 2006.

This project is funded by the National Institute of Justice (NIJ), the research, development and evaluation agency of the US Department of Justice and conducted through Columbia University's Teachers College graduate school of education.

For more information, contact:
Steffani Burd, Ph.D.
sburd@infosecurityresearch.org
(917) 783 – 8496

Or visit our website:
www.infosecurityresearch.org

Project Team Members:

Executive Director:	Steffani Burd, Ph.D.
Strategic Development Director:	Scott Cherkin
Forensics Expert:	Nasir Memon, Ph.D.
Intrusion Detection Expert:	Michael Poor
Forensics Analyst:	Efstratios Gavas
Forensics Analyst:	Boris Kochergin
Academic Institution Expert:	Matthew Haschak
Data Analyst:	Jamie Condrey
Public Relations Consultant:	Aldina Tracey
Project Coordinator:	Roberta Borovetz
Research Advisor:	W. Warner Burke, Ph.D.
Policy Advisor:	Andrew MacPherson

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

DEFINITION OF KEY TERMS

1. **Information security:** protecting information and systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide:

- Confidentiality - preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity - guarding against improper information modification or destruction, including ensuring the nonrepudiation and authenticity of information
- Availability - ensuring timely and reliable access to and use of information

2. **Information:** data that has been created, collected, stored, and/or distributed at your academic institution, such as:

- Research data - technical, medical, government-related research data
- Private data - social security number, drivers license number, financial data, health information

3. **Academic institutions:** provide formal instruction for students beyond high school and may award associate, bachelor, master and/or doctoral degrees. They include academic, vocational, and continuing professional education programs such as traditional colleges, universities and US Service Academies; they exclude adult basic education and leisure programs.

4. **Incident:** any adverse event that could threaten information security, including loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Examples include viruses, worms, spam, spyware, phishing, wireless and network bandwidth misuse, and bots.

5. **Attack:** an assault on system security that derives from a deliberate attempt to evade security services and violates the security policy of a system. An attack can be active or passive and conducted by "outsiders" (e.g., hackers, terrorists, criminals), "insiders" (e.g., employees, students, faculty, staff), or via an attack mediator.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

APPENDIX B:
ISAI SURVEY MATERIALS

- Survey Structure
- ISAI Survey
- Criteria for Inclusion and Exclusion
- Postcard Invitation
- Telephone Invitation Scripts

This project was supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions
Strengthening Our Infrastructure and Public Safety

SURVEY STRUCTURE

January 31, 2006

Section 0: Explanatory Notes

a. Purpose and respondents
b. Anonymity, timing and contents
c. Thank you and date to expect results
d. Definitions of key terms

Section 1: Environment

a. Number of attacks
b. Impact of laws and regulations
c. Results of incidents
d. Likelihood may compromise others

Section 2: Policy

a. Information Security Officer
b. Who is responsible for IS
c. Formality of policy
d. End user groups provided with policy
e. End user groups officially agreeing with policy
   i. – iv. Effectiveness of students, staff, faculty, affiliates agreeing
f. Consequences for violating policy
g. Enforcement of consequences

Section 3: Information Security Controls

A. Operational Practices

a. Assessments over past 12 months
b. Patch management – computers owned by institution
c. Patch management – computers NOT owned by institution
d. Standardized computers
e. Vetting procedures for staff handling sensitive information
f. Government agencies with whom share sensitive information
g. Methods to secure sensitive information
h. Techniques evaluate IS effectiveness

B. Incidents and Disaster Management

a. Documented IT Disaster recovery plan
   i Last time tested
b. Documented Cyber incident response plan
   i. Last time tested
   ii. Last time implemented
c. Documented process for notifying individuals
   i. Last time implemented
d. Forensic analysis in-house
e. Procedure for collaborating with law enforcement
f. Groups reported incidents

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

C. Awareness and Training

a. Methods to raise awareness
b. Methods to teach awareness
c. Mandatory training and awareness
d. Effectiveness of mandatory training and awareness

D. Technology

a. Network Monitoring
b. Instant Messaging
c. Wireless
d. Identity Management
e. Filtering
f. Peer-to-Peer
g. Encryption

Section 4: Challenges

a. Culture
b. End user awareness and knowledge
c. Technology
d. Structure and systems

Section 5: Resources

A. Strategic Inputs

a. Strategic objectives
b. Priority of IS for stakeholders
c. Sponsorship of IS policy

B. Budget

a. Budget allocated to IS this year
b. Budget allocated to IS upcoming year
c. Methods justify IS expenditures

C. Structure and Roles

a. Number full-time IS staff
b. Certifications look for in staff
c. Prepared to defend against a major incident
d. Current level of preparation compared to two years ago
e. Additional comments or suggestions
f. Title
g. Contact details if not original recipient

Additional: Demographics

a. Region
b. Public/Private Funding
c. Degrees Granted (e.g., 2-year, 4-year, grad)
d. Type of Institution (e.g., general studies, specialized)
e. Size
    i. Students: number, types(undergrad or grad, on-campus or off, techies or others)
    ii. Faculty: number, type (e.g., type of faculty, job description, effectiveness)
    iii. IT staff: number, type (e.g., job description, effectiveness)
f. EDUCAUSE Member
g. NSA CAE Certification

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions
Strengthening Our Infrastructure and Public Safety

INFORMATION SECURITY IN ACADEMIC INSTITUTIONS RESEARCH SURVEY

Purpose and Respondents:

The purpose of this survey is to understand the information security issues of America's colleges and universities. Respondents to this survey are professionals with responsibility for information security in academic institutions, such as IT Directors, Information Security Officers, and CIOs.

Results of this survey will be used to develop best-practice solutions for information security in academic institutions. A detailed report will be provided to survey participants, and a general report will be provided to the public. All identifying information about you and your academic institution is confidential and anonymous, and will be strictly protected.

Timing and Contents:

This survey requires approximately 15 to 25 minutes to complete. It consists of 55 questions in five sections:

- Environment
- Policy
- Approaches to information security
- Challenges of information security
- Resources

To move to the next page of these instructions, simply click on the **SUBMIT** button below.

SUBMIT

Definitions

Five terms are used throughout this survey. Please take a moment to review their definitions.

1. Information security: protecting information and systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide:

- Confidentiality - preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity - guarding against improper information modification or destruction, including ensuring the nonrepudiation and authenticity of information
- Availability - ensuring timely and reliable access to and use of information

2. Information: data that has been created, collected, stored, and/or distributed at your academic institution, such as:

- Research data - technical, medical, government-related research data
- Private data - social security number, drivers license number, financial data, health information

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

3. Academic institutions: provide formal instruction for students beyond high school and may award associate, bachelor, master and/or doctoral degrees. They include academic, vocational, and continuing professional education programs such as traditional colleges, universities and US Service Academies; they exclude adult basic education and leisure programs.

4. Incident: any adverse event that could threaten information security, including loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. Examples include viruses and worms, spam, spyware, phishing, wireless network and network bandwidth misuse, and bots.

5. Attack: an assault on system security that derives from a deliberate attempt to evade security services and violates the security policy of a system. An attack can be active or passive and conducted by "outsiders" (e.g., hackers, terrorists, criminals), "insiders" (e.g., employees, students, faculty, staff), or via an attack mediator.

Additional Information

Space for your comments is provided at the end of this survey. If you need clarification while completing the survey or would like additional information, please email us at contact@infosecurityresearch.org or call (212) 396 – 2660.

Thank you in advance for your participation
and frank responses.
We look forward to sharing the survey results with you in the upcoming months.

To start the survey, simply click on the **SUBMIT** button below!

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SECTION 1: ENVIRONMENT

The purpose of this first section of the survey is to understand the relationship between academic institutions and the environment in which they operate. The following four questions require two to five minutes to complete in total.

Please select the option that best describes your response to each question. If you feel that you do not have adequate information to respond, please select the option “Not Sure”.

Please press the SUBMIT button to continue...

SUBMIT

1. Please indicate whether the number of attacks on your academic institution this year, when compared to the previous year, have:

(Please select one response.)

- Increased over the past year
- Decreased over the past year
- Remain the same as the past year
- Not sure

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

2. How would you rate the impact of the following laws and regulations on improving information security at your institution?

(Please indicate the one option that best indicates your response for each line in the table.)

	1 No Impact	2 Low Impact	3 Moderate Impact	4 High Impact	5 Not Sure
California Law SB1386	1	2	3	4	5
FERPA	1	2	3	4	5
Gramm-Leach-Bliley Act (GLB)	1	2	3	4	5
HIPAA	1	2	3	4	5
Sarbannes Oxley	1	2	3	4	5

SUBMIT

3. Which of the following results of information security incidents has your institution experienced within the past 12 months?

(Please select all options that reflect your response.)

- ☐ Denial of service
- ☐ Web site defacement
- ☐ Unauthorized access to information, systems or networks
- ☐ Exposure of private or sensitive information
- ☐ Theft of private information (e.g., social security numbers, medical/financial data, phishing scams)
- ☐ Theft of intellectual property (e.g., research, courseware)
- ☐ Sabotage - deliberate disruption, deletion or destruction of information, systems or networks
- ☐ Fraud (e.g., identity theft, credit card theft)
- ☐ Conduit or host for bots (i.e., zombies)
- ☐ Copyright infringement (e.g., music, movies)
- ☐ Unauthorized use of wireless network
- ☐ Laptop or mobile hardware theft
- ☐ Other, specify _____

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

4. This question explores the likelihood that your institution may compromise others outside the institution — that is, individuals, organizations, or critical infrastructure. These compromises may originate from within the institution via "insiders" (e.g., students, staff, faculty), or your institution may be used as a launching pad for attack by "outsiders" (e.g., hackers, criminals).

Please consider the current state of your institution's information security. What is the likelihood that your institution may compromise the following:

(Select one response for each line below.)

1 None	2 Low	3 Moderate	4 High	5 Not Sure
Individuals' private data (e.g., insider or outsider uses institution's systems or information to obtain individuals' private information such as social security number, financial data)				
1	2	3	4	5
Other organizations' data or functionality (e.g., insider or outsider uses institution's systems or information to launch a denial of service attack on / steal information from another organization such as a corporation or internet service provider)				
1	2	3	4	5
Critical infrastructure data or functionality (e.g., insider or outsider uses institution's systems or information to compromise sensitive information or to conduct a denial of service attack on communications, water, or energy systems)				
1	2	3	4	5

SUBMIT

Congratulations!
You have just completed the first section of the Information Security in Academic Institutions survey.

Please proceed to Section 2.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SECTION 2: POLICY

The purpose of this section is to understand your academic institution's information security policy. This section has eight questions that require four to six minutes to complete in total.

Please select the option that best describes your response to each question. If you feel that you do not have sufficient information to respond to to a question, please select the option "Not sure".

Below are definitions of key terms used in this section:

- **Information Security Policy:** the aggregate of directives, regulations, rules, and practices that prescribes how your institution manages, protects, and distributes information.

- **End User:** any individual who accesses information at your academic institution, including:
  - Students (both full-time and part-time; on-campus and off-campus)
  - Faculty (both full-time and part-time; on-campus and off-campus)
  - Staff (both full-time and part-time; on-campus and off-campus)
  - Affiliates (contractors, visitors, library users, alumni)

SUBMIT

5. Does your academic institution employ a full-time Information Security Officer or person with a similar role?

(Please select one response)

- No
- Hiring in upcoming year
- Yes
- Not Sure

If "Yes", survey program skips to Q7.

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

6. Who is responsible for information security at your institution?

(Please select one response.)

- Dedicated information security team
- IT Department's staff share responsibility
- Multiple functions share responsibility (e.g., IT Department, individual departments, executive-level)
- Third party
- Not sure
- Other, specify

SUBMIT

7. How would you describe the formality of your institution's information security policy?

(Please select one response.)

- No policy
- Informal policy
- Formal policy is being developed or implemented
- Formal policy is in place
- Combination - some areas are formal and others are informal
- Other, specify

SUBMIT

8. Please indicate the end user groups to whom your institution has provided its information security policy within the past 12 months.

Note: This means a written or electronic version has been specifically provided to end user groups. It excludes simply posting as part of the institution's website.

(Select all responses that apply.)

- Students
- Staff
- Faculty
- Affiliates (e.g., contractors, visitors, library users, alumni)
- None of the above
- Other, specify

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

9. Please indicate the end users who have <u>officially agreed</u> to your institution's information security policy.

NOTE: This means they have signed a written version of the policy or provided agreement to an electronic version of the policy within the past 12 months.

(Please select <u>all</u> responses that reflect your response.)

- ☐ Students
- ☐ Staff
- ☐ Faculty
- ☐ Affiliates (e.g., contractors, visitors, library users, alumni)
- ☐ None of the above
- ☐ Other, specify

SUBMIT

10. Please indicate the <u>effectiveness</u> of requiring STUDENTS to officially agree to the information security policy:

(Please select <u>one</u> option that best reflects your response.)

- ☐ Not effective
- ☐ Moderately effective
- ☐ Very effective
- ☐ Not sure

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

11. Please indicate the effectiveness of requiring STAFF to officially agree to the information security policy:

(Please select one option that best reflects your response.)

- Not effective
- Moderately effective
- Very effective
- Not sure

SUBMIT

12. Please indicate the effectiveness of requiring FACULTY to officially agree to the information security policy:

(Please select one option that best reflects your response.)

- Not effective
- Moderately effective
- Very effective
- Not sure

SUBMIT

13. Please indicate the effectiveness of requiring AFFILIATES to officially agree to the information security policy:

(Please select one option that best reflects your response.)

- Not effective
- Moderately effective
- Very effective
- Not sure

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

14. These last two questions of Section 2 address consequences of violating the institution's information security policies for Students, Staff, and Faculty.

Which of the following consequences of violating the institution's information security policy have been implemented for Students, Staff and/or Faculty within the past 12 months?

(Please select all responses that apply.)

- [ ] Warning
- [ ] Suspension
- [ ] Dismissal
- [ ] Law enforcement involvement
- [ ] Criminal investigation
- [ ] Civil litigation
- [ ] Legal prosecution
- [ ] Restricted access to the network
- [ ] None of the above
- [ ] Other, specify

SUBMIT

15. How would you characterize the consequences for violating your institution's information security policy over the past 12 months?

(Please select one response.)

- ( ) No real consequences (e.g., IT Department has insufficient support, Student Affairs tends to downplay, unions intervene)
- ( ) Consequences are inconsistently applied (e.g., depends on end user group committing violation, department handling the user group)
- ( ) Consequences are consistently applied (e.g., consequences are commensurate with type and severity of violation)

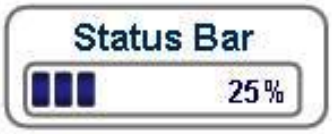
SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Congratulations!

You have just completed the first two sections of the survey.

Just press the SUBMIT button to continue . . .



SUBMIT

SECTION 3: INFORMATION SECURITY CONTROLS

The purpose of this section is to understand your academic institution's information security controls — that is, the safeguards or countermeasures that protect the confidentiality, integrity, and availability of your institution's systems and information. These operational, management, and technical controls include the following:

- **Operational Practices**
- **Awareness and Training**
- **Technology**

Several questions ask you to describe the effectiveness of information security controls used at your institution; please select the option that best describes your response to each question. If you use a particular control, but feel that you do not have adequate information about its effectiveness to respond, please select the option "Not sure".

This is the longest section of the survey. It has 17 questions that will require approximately eight to twelve minutes to complete in total.

SUBMIT

A. OPERATIONAL PRACTICES

This portion of Section 3 focuses on operational practices - that is, the processes your academic institution may use to maintain its information security. The following five questions require two to four minutes to complete.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

16. Which of the following assessments has your institution completed in the past 12 months?

(Please select all that apply.)

- ☐ Vulnerability assessment
- ☐ Information asset classification
- ☐ Risk assessment
- ☐ Penetration testing
- ☐ Application-level testing
- ☐ Audit
- ☐ None of the above
- ☐ Other, specify

SUBMIT

17. Please describe the methods your institution uses to patch computers owned by the university (e.g., departmental computers):

(Please select one option for each line in the table below that best describes your response.)

	1 Not Used	2 Not Effective	3 Moderately Effective	4 Very Effective	5 Not Sure
Manually apply patches	1	2	3	4	5
Automatic: MS Automatic Update	1	2	3	4	5
Automatic: MS Automatic Update - SMS or SUS	1	2	3	4	5
Automatic: 3rd Party Software	1	2	3	4	5
Other	1	2	3	4	5

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

18. Please describe the methods your institution uses to patch computers NOT owned by the university (e.g., students' laptops):

(Please select one option for each line in the table below that best describes your response.)

	1 Not Used	2 Not Effective	3 Moderately Effective	4 Very Effective	5 Not Sure
Manually apply patches	1	2	3	4	5
Automatic: MS Automatic Update	1	2	3	4	5
Automatic: MS Automatic Update - SMS or SUS	1	2	3	4	5
Automatic: 3rd Party Software	1	2	3	4	5
Other	1	2	3	4	5

SUBMIT

19. Does your institution currently issue standardized computers to Students?

(Please select one response.)

- **No, we do not issue standardized computers**
- **Yes, issuing standardized computers is optional</FONT< font>**
- **Yes, issuing standardized computers is required to access the network**
- **Not sure**

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

20. Please indicate the effectiveness of issuing standardized computers on an optional basis to students:

(Please select one response.)

- Very effective
- Moderately effective
- Not effective
- Not sure

SUBMIT

21. Please indicate the effectiveness of issuing standardized computers to students as a requirement for accessing the network:

(Please select one response.)

- Very effective
- Moderately effective
- Not effective
- Not sure

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

22. Many academic institutions deal with sensitive information such as:

- **Personally identifiable information about students, faculty, or staff (e.g., social security number, date of birth, medical data)**
- **Non-public information of the institution (e.g., technical, medical, government-related research data)**

Please describe the vetting procedures - if any - your institution currently uses with staff who are responsible for creating, processing, or sharing sensitive information:

(Please select one response for each line in the table below.)

	1 Not Used	2 Sometimes Used	3 Always Used	4 Not Sure
Reference check – IT staff	1	2	3	4
Reference check – All staff	1	2	3	4
Criminal background check – IT staff	1	2	3	4
Criminal background check – All staff	1	2	3	4

SUBMIT

23. With which of the following government organizations - if any - do you share sensitive information?

(Please select all that apply.)

- ☐ **Research and development programs (e.g., NSF, DARPA/HSARPA)**
- ☐ **REN-ISAC - Research and Education Networking Information & Analysis Center**
- ☐ **SEVIS - Student and Exchange Visitor Information System**
- ☐ **US-CERT - Computer Emergency Readiness Team**
- ☐ **US Department of Education**
- ☐ **IRS - Internal Revenue Service**
- ☐ **None of the above**
- ☐ **Not sure**
- ☐ **Other, specify**

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

24. Please describe the methods you use - if any - to secure the sensitive information you share while it resides on your network.

(Please select one response for each line in the table below.)

	1 Not Used	2 Sometimes Used	3 Always Used	4 Not Sure
Encrypt data on hard drive	1	2	3	4
Encrypt backup data for off-site storage	1	2	3	4
Monitor use of backup media (e.g., thumb drives/USBs, CDs)	1	2	3	4
Identity management	1	2	3	4
Internal firewall	1	2	3	4
Physical separation	1	2	3	4
Role-based access control	1	2	3	4

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

25. Which techniques - if any - has your institution used in the past 12 months to assist in evaluating the effectiveness of its information security?

(Please select all that apply.)

- ☐ Incidents (volume or type)
- ☐ Help desk calls (volume or type)
- ☐ Reports from staff
- ☐ Network traffic flow reports
- ☐ Results from web activity monitoring software
- ☐ Results from email monitoring software
- ☐ Firewall Logs
- ☐ Intrusion detection system (IDS) logs
- ☐ Intrusion prevention system (IPS) logs
- ☐ Bot (zombie) monitoring
- ☐ Security audits - conducted by internal staff
- ☐ Security audits - conducted by external organization
- ☐ Penetration testing
- ☐ None of the above
- ☐ Other, specify

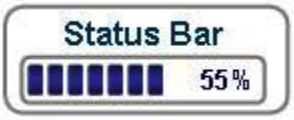
SUBMIT

CONGRATULATIONS!

You have just finished the first part of Section 3.

You are over half-way through the survey!

Please press the SUBMIT button to continue. . .



SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

B. INCIDENTS AND DISASTER MANAGEMENT

This portion of Section 3 addresses plans for supporting operations during and after an incident or disaster. The following six questions require between two to four minutes to complete.

Sources of incidents or disasters may be natural (e.g., flood, fire), human (e.g., malicious code, terrorist attack), or environmental (communications, power failure).

SUBMIT

26. Does your institution have a documented IT disaster recovery plan - that is, a plan for recovering IT systems, applications and data at an alternate site after a major disruption with long-term impact?

(Please select one response.)

- No
- Being considered or developed
- Yes
- Not sure

SUBMIT

27. When was the last time this IT disaster recovery plan was tested?

(Please select one response.)

- Never
- Within the past 12 months
- Between 13 and 18 months ago
- More than 18 months ago
- Not sure

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

28. Does your institution have a documented cyber incident response plan - that is, a plan to detect, respond to, and limit consequences of a cyber incident?

(Please select one response.)

- No
- Being considered or developed
- Yes
- Not sure

SUBMIT

29. When was the last time this cyber incident response plan tested?

(Please select one response.)

- Never
- Within the past 12 months
- Between 13 and 18 months ago
- More than 18 months ago
- Not sure

SUBMIT

30. When was the last time this cyber incident response plan was implemented?

(Please select one response.)

- Never
- Within the past 12 months
- Between 13 and 18 months ago
- More than 18 months ago
- Not sure

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

31. Does your institution have a documented procedure for notifying individuals when personal information has been accessed without authorization?

(Please select one response.)

- No
- Being considered or developed
- Yes
- Not sure

SUBMIT

32. When was the last time this notification procedure was implemented?

(Please select one response.)

- Never
- Within the past 12 months
- Between 13 and 18 months ago
- More than 18 months ago
- Not sure

SUBMIT

33. Does your institution have in-house forensic analysis - that is, a capability to address illegal intrusion, denial of service attack, introduction of malicious code or to assess whether sensitive data has been exposed?

(Please select one response.)

- No
- Being considered or developed
- Yes
- Not sure

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

34. Does your institution have a documented procedure for collaborating with law enforcement (local, state or federal) when a cyber incident occurs?

(Please select one response.)

- No
- Being considered or developed
- Yes
- Not sure

SUBMIT

35. Please indicate below the groups to whom your institution has reported information security incidents within the past 12 months.

(Please select all that apply.)

- IT department
- Legal affairs
- Executive level (e.g., Dean, President)
- Student affairs
- Local law enforcement
- Federal law enforcement
- ISP (Internet Service Provider)
- REN-ISAC
- SANS (SysAdmin, Audit, Network, Security)
- US-CERT
- District Attorney
- US Attorney's office
- None of the above
- Not sure

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

CONGRATULATIONS!

You are almost three-fourths of the way through this study.

We thank you in advance for your contribution and look forward to sharing the results with you!

Just press the SUBMIT button to continue . . .

C. AWARENESS AND TRAINING

This portion of Section 3 addresses awareness and training, which involves providing end users with sufficient information security knowledge such that they do not pose a significant threat to the institution's information security. The following four questions require between one and three minutes to complete in total.

- **AWARENESS involves understanding potential information security issues and vulnerabilities (e.g., weak passwords, exposed private information, un-updated virus protection).**
- **TRAINING involves providing sufficient knowledge such that end users can act on their awareness (e.g., install antivirus programs, perform system checks).**

Please press the SUBMIT button below to continue . . .

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

36. Please describe below the methods your academic institution uses to raise awareness of information security issues and vulnerabilities:

(Select one response for each line below.)

1 Not Used	2 Not Effective	3 Moderately Effective	4 Very Effective	5 Not Sure
Post information on the institution's web site				
1	2	3	4	5
Emails to end users				
1	2	3	4	5
Login banner when users log onto the network				
1	2	3	4	5
Newsletters to end users				
1	2	3	4	5
Posters on walls				
1	2	3	4	5
Tips and techniques (e.g., password management, wireless security)				
1	2	3	4	5

SUBMIT

37. Please describe below the methods your academic institution uses for teaching awareness in information security issues and vulnerabilities:

(Select one response for each line below.)

1 Not Used	2 Not Effective	3 Moderately Effective	4 Very Effective	5 Not Sure
Post information on the institution's web site				
1	2	3	4	5
Part of orientation - mandatory				
1	2	3	4	5
Seminars on request				
1	2	3	4	5
Formal courses offered by IT department				
1	2	3	4	5

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

38. Some institutions require end users to attend awareness and training sessions before being granted access to the network - that is, training is mandatory. Does your institution require mandatory awareness and training?

(Please select one response.)

- Yes
- No
- Not sure

SUBMIT

39. Please describe below your institution's mandatory awareness or training methods. If a method is not used, please select the "Not Used" option.

(Please select one response for each line below.)

	1 Not Used	2 Very Effective	3 Moderately Effective	4 Not Effective	5 Not Sure
Part of student orientation	1	2	3	4	5
Part of staff orientation	1	2	3	4	5
Part of faculty orientation	1	2	3	4	5
Part of performance review for staff	1	2	3	4	5
Part of performance review for faculty	1	2	3	4	5
Course credit for students	1	2	3	4	5

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Congratulations!

You are now over three-fourths of the way through the entire survey!

If you have comments, please note them now and you can include them in the space provided at the end of the survey.

Thank you again for participating in this survey - your input is critical to protecting the information assets of America's colleges and universities!

Just press the SUBMIT button to continue...

SUBMIT

D. TECHNOLOGY

The purpose of this final portion of Section 3 is to understand the technology solutions that your institution may currently use in securing its network and information. The following eight questions require between two to four minutes to complete in total. Below are definitions of the responses:

- **In Progress: Solution is being implemented OR has been implemented in some areas with plans for additional implementation in the future**
- **Implemented: Solution has been implemented across the entire institution OR implemented in some areas with no plans for additional implementation in the future**
- **Considering in 12 months: Solution is being considered for implementation in the upcoming twelve months**
- **Not Considering: Solution is not being considered for implementation**

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

40. Please describe the network monitoring approaches that your academic institution may be using or considering.

(Please select one response for each line).

1 Implemented	2 In Progress	3 Piloting	4 Considering in 12 months	5 Not Considering
Firewall – perimeter				
1	2	3	4	5
Firewall – interior				
1	2	3	4	5
Intrusion detection system (IDS)				
1	2	3	4	5
Intrusion prevention system (IPS)				
1	2	3	4	5
Anti-virus software				
1	2	3	4	5
Anti-spyware software				
1	2	3	4	5
Bot (zombie) monitoring				
1	2	3	4	5
Honeypot (i.e., identifying malicious hackers)				
1	2	3	4	5
Honeynet (i.e., identifying bots/zombies)				
1	2	3	4	5

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

41. Please describe the instant messaging technology approaches that your academic institution may be using or considering.

(Please select one response for each line)

	1 Implemented	2 In Progress	3 Piloting	4 Considering in 12 months	5 Not Considering
Monitor activity	1	2	3	4	5
Use content filtering	1	2	3	4	5

SUBMIT

42. Please describe the wireless technology approaches that your academic institution may be using or considering.

(Please select one response for each line).

	1 Implemented	2 In Progress	3 Piloting	4 Considering in 12 months	5 Not Considering
Monitor for rogue devices	1	2	3	4	5
Encryption (e.g., WEP, WPA)	1	2	3	4	5
Authentication	1	2	3	4	5
MAC address filtering	1	2	3	4	5

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

43. Please describe the identity management technology approaches that your academic institution may be using or considering.

(Please select one response for each line).

	1 Implemented	2 In Progress	3 Piloting	4 Considering in 12 months	5 Not Considering
Access control lists	1	2	3	4	5
Biometrics	1	2	3	4	5
Digital signatures	1	2	3	4	5
Password management	1	2	3	4	5
Single sign on	1	2	3	4	5
Smart cards/tokens	1	2	3	4	5

SUBMIT

44. Please describe the filtering technology approaches that your academic institution may be using or considering.

(Please select one response for each line).

	1 Implemented	2 In Progress	3 Piloting	4 Considering in 12 months	5 Not Considering
Email content filtering	1	2	3	4	5
Spam filtering	1	2	3	4	5
Web content filtering	1	2	3	4	5

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

45. Please describe the peer-to-peer technology approaches that your academic institution may be using or considering.

(Please select one response for each line).

	1 Implemented	2 In Progress	3 Piloting	4 Considering in 12 months	5 Not Considering
Monitor bandwidth	1	2	3	4	5
Shape bandwidth	1	2	3	4	5
Use content filtering	1	2	3	4	5

SUBMIT

46. Please describe the encryption technology approaches that your academic institution may be using or considering.

(Please select one response for each line).

	1 Implemented	2 In Progress	3 Piloting	4 Considering in 12 months	5 Not Considering
Data in transit (PKI, SSL, HTTPS)	1	2	3	4	5
Data on network or computers	1	2	3	4	5
Backup data for off-site storage	1	2	3	4	5

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Congratulations!

You have completed Section 3, which was by far the longest and most complex portion of the Information Security in Academic Institutions survey.

Please proceed to Section 4 . . . you will find this section moves much more quickly.

SUBMIT

SECTION 4: INFORMATION SECURITY CHALLENGES

The purpose of this section is to understand the challenges that your institution may be encountering in maintaining its information security.

If you wish to include any challenges that are not presented in the questions below, please make note and include them in the comments section at the end of the survey.

If you feel that you do not have adequate information to respond, please select the option "Not Sure".

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

47. Please rate the impact of the following challenges in attempting to maintain information security at your institution.

(For each line in the table, please select one response.)

Culture Challenges

	1 No Impact	2 Low Impact	3 Medium Impact	4 High Impact
Academic freedom	1	2	3	4
Privacy concerns	1	2	3	4
Resistance to security measures	1	2	3	4
Executive-level awareness of issues	1	2	3	4
Executive-level support of initiatives	1	2	3	4
Inadequate information security policy	1	2	3	4
Inadequate enforcement of information security policy	1	2	3	4

SUBMIT

48. Please rate the impact of the following challenges in attempting to maintain information security at your institution.

(For each line in the table, please select one response.)

End User Awareness and Knowledge Challenges

	1 No Impact	2 Low Impact	3 Medium Impact	4 High Impact
Insufficient awareness of information security issues (e.g., wireless threats, phishing scams)	1	2	3	4
Limited technical ability (e.g., don't know how to install antivirus software)	1	2	3	4

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

49. Please rate the impact of the following challenges in attempting to maintain information security at your institution.

(For each line in the table, please select one response.)

Technology Challenges

	1 No Impact	2 Low Impact	3 Medium Impact	4 High Impact
Rogue, unsupported software (e.g., freeware, P2P, specialized applications)	1	2	3	4
Rogue, unsupported computing systems (e.g., departmental computers and systems)	1	2	3	4
Unpatched systems (e.g., operating system and application holes)	1	2	3	4

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

50. Please rate the impact of the following challenges in attempting to maintain information security at your institution.

(For each line in the table, please select one response.)

Structure and Systems Challenges

	1 No Impact	2 Low Impact	3 Medium Impact	4 High Impact
Budgetary constraints	1	2	3	4
Difficulty measuring effectiveness of infosecurity initiatives	1	2	3	4
Difficult to justify expenses / articulate business case	1	2	3	4
Distributed computing systems (e.g., departmental computers)	1	2	3	4
Internal availability of skills	1	2	3	4
Internal division of responsibilities for infosecurity	1	2	3	4
Number of IT staff	1	2	3	4

SUBMIT

Congratulations!

You have completed Section 4 of the Information Security in Academic Institutions survey, and are almost finished!

Please proceed to Section 5, the final section of this survey!

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SECTION 5: RESOURCES

The purpose of this section is to understand key inputs and allocations of your academic institution's resources for information security. This section is comprised of 14 questions and requires between five and seven minutes to complete in total.

Please select the option that best describes your response to each question. If you feel that you do not have adequate information to respond, please select the option "Not Sure".

- **RESOURCES: inputs to the information security policy and practices at your institution, such as:**
  - **Stragegy - goals and priorities, policy attributes, information sources**
  - **Budget - allocation, methods for justifying expenditures and quantifying losses**
  - **Structure and roles - staffing, responsibility for information security**

SUBMIT

A. STRATEGIC INPUTS

51. Please rate the impact of the following strategic objectives of information security at your institution.

(Please select one response for each line in the table below.)

	1 Not an Objective	2 Minor Objective	3 Major Objective	4 Critical Objective	5 Not Objective
Avoid negative publicity	1	2	3	4	5
Fulfill legislative regulations (e.g., HIPAA)	1	2	3	4	5
Fulfill executive (Dean, President) directive	1	2	3	4	5
Fulfill NSA/NIETP CAE requirements	1	2	3	4	5
Improve end users' satisfaction	1	2	3	4	5
Enhance institution's image	1	2	3	4	5
Prepare for future IT initiatives	1	2	3	4	5
Fulfill ethical responsibility to protect data	1	2	3	4	5
Protect end users' privacy	1	2	3	4	5

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

52. How would you describe the current priority of information security for each of the following groups?

(Please select one response for each line in the table below.)

	1 Number 1 Priority	2 Within Priority	3 Within Priority	4 Less than Priority	5 Not Sure
Executive (e.g., Dean, President)	1	2	3	4	5
Board of Directors	1	2	3	4	5
Faculty	1	2	3	4	5
Staff – Administrative	1	2	3	4	5
Staff - IT department	1	2	3	4	5
Students	1	2	3	4	5
Parents of students	1	2	3	4	5

SUBMIT

53. Information security policies may be sponsored at various levels within universities (e.g., IT department, executive - level). How would you describe the level at which your institution's information security policy is sponsored?

(Please select one option that best reflects your response.)

- **Sponsored by IT Department**
- **Sponsored by some Departments in addition to IT department**
- **Sponsored at Executive-level within my division**
- **Sponsored at Executive-level of entire institution**
- **Sponsored by Board of Directors of entire institution**
- **Not sure**
- **Other, specify**

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

B. BUDGET

54. Please consider your central IT budget for this year. Approximately what percentage of your budget was allocated to information security (e.g., hardware/software, training, staffing)?

(Please select one response.)

- Less than 2%
- 3% - 5%
- 6% - 7%
- 8% - 10%
- Over 25%
- Prefer not to disclose
- Not sure

SUBMIT

55. How do you expect your institution's central IT budget for information security to change in the upcoming calendar year?

(Please select one response.)

- Decrease in upcoming year
- Remain the same in upcoming year
- Increase in upcoming year
- Not sure yet

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

56. Which of the following methods, if any, are used at your institution to justify expenditures for information security (e.g., hardware, software, budget, staff)?

(Please select all responses that apply.)

- ☐ Reaction to a major incident
- ☐ Outcome of assessment (e.g., risk or vulnerability assessment, audit, penetration testing)
- ☐ Incident prevention
- ☐ Part of long-term security strategy
- ☐ Requirement of law or regulation (e.g., HIPPA, SB1386)
- ☐ Cost-benefit analysis
- ☐ Investment analysis (e.g., NPV, IRR, ROI, RORI)
- ☐ None of the above
- ☐ Not sure
- ☐ Other, specify

SUBMIT

C. STRUCTURE AND ROLES

57. Approximately how many full-time central IT staff at your institution have a role solely dedicated to information security?

(Please select one response.)

- ☐ 0
- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4
- ☐ 5
- ☐ 6+
- ☐ Not sure

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

58. Which certifications - if any - do you look for when hiring or promoting your staff?

(Please select all that apply - they are listed alphabetically.)

- ☐ CISA - Certified Information Security Auditor
- ☐ CISM - Certified Information Security Manager
- ☐ CISSP - Certified Information Security Professional
- ☐ CNSS - National Security Systems Certification
- ☐ GIAC - Global Information Assurance Certification
- ☐ SCCP - Systems Security Certified Professional
- ☐ None of the above
- ☐ Not sure
- ☐ Other, specify

SUBMIT

59. How prepared do you think your academic institution is to defend against a major information security incident - that is, an incident that would compromise the confidentiality, integrity, or availability of your institutions' systems or information?

(Please select one response.)

- ○ Very prepared
- ○ Well prepared
- ○ Somewhat prepared
- ○ Not well prepared
- ○ Not at all prepared
- ○ Not sure

SUBMIT

60. How would you compare your academic institution's current level of preparation to defend against a major information security incident with its level of preparation two years ago?

(Please select one response.)

- ○ Less prepared than two years ago
- ○ Equally prepared as two years ago
- ○ More prepared than two years ago
- ○ Not sure

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

CONGRATULATIONS!

You have completed the Information Security in Academic Institutions study!

SUBMIT

61. The following two questions ask you to provide comments and information so we can create a report customized for your academic institution.

Please include any comments or suggestions below:

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

62. Please provide your title. We are asking you for this information so we can better understand the survey results. Please note that this information is strictly confidential and private. (The options are listed in alphabetical order.)

Please select the one response that most closely describes your title:

- Chancellor / President / Provost
- CIO
- CSO / Information Security Officer
- CTO
- Director of Academic Computing
- Director of Administrative Computing
- Director of Networking
- Information Security Analyst
- Vice President / Vice Provost (non-CIO)
- Other, specify

SUBMIT

63. In some academic institutions, a professional other than the individual to whom we sent the survey may complete it. We need this information to understand our response rate and to send you the summary report of survey results.

If you have been forwarded this survey from someone else within your academic institution, please provide your name and email address. Please note that this information is confidential and will be strictly protected.

Name:

Email Address:

SUBMIT

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

CONGRATULATIONS AND THANK YOU FOR YOUR TIME!

We look forward to sharing the results of this study with you in the upcoming months.
If you have any questions or would like to receive additional information, please contact us:

- **Email: contact@infosecurityresearch.org**
- **Phone: 212.396.2660**
- **Mail: Teachers College, Columbia University**
  525 West 120th Street, Box 24
  New York, NY 10028
  Attn: Steffani A. Burd, Ph.D.
- **Web Site: www.infosecurityresearch.org**

If you would like to review the list of resources that our research team is compiling, please go to the "In the News" section of our web site and click on "Resources".

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice.
Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

CRITERIA FOR INCLUSION AND EXCLUSION OF INSTITUTIONS IN THE SURVEY SAMPLE

Title IV Status

The survey's sample frame included all Title IV postsecondary institutions, as defined by the Department of Education's National Center for Education Statistics (NCES) Integrated Postsecondary Education Data System (IPEDS). Institutions participating in Title IV programs are accredited by an agency or organization recognized by the Secretary of the U.S. Department of Education, have a program of over 300 clock hours or 8 credit hours, have been in business for at least 2 years, and have a signed Program Participation Agreement (PPA) with the Office of Postsecondary Education. This criterion ensures consistency and comparability with the databases of the Department of Education and other organizations (e.g., The Chronicle of Higher Education).

Jurisdiction

The sample frame included all Title IV postsecondary institutions with jurisdiction in the United States, as defined by the Department of Education's NCES IPEDS. Thus, institutions in the 50 U.S. states and Washington DC were included in the sample frame and all Title IV postsecondary institutions outside of the U.S. (i.e., American Samoa, Guam, Federated States of Micronesia, Marshall Islands, Northern Marianas, Palau, Puerto Rico, Virgin Islands) were excluded. This decision was made because a) the focus of this study is academic institutions in the U.S., b) logistics and timing would have been complicated by sending hard-copy documentation outside the U.S., and c) respondents' primary languages other than English may have impacted the validity of survey responses.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Degree Granting

All Title IV postsecondary institutions within in the U.S. that grant degrees, as defined by Department of Education's NCES IPEDS, were included in the sample frame while non-degree granting institutions, such as vocational and technical schools, were excluded from the sample frame. Degree-granting and non-degree granting institutions pose different information security issues due to their computing power (bandwidth, machines, users), private data (health data, SSN, financial data) and intellectual property (research and development, federal grants). For example, the raw computing power, type and volume of private student data, and sensitivity and volume of intellectual property of degree-granting institutions such as Indiana University are not comparable with those of non-degree granting institutions such as the Chillicothe Beauty Academy. This decision also ensures comparability of the sample with the databases and research efforts of the Department of Education and other organizations.

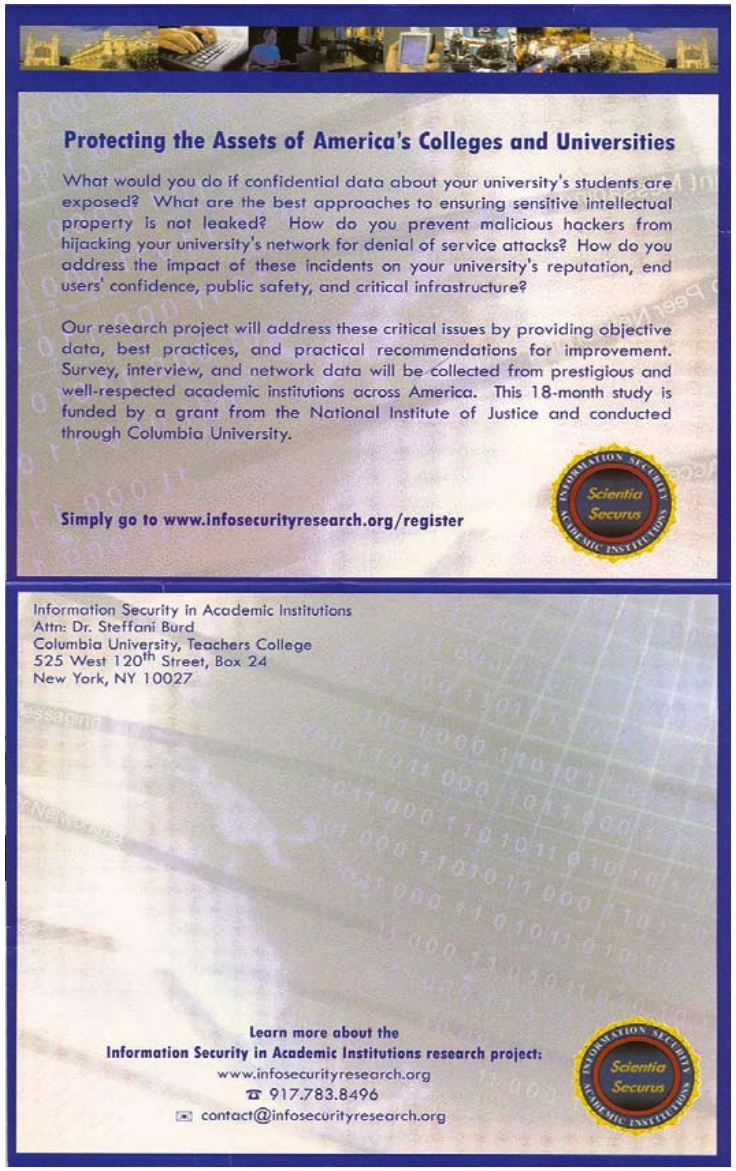
Administrative Offices

No administrative offices (i.e., central and system offices) were included in the sample frame, since they are not authorized to grant degrees and represent different information security issues than those under study in this project.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

POSTCARD INVITATION SENT TO POTENTIAL SURVEY PARTICIPANTS

Outside (front and back - visible before postcard opened)



Protecting the Assets of America's Colleges and Universities

What would you do if confidential data about your university's students are exposed? What are the best approaches to ensuring sensitive intellectual property is not leaked? How do you prevent malicious hackers from hijacking your university's network for denial of service attacks? How do you address the impact of these incidents on your university's reputation, end users' confidence, public safety, and critical infrastructure?

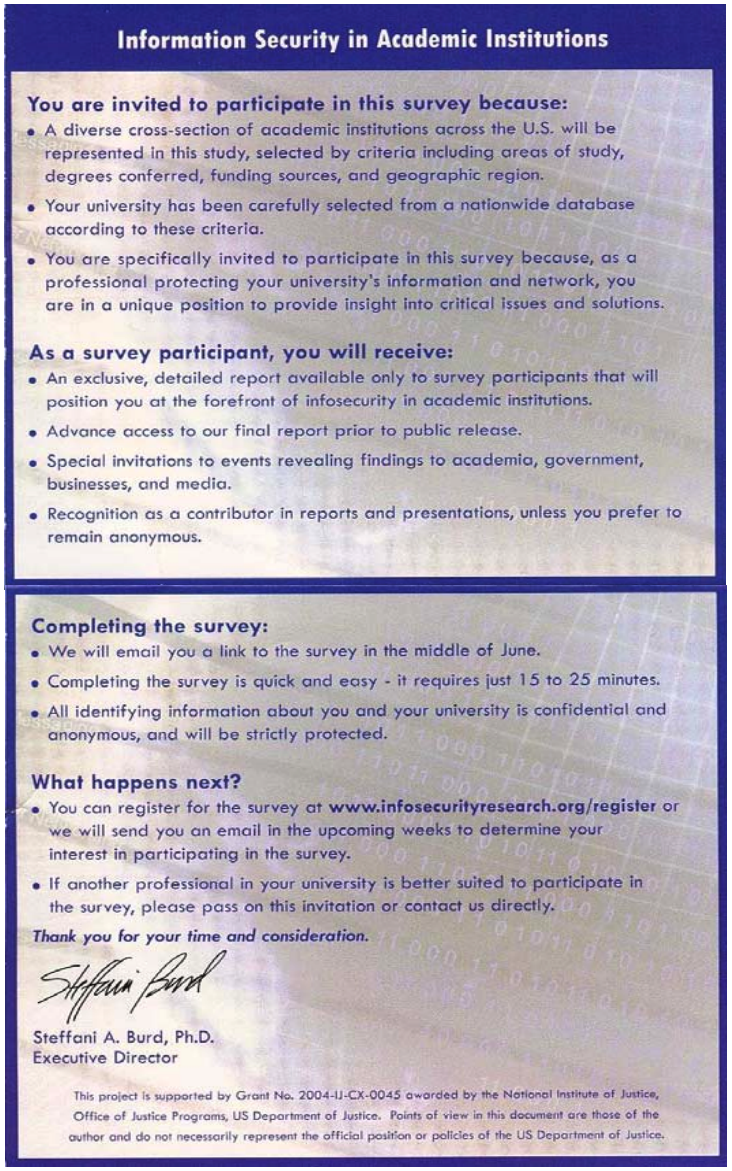
Our research project will address these critical issues by providing objective data, best practices, and practical recommendations for improvement. Survey, interview, and network data will be collected from prestigious and well-respected academic institutions across America. This 18-month study is funded by a grant from the National Institute of Justice and conducted through Columbia University.

Simply go to www.infosecurityresearch.org/register

Information Security in Academic Institutions
Attn: Dr. Steffani Burd
Columbia University, Teachers College
525 West 120th Street, Box 24
New York, NY 10027

Learn more about the
Information Security in Academic Institutions research project:
www.infosecurityresearch.org
☎ 917.783.8496
contact@infosecurityresearch.org

Inside (visible once postcard opened)



Information Security in Academic Institutions

You are invited to participate in this survey because:

- A diverse cross-section of academic institutions across the U.S. will be represented in this study, selected by criteria including areas of study, degrees conferred, funding sources, and geographic region.
- Your university has been carefully selected from a nationwide database according to these criteria.
- You are specifically invited to participate in this survey because, as a professional protecting your university's information and network, you are in a unique position to provide insight into critical issues and solutions.

As a survey participant, you will receive:

- An exclusive, detailed report available only to survey participants that will position you at the forefront of infosecurity in academic institutions.
- Advance access to our final report prior to public release.
- Special invitations to events revealing findings to academia, government, businesses, and media.
- Recognition as a contributor in reports and presentations, unless you prefer to remain anonymous.

Completing the survey:

- We will email you a link to the survey in the middle of June.
- Completing the survey is quick and easy - it requires just 15 to 25 minutes.
- All identifying information about you and your university is confidential and anonymous, and will be strictly protected.

What happens next?

- You can register for the survey at **www.infosecurityresearch.org/register** or we will send you an email in the upcoming weeks to determine your interest in participating in the survey.
- If another professional in your university is better suited to participate in the survey, please pass on this invitation or contact us directly.

Thank you for your time and consideration.

Steffani Burd

Steffani A. Burd, Ph.D.
Executive Director

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions
Strengthening Our Infrastructure and Public Safety

TELEPHONE SCRIPT
INITIAL INVITATION

Hello,

My name is _____ and I am calling about a **research study exploring information security in academic institutions**. This project is conducted through **Columbia University** and funded by the **National Institute of Justice.**

The reason I'm calling is to **invite you to participate in our research study**, and to provide you with a bit more information. This study is the **first of its kind to address** the impact of infosecurity in academic institutions on critical infrastructure, and our **goal is to understand the vulnerabilities universities face and help them better safeguard their information assets.**

There are **several benefits** for participating in the study. In addition to contributing to this critical area of research, you will receive a **benchmark report created for your institution,** a **detailed report not available to the public, advance access** to our research results and, if you choose, **recognition in our reports and presentations for participation** in the study.

If you have any questions, you can review our website at www.infosecurityresearch.org or feel free to contact me, _____, at _____ . In the meantime, I'll send you a postcard with more information about the project this week. Then in early October I'll send you an email link to a website so you can participate in the study.

Again, **thank you** in advance for your time and if you want more information feel free to call me at _____.

NOTE: If they are in person, please confirm their mailing address, title, name spelling, and email address.

Notes:

- Don't say the word "survey" – they automatically say no!!
- Try to get as many of the benefits in there up front, so they can see they will get something out of this.
- Some of them are cranky and some are really nice – it's a bit of chance in who you get.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Common questions:

Are you a vendor?

No, we are a group of experts that have formed to address this important issue. We are funded by the National Institute of Justice and the study is conducted through Columbia University.

What is the National Institute of Justice?

It's the research division of the Department of Justice. Its objective is to provide empirical, objective research to the general public.

Are you working with Educause?

Yes, we have worked with Educause to ensure our efforts are complementary. They've reviewed the survey and we will work together to share results with the public.

Will my results be given to other people?

Your specific responses will absolutely not be given to anyone – only the Executive Director of the research project will have access to all participants' data. We will report the data in aggregate, so you can be assured of your confidentiality and anonymity.

Will the name of my institution and/or my name be shared with the public?

If you would like to be recognized for participation in this study, we would be delighted to include your institution and/or your name in the final reports and presentations. However, if you prefer that your contribution remain anonymous, we will certainly respect your wishes.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions
Strengthening Our Infrastructure and Public Safety

TELEPHONE SCRIPT

FOLLOW UP #1

Hello,

My name is _____ and I am calling you about a **research study exploring information security in academic institutions**. This project is conducted through **Columbia University** and funded by the **National Institute of Justice.** Our **goal is** to understand the **vulnerabilities that academic institutions face and to develop practical, best practice solutions to help safeguard your information assets.**

The reason I'm calling is to **invite you to participate in our research study.** Rather than calling you back again, I'll **go ahead and send you a postcard** with information about our project and its objectives. If you could **keep an eye out for it that would be wonderful** – it's just a double-sided postcard with a blue border and it's title is "Help protect the information assets of America's colleges and universities". The **next step is to send you an email link** so you can complete the study on-line, should you choose to based on the information in our postcard.

If you have any questions, feel free to contact me, _____, at _____ or you can review our website at www.infosecurityresearch.org.

Again, **thank you** in advance for your time.

NOTE: If they are in person, please confirm their mailing address, title, name spelling, and email address.

Notes:

- Don't say the word "survey" – they automatically say no!!
- Try to get as many of the benefits in there up front, so they can see they will get something out of this.
- Some of them are cranky and some are really nice – it's a bit of chance in who you get.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Common questions:

Are you a vendor?

No, we are a group of experts that have formed to address this important issue. We are funded by the National Institute of Justice and the study is conducted through Columbia University.

What is the National Institute of Justice?

It's the research division of the Department of Justice. Its objective is to provide empirical, objective research to the general public.

Are you working with Educause?

Yes, we have worked with Educause to ensure our efforts are complementary. They've reviewed the survey and we will work together to share results with the public.

Will my results be given to other people?

Your specific responses will absolutely not be given to anyone – only the Executive Director of the research project will have access to all participants' data. We will report the data in aggregate, so you can be assured of your confidentiality and anonymity.

Will the name of my institution and/or my name be shared with the public?

If you would like to be recognized for participation in this study, we would be delighted to include your institution and/or your name in the final reports and presentations. However, if you prefer that your contribution remain anonymous, we will certainly respect your wishes.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions
Strengthening Our Infrastructure and Public Safety

TELEPHONE SCRIPT

FOLLOW UP #2 and #3

Hello,

My name is _____ and I am calling you about a **research study exploring information security in academic institutions**. This project is conducted through **Columbia University** and funded by the **National Institute of Justice.** Our **goal is** to understand the **vulnerabilities that academic institutions face and to develop practical, best practice solutions to help safeguard your information assets.**

The reason I'm calling is to **invite you to participate in our research study**. We sent you an email with a link to the study last week, and I would like to ensure that you received it, since the email has been filtered as spam at some of the institutions. **I'll send you another link later this week, and if you could keep an eye out for it that would be wonderful** - the title of the email is "Help protect the information assets of America's colleges and universities".

*Blurb re level if appropriate

If you have any questions, feel free to contact me, _____, at 212-396-2660 or you can review our website at www.infosecurityresearch.org. In the meantime, I'll re-send you the link to our study.

Again, **thank you** in advance for your time and if you want more information feel free to call me at 212-396-2660.

Notes:

- Don't say the word "survey" – they automatically say no!!
- Try to get as many of the benefits in there up front, so they can see they will get something out of this.
- Some of them are cranky and some are really nice – it's a bit of chance in who you get.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Common questions:

Are you a vendor?

No, we are a group of experts that have formed to address this important issue. We are funded by the National Institute of Justice and the study is conducted through Columbia University.

What is the National Institute of Justice?

It's the research division of the Department of Justice. Its objective is to provide empirical, objective research to the general public.

Are you working with Educause?

Yes, we have worked with Educause to ensure our efforts are complementary. They've reviewed the survey and we will work together to share results with the public.

Will my results be given to other people?

Your specific responses will absolutely not be given to anyone – only the Executive Director of the research project will have access to all participants' data. We will report the data in aggregate, so you can be assured of your confidentiality and anonymity.

Will the name of my institution and/or my name be shared with the public?

If you would like to be recognized for participation in this study, we would be delighted to include your institution and/or your name in the final reports and presentations. However, if you prefer that your contribution remain anonymous, we will certainly respect your wishes.

What are the benefits?

There are several benefits for participating in the study. In addition to contributing to this critical area of research, you will receive a benchmark report created for your institution, a detailed report not available to the public, advance access to our research results and, if you choose, recognition in our reports and presentations for participation in the study.

Why was I selected?

We used the Department of Education's database to randomly select academic institutions to participate in the study. Your institution was selected on this basis, and you were identified as the professional within your institution who protects its information assets.

I'm a community (technical) college – should I participate?

Yes! Since community (technical) colleges are typically under-represented in studies such as this, we are eager to make sure we understand your issues and develop solutions to help you protect your assets.

** If they are a Chief Information Officer (CIO) or Director:*

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Since you're the CIO (Director), you may wish to have someone on your team with a more hands-on role complete the study. If so, you can forward the invitation to them so they can complete it, or you can contact us directly and we'll send it to them – whichever is better for you.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

APPENDIX C:
ISAI INTERVIEW MATERIALS

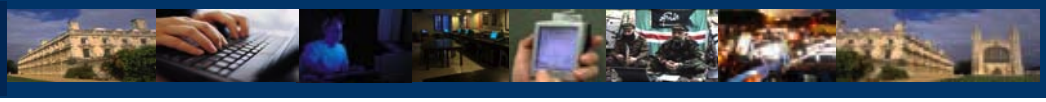
- Interview Protocol Overview
- Interview Protocol
- Telephone Invitation Scripts

This project was supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions

Strengthening Our Infrastructure and Public Safety



ISAI INTERVIEW PROTOCOL

The purpose of the Information Security in Academic Institutions (ISAI) research study is to empirically assess information security in America's colleges and universities and to provide practical recommendations for improvement. Fifteen IT Directors and Security Officers will be interviewed via a semi-structured protocol to obtain textured data and real-life scenarios. Approximately 100 IT Directors and Security Officers will complete an on-line survey that explores the objectives, challenges, and approaches involved in securing their systems and information. Two institutions will participate in a network analysis of their system's activity.

Outcomes of the interviews include: a detailed, sanitized report presented to interview participants; a high-level, sanitized report available to the general public; input to the survey and final report; and insight into linkages between universities' information security and critical infrastructure.

Benefits to participants are a detailed, sanitized report available only to interview participants and, if the participant chooses, recognition for participation in reports and presentations.

All information in the interviews is absolutely confidential and anonymous. Names of universities and participants are not disclosed and any potentially identifying information is removed. Data collected and reports are sanitized to remove all identifying information.

The interview protocol is based on the Information Security in Academic Institutions model, input from experts in academia and information security, surveys by other organizations, and a pilot study. It is designed to provide insight into participants' objectives, challenges and control measures and to provide input to the on-line survey.

The protocol requires approximately one hour to complete and is comprised of seven sections:

1. **Introduction:** purpose, use of interview results, confidentiality, definitions, timing
2. **Environmental Conditions:** attacks, technology enablers, potential exposure and threat
3. **Approaches:** policy, awareness/ training, technology, information value and sharing
4. **Challenges:** culture, end users, technology, structure and systems
5. **Resources:** strategic inputs, structure and roles, budget
6. **Insights**: overall rating, priority of security, "big picture" questions
7. **Close:** interest in report, permission to contact, thank you, contact for further information

For more information visit www.infosecurityresearch.org or email sburd@infosecurityresearch.org.

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions
Strengthening Our Infrastructure and Public Safety

ID Number: _____
Date: _____

ISAI INTERVIEW PROTOCOL

Project Overview

The purpose of the Information Security in Academic Institutions (ISAI) research study is to empirically assess information security in America's colleges and universities and to provide practical recommendations for improvement. Fifteen IT Directors and Security Officers will be interviewed via a semi-structured protocol to obtain textured data and real-life scenarios. Approximately 100 IT Directors and Information Security Officers will complete an on-line survey that explores the objectives, challenges, and approaches involved in securing their systems and information. Three universities will participate in a network analysis of their system's activity.

Interview overview

The interview protocol is intended to provide insight into academic institutions' information security objectives, challenges and approaches. It is comprised of five sections: Environment, Approaches, Challenges, Resources, and Insights. Completion time is 45 minutes to 1.5 hours.

Outcomes of the interviews include: a detailed, sanitized report presented to interview participants; a high-level, sanitized report available to the general public; and input to the survey and final report. Benefits to participants are a detailed, sanitized report available only to interview participants and, if the participant chooses, recognition in reports and presentations.

Confidentiality, voluntary nature of participation

All information in the interviews is absolutely confidential and anonymous. Names of universities and participants are not disclosed and any potentially identifying information is removed. Data collected and reports are sanitized to remove all identifying information.

Selecting participants

Four groups of universities were created based on region, level and type of education, and funding sources, then specific universities were identified based on random sampling from these pools. Individual IT Directors, Information Security Officers, and other appropriate professionals were identified at these universities as potential participants via the Internet.

Note taking

The interviewer will take thorough notes to ensure all information provided by the participant is accurately collected. The notes will be coded by number to protect participants' identity. Any quotes to be used in the reports will be sanitized to ensure participants' anonymity.

Questions and comments

Please feel free to ask questions throughout the interview and to provide suggestions for improvement. Your input is important to us and we will incorporate it into future interview protocols and/or the project's survey instrument.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Definitions

Information security:

For purposes of this interview, "information security" is defined as the protection of sensitive and valuable information against potential loss, inaccessibility, alteration, or wrongful disclosure.
Key indicators of information security include:

- Disclosed only to those who have a right to know the information (confidential)
- Protected against unauthorized modification (integrity)
- Available and usable when required (availability)

Information security involves all processes, systems, systems, services, and technologies that facilitate the use of information.

Information:

In the context of this interview, "information" includes:

- Research data - technical, medical, government-related research data
- Private data - social security number, drivers license number, date of birth, medical data

Information may be located in the centralized network as well as on departmental and individual computers. It may be resident on the network or in transit.

Information assets:

"Information assets" are defined in this interview as information that has been created, collected, stored, and/or distributed at your institution (see definition of information above). Information assets are often considered in terms of their "value" – that is, their monetary and non-monetary aspects, including:

- Costs associated with creating the information
- Losses due to compromised information
- Recovery costs, and
- Implications of compromise (e.g., reputation damage, law suits).

Network security:

"Network security" involves the protection of networks and their services from unauthorized modification, destruction, or disclosure. Network security provides assurance that a network performs its critical functions correctly and there are no harmful side effects.

Academic institution:

For purposes of this interview, an "academic institution" is an institution for higher learning (i.e., college or institution) with teaching and/or research facilities. Academic institutions may award associate, bachelor, master and/or doctoral degrees.

We thank you in advance for your participation and frank responses.
We look forward to sharing the interview outputs with you in July 2006.

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SECTION 1: ENVIRONMENT

Environment: For purposes of this interview, "environment" is defined as the external factors that affect the security of information and systems at America's colleges and universities. This includes attack trends, emerging technologies, and federal regulations.

Attack: "Attack" is defined as unauthorized network usage conducted by "outsiders" (e.g., script kiddies, hackers, criminals, terrorists) or "insiders" (e.g., students, faculty, staff).

1. **Based on the incidents at your institution over the past year, would you say that the number of attacks this year, when compared to the previous year, have:**
   (*Please select one response)*
   - ☐ Increased over the past year
   - ☐ Decreased over the past year
   - ☐ Remained the same as the past year
   - ☐ Not sure

2. **Based on this past year's incidents, which are the three groups who attack your network the most frequently?** (*Please rank order the three groups you selected)*
   - ☐ Malware writers (e.g., virus, worm, bot creators)
   - ☐ Organized criminals
   - ☐ Peer-to-peer users (e.g., music / movie theft)
   - ☐ Script kiddies
   - ☐ Students
   - ☐ Terrorists
   - ☐ Not sure
   - ☐ Other (please specify) _____

3. **Some emerging technologies may facilitate attackers' efforts. Please select the top three emerging technologies that enable attackers of your institution:**
   (Please rank order the technologies you selected)
   - ☐ Instant messaging
   - ☐ PDAs (e.g, Palm pilot, Blackberry)
   - ☐ Peer to Peer systems
   - ☐ USB / Flash drives
   - ☐ VOIP
   - ☐ Wireless LAN (WLAN) 802.X
   - ☐ Other (please specify) _____
   - ☐ None of the above

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

4. To what extent would you say that the following laws and regulations have improved information security at your institution?
(Please indicate the option that best indicates your response to each line in the table)

Law or Mandate	**Impact**				
	No Impact	Low Impact	Moderate Impact	High Impact	Not Sure
California Law SB 1386	1	2	3	4	5
FERPA	1	2	3	4	5
Gramm-Leach-Bliley Act (GLB)	1	2	3	4	5
HIPAA	1	2	3	4	5
Sarbanes-Oxley	1	2	3	4	5
Other (please specify)	1	2	3	4	5

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SECTION 2: INSTITUTION'S POTENTIAL VULNERABILITY

Vulnerability: For purposes of this interview, "vulnerability" refers to the potential for compromise of the confidentiality, integrity, or availability of the institution's network or information. Vulnerabilities may be exploited by "outsiders" (e.g., hackers, terrorists, criminals) or "insiders" (e.g., students, faculty, staff).

1. **What do you consider are the top three vulnerabilities at your institution?**
   (Please indicate your responses in the blank spaces below)

   1. _____

   2. _____

   3. _____

2. **Do you believe these top three areas of vulnerability at your institution are different from those of other universities?**
   (Please place an X next to the option that most closely matches your response)

   ___ Yes

   ___ No

   ___ Not sure

3. **On a scale from 1 to 7, where 1 is "no vulnerability" and 7 is "critical vulnerability", how would you rate the overall level of vulnerability in maintaining the security of your institution's network?**
   (Please indicate the option that most closely matches your response)

1	2	3	4	5	6	7
No Vulnerability	Very Low Vulnerability	Low Vulnerability	Moderate Vulnerability	High Vulnerability	Very High Vulnerability	Critical Vulnerability

4. **Based on your observations, do you predict that the vulnerability of your institution in maintaining its network security in the *upcoming one to three years* will:** *(please select <u>one</u> response)*

   ☐ Increase in the upcoming 1 – 3 years

   ☐ Decrease in the upcoming 1 – 3 years

   ☐ Remain the same in the upcoming 1 – 3 years

   ☐ Not sure

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SECTION 3: INSTITUTION'S POTENTIAL THREAT

Threat: Breaches in the security of universities' networks can be leveraged into attacks from the institution to compromise individuals, organizations, and critical infrastructure. These outbound attacks may originate from the institution or the institution may be used as a conduit for an attack.

For purposes of this interview, "threat" is defined as the potential your institution's network may pose to compromising individuals, organizations, or critical infrastructure. Examples are below:

- Threats to ***individuals*** may include identity theft, credit card fraud, and spam.
- Threats to ***organizations*** may include theft or disclosure of information, dedicated denial of services (DDOS) against specific organizations, worms, viruses, or spam.
- Threats to ***critical infrastructure*** may include DDOS to SCADA and communication systems or compromise of sensitive or classified information, including research and development (e.g, DARPA, HASARPA).

1. Based on your institution's information security posture, which of the following are ways your institution may pose a threat to individuals, other organizations, or critical infrastructure? *(Please check all that apply.)*

- ☐ Attacking critical infrastructure (e.g,. DDOS on SCADA, communications)
- ☐ Attacking specific organizations (e.g., DDOS, virus, worms, bots)
- ☐ Phishing scams
- ☐ Stealing individuals' private information (e.g., for identity theft / credit card fraud)
- ☐ Stealing intellectual property (e.g, R&D, patents)
- ☐ Spam/spim
- ☐ Spreading malware (e.g, viruses, worms, blended threats)
- ☐ Unauthorized use of bandwidth
- ☐ Other (please specify) _____
- ☐ Not sure

For the following questions, please circle the option that best reflects your response.

Potential threat target	Rating of potential threat				
2. What do you believe is the current level of potential threat that the institution may pose in compromising *individuals*?	1 No Threat	2 Low Threat	3 Moderate Threat	4 High Threat	5 Not Sure
3. What do you believe is the current level of potential threat that the institution may pose in compromising other *organizations*?	1 No Threat	2 Low Threat	3 Moderate Threat	4 High Threat	5 Not Sure
4. What do you believe is the current level of potential threat that your institution may pose in compromising *critical infrastructure*?	1 No Threat	2 Low Threat	3 Moderate Threat	4 High Threat	5 Not Sure

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SECTION 4: INFORMATION VALUE AND SHARING

Information: For purposes of this interview, "information" includes research data (e.g, technical, medical, government-related) and private data (e.g., social security number, drivers license number, date of birth, medical data). It may be resident on the network or in transit. It includes data located in the centralized network as well as on departmental and individual computers.

Value: "Value" addresses the monetary and non-monetary aspects of information, including costs associated with creating the information, losses due to compromised information, recovery costs, and implications of compromise (e.g., reputation damage, law suits).

1. **What do you consider to be the three most valuable types of information at your institution?** (*Please rank order from 1 = most valuable, 2 = second-most valuable, 3 = third-most valuable.)*
   - ☐ Grades, evaluations and recommendations
   - ☐ Private identifying data (e.g., social security number, drivers license, date of birth)
   - ☐ Private financial data (e.g., credit history, credit card information, family's finances)
   - ☐ Private medical data
   - ☐ Institution intellectual property (e.g., coursework, distance learning, articles)
   - ☐ Institution research data (e.g., technical, medical, government-related)
   - ☐ SCADA and communications data
   - ☐ Other (please specify) _____

2. **Why do you consider this information to be the most valuable at your institution?**

   _____

   _____

3. **With which government agencies, if any, do you share sensitive information?** *(Please select all that apply)*
   - ☐ DARPA/HSARPA
   - ☐ REN-ISAC
   - ☐ SEVIS
   - ☐ US-CERT
   - ☐ Other (please specify) _____
   - ☐ None of the above
   - ☐ Not sure

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

4. **Which methods do you use to secure sensitive information at your institution?** *(Please select all that apply)*
   - ☐ Identity management
   - ☐ Internal firewall
   - ☐ Physical separation
   - ☐ Role-based access control
   - ☐ Other (please specify) _____
   - ☐ None of the above
   - ☐ Not sure

5. **Which methods do you use, if any, to share sensitive information with government organizations?**
   (Please select all that apply)
   - ☐ Email (encrypted)
   - ☐ Email (unencrypted)
   - ☐ FTP
   - ☐ HTTP
   - ☐ HTTPS
   - ☐ VPN (SSL or IPSec)
   - ☐ Other (please specify) _____
   - ☐ None of the above
   - ☐ Not sure

6. **Which vetting procedures, if any do you use for IT staff who handle sensitive information?**
   (Please select all that apply)
   - ☐ Reference check – sometimes
   - ☐ Reference check – always
   - ☐ Criminal background check – sometimes
   - ☐ Criminal background check - always

7. **Which vetting procedures, if any do you use for administrative staff who handle sensitive information?**
   (Please select all that apply)
   - ☐ Reference check – sometimes
   - ☐ Reference check – always
   - ☐ Criminal background check – sometimes
   - ☐ Criminal background check - always

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SECTION 5: END USERS

End user: "End user" is any individual who accesses information at your institution, including:

- Students (both full-time and part-time; on-campus and off-campus)
- Faculty (both full-time and part-time; on-campus and off-campus)
- Staff (both full-time and part-time; on-campus and off-campus)
- Affiliates (contractors, visitors, library users, alumni)

1. **What are the key issues you encounter with <u>end users</u> in attempting to maintain information security at your institution?** *(Please select <u>all</u> that apply)*

   a. Culture

   ☐ Belief in freedom of information
   ☐ Low security or safeguards on information
   ☐ Privacy issues
   ☐ Resistance to security measures
   ☐ Senior management does not support information security efforts

   b. Policy

   ☐ Policy does not exist
   ☐ Policy is not adequate
   ☐ Policy is not sufficiently enforced

   c. Awareness and Knowledge

   ☐ Insufficient awareness of security issues (e.g., wireless security threats)
   ☐ Inadequate understanding of actions (e.g., storing sensitive information on palm pilots)
   ☐ Inadequate knowledge of the internet and computing (e.g., phishing scams)
   ☐ Limited technical ability (e.g., don't know how to install antivirus software)

   d. Technology, Structure & Systems

   ☐ Distributed computing systems (e.g., departmental computers)
   ☐ Emerging technology (e.g., wireless, instant messaging, P2P networking)
   ☐ Remote access issues
   ☐ Rogue, unsupported computing systems (e.g., departments' systems)
   ☐ Unpatched systems (e.g., operating system and application holes)

2. **Of all the end user security issues listed above, which is your biggest challenge?** *(Please indicate the biggest challenge below.)*

   _____

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

3. **When you consider the different types of end users, which group poses the greatest challenge in maintaining the security if the institution's information and systems?**
(Please select the one option that most closely reflects your response.)
   - ☐ Faculty
   - ☐ Staff
   - ☐ Students
   - ☐ Other (please specify) _____

4. **Why is this type of end user the most challenging?**

   _____

5. **How does your institution process new students' personal computers – if at all?**
(Please select all that apply)
   - ☐ Clean computer when student arrives at the institution
   - ☐ Install firewall application on the computer
   - ☐ Install intrusion detection/intrusion prevention application on the computer
   - ☐ Install virus protection application on the computer
   - ☐ Notify student that computer should be cleaned
   - ☐ Notify student of virus protection, firewall, intrusion detection/prevention options
   - ☐ Provide security awareness training – optional
   - ☐ Provide security awareness training – mandatory
   - ☐ Require cleaning and protection prior to logging onto institution's system
   - ☐ Require signature accepting institution's security policy (e.g., via click through)
   - ☐ Other (please specify) _____
   - ☐ None of the above

6. **How does your institution process new faculty members' personal computers – if at all?**
(Please select all that apply)
   - ☐ Clean computer when faculty member arrives at the institution
   - ☐ Install firewall application on the computer
   - ☐ Install intrusion detection/intrusion prevention application on the computer
   - ☐ Install virus protection application on the computer
   - ☐ Notify faculty member that computer should be cleaned
   - ☐ Notify faculty member of virus protection, firewall, intrusion detection/prevention options
   - ☐ Provide security awareness training – optional
   - ☐ Provide security awareness training – mandatory
   - ☐ Require cleaning and protection prior to logging onto institution's system
   - ☐ Require signature accepting institution's security policy
   - ☐ Other (please specify) _____
   - ☐ None of the above

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SECTION 6: COUNTERMEASURES

A. POLICY

For purposes of this interview, an "information security policy" is defined as the procedures, guidelines and practices for establishing and managing security in the institution's environment.

1. How would you characterize the formality of the institution's information security policy?
(Please select the one option that most closely matches your response)

- ☐ No policy
- ☐ Informal policy
- ☐ Currently developing a formal policy
- ☐ Currently implementing a formal policy
- ☐ Formal policy
- ☐ Other (please specify) _____

2. Information security policies may be sponsored at various levels within institutions (e.g., IT Department, executive-level). How would you describe the level at which your institution's information security policy is sponsored?
(Please select all of the options that reflect your response)

- ☐ Not applicable – we do not have a policy
- ☐ Sponsored by IT department
- ☐ Sponsored by some departments in addition to IT department
- ☐ Sponsored by all departments in addition to IT department
- ☐ Sponsored at executive-level (e.g., President, Dean)
- ☐ Not sure
- ☐ Other (please specify) _____

3. How do you distribute the information security policies to your institution's end-users?
(Please place an X next to all of the options that most closely match your responses)

- ___ Post information security policies on the institution's web site
- ___ Written document when end user first enters the institution
- ___ Electronic document when end user first enters institution
- ___ Written document provided periodically during end user's affiliation with institution
- ___ Electronic document provided periodically during end user's affiliation with institution
- ___ Other (please specify) _____

.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

4. Please indicate below which, if any, of the following end users are required to sign an information security policy:

(Please place an X next to all of the options that most closely match your responses)

___ Faculty
___ Staff (IT department)
___ Staff (administrative)
___ Students
___ No end users
___ Other (please specify) _____

5. What are the consequences, if any, of violating the institution's information security policy?

(Please indicate your response in the space below)

_____

6. On a scale of 1 to 7, where 1 is "not at all effective" and 7 is "extremely effective", how would you rate the effectiveness of your institution's policy in maintaining network security?

1	2	3	4	5	6	7
No at all Effective	Not very Effective	Somewhat Effective	Moderately Effective	Highly Effective	Very Highly Effective	Extremely Effective

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

B. AWARENESS AND TRAINING

For purposes of this interview, "awareness and training" involves providing end users with sufficient information security knowledge that they do not pose a significant threat to the institution's information. "Awareness" includes developing sensitivity to potential vulnerabilities (e.g., USBs and palm pilots) and understanding potential security issues (e.g., wireless and IM security). "Training" involves providing sufficient knowledge that end users can act on their awareness (e.g., install antivirus programs, perform system checks)

1. What type of optional or mandatory training - if any - does your institution provide to its end users in maintaining information security?
(Please place an X for all options that apply)

Type of training	Students	Faculty	Staff
Orientation for new end users – optional			
Orientation for new end users – mandatory			
Ongoing security training - optional			
Ongoing security training – mandatory			
Periodic alerts for new threats			
Incident identification			
Other (please specify) _____			
Not sure			

2. Does your institution measure the effectiveness of its security training?

- ☐ No
- ☐ Yes
- ☐ Not sure

If yes,

2a. How do you measure the effectiveness of your security training?

- ☐ Mandatory written/digital test based on content of security training
- ☐ Social engineering testing (i.e. sending out mock phishing scheme)
- ☐ Staff reports of experiences
- ☐ Track volume of incidents per week
- ☐ Track volume and type of help desk issues
- ☐ None of the above
- ☐ Not sure

3. If you had unlimited resources and could change one aspect of awareness and training at your institution, what would you do? *(Please indicate your response in the space below)*

_____

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

C. OPERATIONAL PRACTICES

Prevention: For purposes of this interview, "prevention" involves proactively addressing compromise of the confidentiality, integrity, or availability of the institution's network and information.

1. Please consider the practices your institution uses to *prevent* information security breaches.
(For each line in the table below, please select the one option that best reflects your response.)

Prevention Practices	Not Considered	Being Considered/ Selected	Being Built	Operating Not Effective	Operating: Effective	Operating: Very Effective	Not Sure
CCTV systems/surveillance							
Key cards							
Network access control							
Password management							
Assessments							
Risk assessment							
Vulnerability assessment							
Penetration testing							
Patch Management							
Ad hoc – central IT system							
Automated – central IT system							
Institution-owned computers							
Privately-owned computers							
Other (specify) _____							

Detection and Investigation: "Detection" involves identifying potential or actual compromise of the confidentiality, integrity, or availability of the institution's network and information. "Investigation" refers to analysis of the causes of compromise to the institution's network and information.

2. Please consider the practices your institution uses to *detect* and *investigate* incidents.
(For each line in the table below, please select the one option that best reflects your response.)

Detection Practices	Not Considered	Being Considered/ Selected	Being Built	Operating Not Effective	Operating: Somewhat Effective	Operating: Very Effective	Not Sure
Bandwidth							
Monitor bandwidth use							
Control bandwidth use							
Firewall							
Track logs							
Review logs							
Act on logs							
Forensic Analysis							
Intrusion Detection / Prevention							
Track logs							
Review logs							
Act on logs							
Other (specify) _____							

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Response: "Response" involves the plans and actions to address incidents, which may range from individual compromises to organization-wide disaster.

3. Please consider the practices your institution uses to *respond* to information security incidents.
(For each line in the table below, please select the one option that best reflects your response.)

Response Practices	Not Considered	Being Considered/ Selected	Being Built	Operating Not Effective	Operating: Somewhat Effective	Operating: Very Effective	Not Sure
Business Continuity Plan							
Disaster Recovery Plan							
Central IT systems & data							
Department systems & data							
Department-owned computers							
Privately-owned computers							
Tested Disaster Recovery Plan							
Core IT systems & data							
Department syst. & data							
Department-owned computers							
Privately-owned computers							
Incident Management Plan							
Identifying incidents							
Reporting incidents							
Alerting appropriate parties							
Other (please specify) _____							

4. Please indicate below to the groups to whom your institution has *reported* information security breaches and/or incidents within the past year.
(For each line in the table below, please select all of the options that reflect your response.)

Within institution

- ☐ IT department
- ☐ Legal affairs
- ☐ Executive level (e.g., Dean, President)
- ☐ Student affairs
- ☐ Other (please specify) _____
- ☐ Not sure

Outside institution

- ☐ Local law enforcement
- ☐ Federal law enforcement
- ☐ ISP (Internet Service Provider)
- ☐ REN-ISAC
- ☐ SANS (SysAdmin, Audit, Network, Security)
- ☐ US-CERT
- ☐ Other (please specify) _____
- ☐ Not sure

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

D. TECHNOLOGY

1. **The following question addresses general technologies that your institution may use in securing its network and information.**
   (For each line in the table, please select the option that best reflects your response.)

Technology	Implemented	In Progress	Piloting	Considering in 12 months	Not Considering
Network monitoring					
Firewall – perimeter					
Firewall – interior					
Intrusion detection system (IDS)					
Intrusion prevention syst. (IPS)					
Anti-virus software					
Anti-spyware software					
Bot (zombie) monitoring					
Honeypot (i.e., identifying malicious hackers)					
Honeynet (i.e., identifying bots/zombies)					
Instant Messaging (IM)					
Monitor activity					
Use content filtering					
Wireless					
Monitor for rogue devices					
Encryption (e.g., WEP, WPA)					
Authentication					
MAC address filtering					
Identity management					
Access control lists					
Biometrics					
Digital signatures					
Password management					
Single sign on					
Smart cards/tokens					
Filtering					
Email content filtering					
Spam filtering					
Web content filtering					
Peer-to-Peer (P2P)					
Monitor bandwidth					
Use content filtering					
Shape bandwidth					
Encryption					
Data in transit (PKI, SSL, SHTTP)					
Data on network or computers					
Backup data for off-site storage					

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

2. Please indicate the programs, if any, you currently use for:

Antivirus: _____

Firewall: _____

IDS/IPS: _____

3. Of all the technologies used at your institution, which one is the <u>most</u> effective in maintaining network security? *(Please indicate your response in the blank space below)*

_____

4. Of all the technologies used at your institution, which one is the <u>least</u> effective in maintaining network security? *(Please indicate your response in the blank space below)*

_____

5. Of all technologies available (e.g., commercial, government), which would you implement if you had unlimited resources? *(Please indicate your response space below)*

_____

6. What do you anticipate will be the top three technologies that your institution will use in the <u>upcoming 1 – 3 years</u> to ensure information security?

1. _____

2. _____

3. _____

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

E. RESOURCES

1. **How many staff at your institution have a role dedicated to information security?**
   (Please indicate your response in the space below)

   Part-time IT staff: _____

   Full-time IT staff: _____

2. **Please consider your central IT budget for this year. Approximately what percentage of this budget is allocated to information security (e.g., systems, technology, training and awareness)?**
   (Please place an X next to the option that most closely matches your response)

   ___ 0% - 2%

   ___ 3% - 5%

   ___ 6% - 10%

   ___ 11% - 25%

   ___ Not sure

4. **Do you use a methodology to quantify losses from security breaches (e.g., worms, viruses, spam, P2P, loss of information)?**
   (Please place an X next to the option that most closely matches your response)

   ____ No

   ____ Yes

   ____ Not sure

   If "Yes", **Which methodology(ies) do you use?**
   (Please indicate your response below)

   _____

5. **Based on compromises over the past year, would you estimate losses at your institution to be:** *(Please select the one option that most closely reflects your response.)*

   ____ $0 - $100K

   ____ $101K - $250K

   ____ $251K - $1M

   ____ $1.1M - $3M

   ____ $3.1M - $M

   ____ Not sure

   ____ Prefer to not disclose

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

6. **Which of the following resources, if any, do you use for obtaining information about best practices?** *(Please select all that apply.)*
   - ☐ Colleagues
   - ☐ EDUCAUSE
   - ☐ HEITA
   - ☐ InfraGard
   - ☐ NSA NIETP
   - ☐ SANS
   - ☐ US-CERT
   - ☐ REN-ISAC
   - ☐ Journals and magazines
   - ☐ Internet
   - ☐ None of the above
   - ☐ Other (please specify) _____

7. **If you had unlimited additional staff, time, and funding allocated to network security at your institution, what would you do differently?**
   (Please indicate your response below)

   _____

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

SECTION 7: INSIGHTS

1. **Overall, on a scale of 1 to 7, where 1 is "not at all effective" and 7 is "extremely effective", how would you rate the effectiveness of information security at your institution?**
   (Please select the option that most closely reflects your response)

1	2	3	4	5	6	7
No at all Effective	Not very Effective	Somewhat Effective	Moderately Effective	Highly Effective	Very Highly Effective	Extremely Effective

2. **Overall, how does information security *currently* rank on your list of priorities?**
   (Please indicate your response in the blank space below)

   _____

   How do you think security will rank on *next year's* list of priorities?
   - ☐ Increase priority
   - ☐ Decrease priority
   - ☐ Remain the same
   - ☐ Not sure

3. **What do you consider to be the biggest challenge in the *upcoming* year in ensuring the security of your institution's network?**
   (Please indicate your response in the blank space below)

   _____

4. **What do you consider to be the <u>one</u> thing your institution does best to protect its network?**
   (Please indicate your response in the blank space below)

   _____

5. **If you had unlimited resources, budget, and authority, what is the <u>one</u> thing you would do to ensure the security of your institution's network?**
   (Please indicate your response in the blank space below)

   _____

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

What other topics, if any, did we not discuss that you would like to address?
(Please indicate your response in the blank space below)

_____

THANK YOU FOR YOUR TIME!

If you have any questions or would like to additional information, please feel free to contact us:

Email: contact@infosecurityresearch.org

Phone: 917.783.8496

Mail: Teachers College, Columbia Institution
525 West 120th Street, Box 24
New York, NY 10028

Website: www.infosecurityresearch.org

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in
Academic Institutions
Strengthening Our Infrastructure and Public Safety

INVITATION SCRIPT
INTERVIEWS

Hello, my name is Steffani Burd, and I am calling to follow up on an email I sent you last week inviting you to contribute to a research study exploring information security in academic institutions.

I'm contacting you directly because we want to make sure we directly address the key issues facing IT Directors of universities across the United States. We're interviewing 15 directors that represent different universities in America – that is, public and private, undergraduate and graduate, general and technical studies, all ranging from the West Coast to the East Coast.

Your university is perfect for the criteria of <public/private>, <undergraduate/graduate>, <general/technical studies>, and <West Coast/Mid Western/East Coast> region, so I would like to learn more about the issues you face in addressing network and information security at <University name>.

The interview should require approximately one hour, and we can do it over the phone at any time that's convenient for you. Note that all interviews are strictly confidential and any identifying information about you and your university is strictly protected – we're just trying to make sure we do the best job in ensuring we address all the different universities' information security issues.

If you participate, we will send you sanitized and aggregate results of the interviews and, at the end of the study once we've finished our interviews and survey, if you'd like I'd be happy to mention your name or your university's name as one of the key contributors.

If you could contact me to let me know if you'd like to help us out, I'd greatly appreciate it. Again, my name is Steffani Burd, and I can be reached at 917.783.8496 or sburd@infosecurityresearch.org. In the meantime, you can also learn more about our research study by checking out our website at www.infosecurityresearch.org.

Thank you again, and I look forward to speaking with you soon.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

APPENDIX D:
NETWORK ANALYSIS MATERIALS

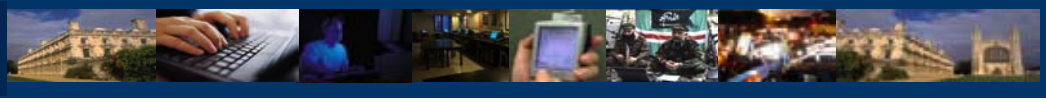
- Network Analysis Overview
- Network Analysis Schematic
- Network Analysis Procedures
- Screen Shots of User Interface

This project was supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions

Strengthening Our Infrastructure and Public Safety



NETWORK ANALYSIS OVERVIEW

The purpose of the Information Security in Academic Institutions research study is to empirically assess information security in America's colleges and universities and to provide practical recommendations for improvement. This study involves collection of survey, interview, and network activity data from academic institutions across the US.

Network analysis of system activity provides an understanding of inbound and outbound attacks plus confirmation or contradiction of survey and interview data. Three approaches – baseline assessment, comparison of threat over time, and granular analysis of network health – are used in the network analysis method to optimize the balance of both control (e.g., standard assessment data sources) and impact (e.g. , real-life, extant assessment data).

The purpose of the baseline assessment is to provide independent, empirical data regarding *actual* exposure of the universities' systems and information and potential threats to other organizations. Three universities will provide their firewall drop logs and intrusion detection logs over three months (Oct – Dec 2005). Sensitive data can be sanitized using DShield scripts. Data will be queried and analyzed at the lowest common denominator to empirically assess level of exposure and threat.

Outcomes of this assessment include: 1) empirical baseline of the level of "exposure" (attacks on the universities) and "threat" (potential attacks on other organizations via universities); 2) confirmation or contradiction of survey and interview data; 3) insight into links between the internet's impact on universities and universities' impact on the internet and critical infrastructure.

Benefits to participants include:

- 24x7 visual monitoring of exposure and threats for their university and high-level viewing of other participants' activity;
- In-depth understanding of potential exposure and threat;
- Renowned intrusion detection and computing experts' advice in reducing exposure and threat;
- Recognition in reports and presentations, if the participant chooses to do so.

All information in the network analysis is absolutely confidential and anonymous. Names of universities and participants are not disclosed and any potentially identifying information is removed. Data collected and associated analyses are sanitized to remove all identifying information and results are presented in aggregate form.

Data sources, types, sanitizing methods, activities and timing are as follows:

Outcome	Data Source	Data Types	Activities and Timing
Potential Exposure	Firewall drop logs	• Date/time stamps • IPs: source & destination • Ports: source & destination	• Collect/sanitize/send • Every half-hour from Oct to Dec 2005
Potential Threat	IDS/IPS logs	• Date/time stamps • IPs: source & destination • Ports: source & destination • Alert messages	• Collect/sanitize/send • Every half-hour from Oct to Dec 2005

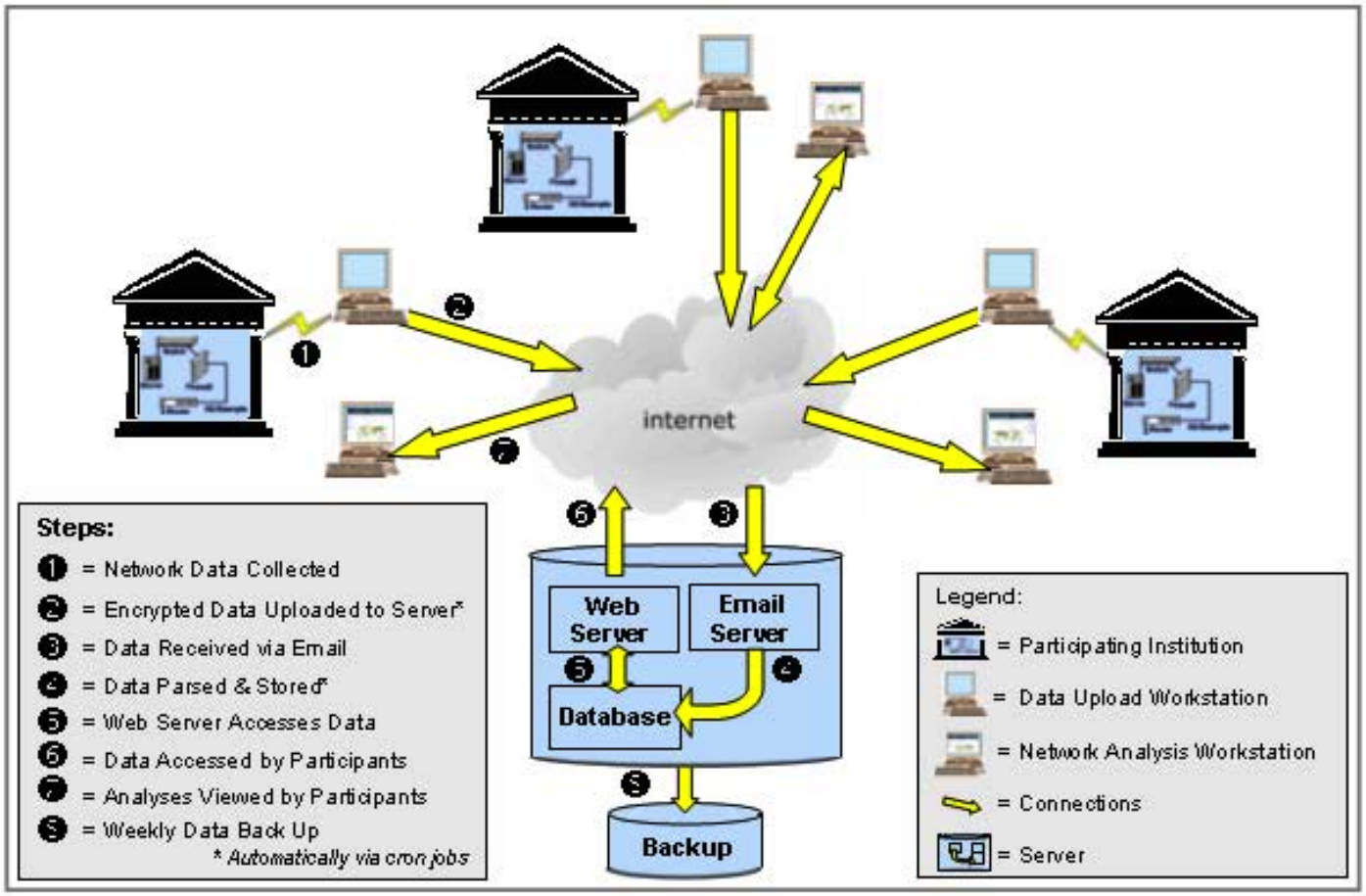
For more information visit www.infosecurityresearch.org or email contact@infosecurityresearch.org.

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions
Strengthening Our Infrastructure and Public Safety

NETWORK ANALYSIS DIAGRAM



August 20, 2005

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

NETWORK ANALYSIS PROCEDURES

This document provides participants in the baseline assessment component of the Information Security in Academic Institutions (ISAI) research project's network analysis with the procedures to collect, sanitize, and send data for the baseline assessment. It should be considered in conjunction with the ISAI project overview, network analysis and baseline assessment overviews, and confidentiality agreement.

The baseline assessment provides independent, empirical data regarding level of "exposure" (attacks on universities) and "threat" (potential attacks on other organizations via universities). Three universities are providing their logs over four months (March – June 2005). Sensitive data can be sanitized using DShield and PERL scripts. Data will be queried and analyzed using the least common denominator to empirically assess level of exposure and threat.

All information in the baseline assessment is absolutely confidential and anonymous. Participants in the study are not disclosed. Data collected and analyzed is sanitized to remove all identifying information and results are presented in aggregate form.

Firewall drop logs and IDS/IPS logs will be automatically culled, parsed, and uploaded from the three participating universities every half-hour. Firewall drop log data collected from the university's firewall application includes date/time stamps, IPs (source & destination) and ports (source & destination). Intrusion Detection/Prevention (IDS/IPS) data collected includes date/time stamps, IPs (source & destination), ports (source & destination) and alert messages. External machine logs (attackers & attackees) include date/time stamps, IPs (source & destination), and ports (source & destination). All payload data transmitted to and from machines within the university is excluded from data collection.

Sending your network activity logs to the ISAI Network Analyst involves three steps, which are outlined on the following pages. Once you have completed these steps, your activity logs will be automatically sent to the Network Analyst every half-hour, with no additional effort on your part.

If you have any questions, please contact either:

- Mike Poor, our Intrusion Detection Expert (240.338.4882, mpoor@infosecurityresearch.org) or
- Efstratios Gavas, our Network Analyst (847.293.4660. egavas@infosecurityresearch.org).

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Step 1: Set Up Your Machine to Process Logs

1. Go to www.dshield.org/howto.php

2. Select appropriate prewritten client

a. Go to **"Prewritten clients"** in red text

b. Look for your firewall to see whether it is listed under either **DShield "Universal" CVTWIN Client** or **Third Party Programs that submit Firewall Logs to DShield**.

c. If your firewall is listed under **DShield "Universal" CVTWIN Client**:

   i. Click on **DShield "Universal" CVTWIN Client**, which will take you to www.dshield.org/windows_clients.php.

   ii. Scroll down ¾ of the page to **CVTWIN-SETUP.EXE** (2.1 megabytes)

   iii. Download CVTWIN-SETUP.EXE (2.1 megabytes) by clicking on it.

d. If your firewall is listed under **Third Party Programs that submit Firewall Logs to DShield**:

   i. Click on **Third Party Programs that submit Firewall Logs to DShield**, which will take you to http://www.dshield.org/windows_clients.php#3rd_party

   ii. Select the appropriate program and follow it instructions.

3. Install appropriate scripts

a. Go to where you saved the file, and unzip the application by double-clicking on the .zip file.

b. Follow the instructions, using the defaults as you continue.

   Note: The second prompt, which has a box for DShield Universal Firewall Client Setup, is not intuitive. You actually need to click on the computer icon in the upper left hand side of the command box.

4. Configure scripts

a. Go to the "Start" menu. Under "Programs" select "DShield" then "DShield Universal Firewall Client"

b. Go to "Edit" on the tool bar and select "Configure . . "

c. Modify the "DShield User ID" field by entering your assigned UserID

d. Modify the "Your Email Address" field by entering your assigned email address

e. Change the "SMTP Server Name" field by entering dshield.infosecurityresearch.org

   Note: If your university blocks the use of external SMTP servers, you must use your internal SMTP server name in this field.

f. Fill in the "Firewall" field by selecting your university's firewall (e.g., Snort, Windows XP, etc) from the drop-down menu

g. Fill in the "Logfile" field by selecting the location where you'd like the log files to be stored (use the browse button)

h. Press OK

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

5. Modify your CVTWIN.INI file

a. Change the destination of your scripts
   i. Go to the "Edit" pull-down and select "'Edit CVTWIN.INI". This will open a notepad screen
   ii. Go to the line specifying where the reports will be sent
   Search for "toaddr" by using the "Edit" pull-down, selecting "Find", and entering "toaddr"
   iii. Change the "toaddr=dshield.org" to "toaddr=reports@dshield.infosecurityresearch.org"

b. Change the Time Zone (if needed)
   i. Go to the line specifying the time zone
   Search for "time zone" by going to the "Edit" pull-down, selecting "Find", and entering "TZ"
   ii. Look at the "TZ=" values corresponding with your time zone (e.g., -5:00 is Eastern Standard Time)
   iii. Change the default of "TZ=-04:00" to the appropriate "TZ=" value

c. Save and Exit the "Edit CVTWIN.INI" file
   i. Go to "File" pull-down and select "Save"
   ii. Go to "File" pull-down and select "Exit"

6. Change the IP Filter Configurations

a. Change the IP Source filter
   i. Go to "Edit" and select "Edit Source IP Filters". This will open a notepad screen called "SourceIP.flt"
   ii. Put a # sign in front of each line of IP numbers so they aren't filtered (the lines start at 0.0.0.0 and end at 255.255.255.255)
   iii. Save and Exit the SourceIP.flt file
      a. Go to "File" pull-down and select "Save"
      b. Go to "File" pull-down and select "Exit"

b. Change the IP Target filter
   i. Go to "Edit" and select "Edit Target IP Filters". This will open a notepad screen called "TargetIP.flt"
   ii. Put a # sign in front of each line so they aren't filtered (starts at 0.0.0.0 and ends at 127.0.0.1)
   iii. Save and Exit the TargetIP.flt file
      a. Go to "File" pull-down and select "Save"
      b. Go to "File" pull-down and select "Exit"

Step 2: Process the Logs

1. Go the "Start" menu and start up DShield by
2. Go to "File" pull-down and select "Convert [*depending on what firewall you configured in Step 1*]"
3. Go to "File" pull-down and select "Mail to reports@dshield.infosecurityresearch.org"

Step 3: Automate Sending the Logs

- If you use Unix: Set your cronjob to every ½ hour
- If you use Windows: Set your scheduler to every ½ hour

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions

Strengthening Our Infrastructure and Public Safety

Network Analysis

As of Wed Jul 27 03:22:57 2005 UTC

Summary Information | Participant Data

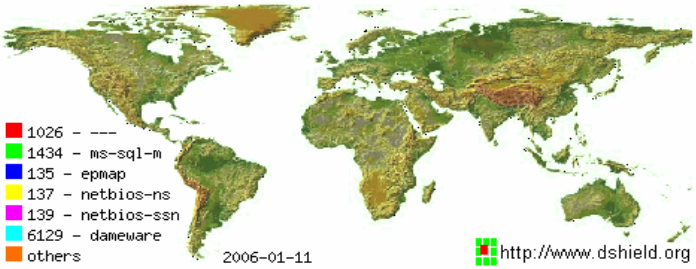
Home | Top 10 Attackers | Top 10 Targets | Top 10 Targeted

Status & Trends

Survival Time: 5 min.
SANS Internet Storm Center Status:

Attackers

Top Attacker: 203.145.133.246
Top 10 Attackers
Past Weeks' Attacks (movie)



Geographic Distribution of Attackers

Targets

Top Attacked Port: 1026
Top 10 Attacked Ports

Resources

Records Added		
Last Month	Last Week	Today
17,076	5,141	707

Last Update: 25/Mar/2006 17:27

DShield is a Servicemark of Euclidian Consulting.

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Program, US Department of Justice.

Points of view in this document are those of the author and do not necessarily represent the offical position or polices of the US Department of Justice.

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions

Strengthening Our Infrastructure and Public Safety

Network Analysis

As of Wed Jul 27 03:22:57 2005 UTC

Summary Information | Participant Data

Home | Top 10 Attackers | Top 10 Targets | Top 10 Targeted

The **Top 10 Attackers** list identifies the ten most frequent attackers of academic institutions in the study at the point in time you access the site. This report is useful for:

- Identifying who is attacking your academic institution
- Assessing whether your institution is undergoing a targeted attack or if all research participants are experiencing a general attack.

IP Address	Host Name
81.244.181.227 $^{2}/_{1}$	227-181.244.81.adsl.skynet.be
69.225.127.0	adsl-69-225-127-0.dsl.sndg02.pacbell.net
201.224.36.129	
140.134.20.44	
12.73.161.55	55.denver-04-05rs.co.dial-access.att.net
159.134.137.49	159-134-137-49.as1.srl.dublin.eircom.net
202.103.213.151 $^{20475}/_{7065}$	
61.150.85.22 $^{7185}/_{4234}$	
221.202.129.164 $^{1273605}/_{162890}$	
211.157.102.70	

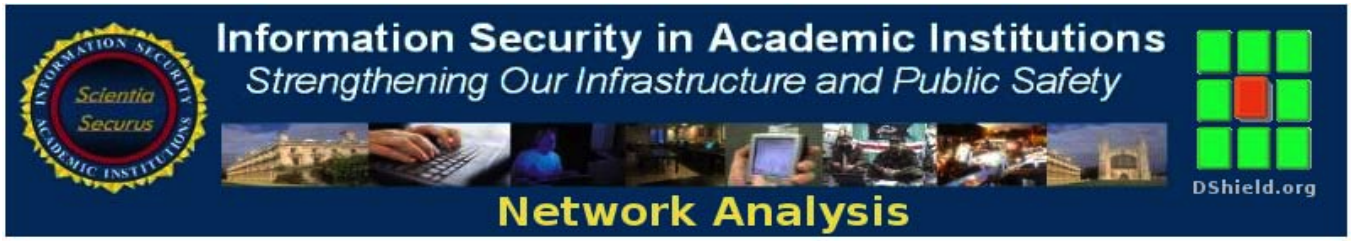
Legend:

IP Address $^{\text{Number of lines implicating this attacker}}/_{\text{Number of attacks at IP address}}$

IPs for which you have notified the DShield administrators as part of the DShield FightBack initiative, so you can check if an administrator was notified (don't forget to sign up for FightBack!)

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.



As of Wed Jul 27 03:22:57 2005 UTC

Summary Information | Participant Data

Home | Top 10 Attackers | **Top 10 Targets** | Top 10 Targeted

This list shows the top 10 most probed ports of the academic institutions in the study – that is, **Top 10 Targets** within institutions participating in this study. Specific IP addresses are available once you've entered the Member Login section. IP addresses are handled in this manner to ensure participants' confidentiality and anonymity.

Service Name	Port Number	Activity Past Month	Explanation
---	53		
Icq	445		icq instant messenger
microsoft-ds	48153		Win2k+ Server Message Block
ms-sql-m	1026		Microsoft-SQL-Monitor
netbios-ns	139		NETBIOS Name Service
netbios-ssn	1027		NETBIOS Session Service
ms-sql-s	135		Microsoft-SQL-Server
Epmap	200		DCE endpoint resolution
www	137		World Wide Web HTTP
Radmin	113		Remote Administrator default port

To read the explanation of the above table, please scroll down . . .

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

The Table Entries for the Top 10 Target Ports table are selected based on the number of accesses to a particular port for the past days. This data was last updated on August 4, 2005 12:39 am GMT.

Service Name Click to see a more extensive explanation of the significance of accesses to this port.

Port Number Click to see a detailed report of accesses to this port for the past thirty days. Note that all information is sanitized to protect confidentiality and anonymity of participants in this research study

Activity Past Month Plot of the past 30 days in terms of this port's activity expressed as a percentage of the number of accesses recorded for this port as compared to of the total number of accesses our database has recorded for this day for all ports. 30% is full scale. Left to right goes from most recent to least recent

Green means less than 30%. Yellow means the percentage has exceeded 30%. (Over.) Red means that it has exceeded 50%. (Way over.)

These "tiny" plots are designed so that you can quickly get an idea of how much activity each port has had during the past month. Click on the graph to see a detailed report for the same period.

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions

Strengthening Our Infrastructure and Public Safety

Network Analysis

As of Wed Jul 27 03:22:57 2005 UTC

Summary Information | Participant Data

Home | Top 10 Attackers | Top 10 Targets | **Top 10 Targeted**

The **Top 10 Targeted** list shows the top 10 external entities (e.g., other academic institutions, government, military, private sector organizations) that have been probed by the institutions participating in the study.

IP Address	Host Name
45.944.286.227 $^{4}/_{1}$	925-181.274.18.usnet.mil
49.235.13.0	adsl-69-225-127-0.dsl.sndg02.pacbell.net
161.244.76.179	
173.134.20.44	
19.73.161.55	55.denver-04-05rs.co.dial-access.att.net
159.134.137.49	159-134-137-49.as1.srl.dublin.eircom.net
202.103.213.151 $^{20475}/_{7065}$	
41.150.85.22 $^{7185}/_{4234}$	
221.202.129.164 $^{1273605}/_{162890}$	
181.157.102.70	

Legend: IP Address $^{\text{Number of lines implicating this attacker}}$ / Number of attacks at IP address

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

As of Wed Jul 27 03:22:57 2005 UTC

Summary Information | **Participant Data**

Reports Overview | Reports Table | Fightback | Change Profile | Logout

Enter your **Member Login** information below to view your institution's information.

If you would like to participate in this study or would like further information, please contact our Executive Director, Dr. Steffani Burd, at sburd@infosecurityresearch.org or 917.783.8496.

E-mail address

User ID

Submit **Remember me**

'Remember me' will send a non expiring cookie to your browser and you will not have to log in. However, this is a potential security risk. Anybody with access to your PC will be able to log in.

Don't have a User ID? Then **Signup**

User ID reminder

Forget your user ID? Then enter the email address that you used to register. We will send your user ID to this address. Or a note saying that this email address isn't in our database. (Maybe you used a different address to sign up?)

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions

Strengthening Our Infrastructure and Public Safety

Network Analysis

As of Wed Jul 27 03:22:57 2005 UTC

Summary Information | **Participant Data**

Reports Overview | Reports Table | Fightback | Change Profile | Logout

The **Reports Overview** provides a dashboard of network activity for your specific academic institution. This dashboard is based on data uploaded to DShield from your network, and includes the following:

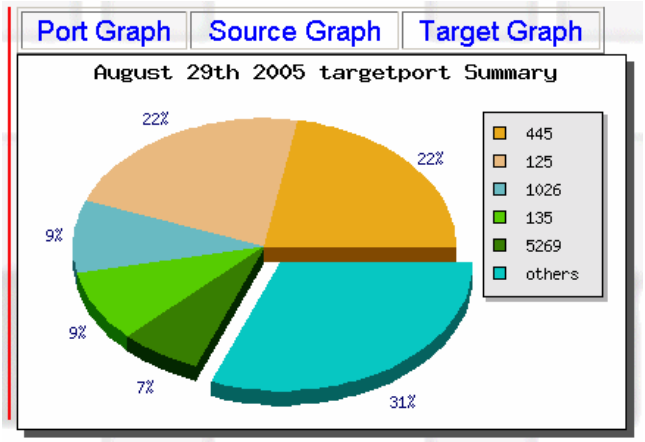
- Date and Time of Attacks
- Attackers (including Source IP and Source Port)
- Targets (including Target IP and Target Port)
- Protocol and Attack Severity Rating

You can "slice" your data by Source, Target, and Target Port. Simply view the graph below, then enter criteria of interest in one of the four fields to its left and press Enter. This will produce tables of data associated with the criteria you selected at the bottom of this page.

When reviewing the tables of data, you can sort the data for easier review. You can sort by Date, Time, Source, Source Port, Target, Target Port, Protocol and Danger simply by clicking on the title at the header of the table.

User ID: 11111
Total lines submitted on 2005-07-14: 2525

Port Graph | Source Graph | Target Graph



Date: Jul-12-2005

Source:

Target:

Target port: 1433

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Color Legend
(Attack Severity based on Target Port):

High	Medium	Low	Possible Firewall Misconfiguration

Not all ports are assigned a 'danger level'. Unassigned ports are represented by an empty white circle (○). Currently showing lines 0 through 20.

Date	Time	Source	Source Port	Target	Target Port	Protocol	Danger
2005-07-11	00:35:04	012.044.103.068	1035	010.000.000.051	53	6	●
2005-07-11	00:35:06	012.044.103.068	1035	010.000.000.051	53	6	●
2005-07-11	00:35:12	012.044.103.068	1035	010.000.000.051	53	6	●
2005-07-11	00:35:24	012.044.103.068	1047	010.000.000.051	53	6	●
2005-07-11	00:35:27	012.044.103.068	1047	010.000.000.051	53	6	●
2005-07-11	00:35:33	012.044.103.068	1047	010.000.000.051	53	6	●
2005-07-11	00:35:45	012.044.103.068	1052	010.000.000.051	53	6	●
2005-07-11	00:35:54	012.044.103.068	1052	010.000.000.051	53	6	●
2005-07-11	00:41:10	012.044.103.068	1164	010.000.000.051	53	6	●
2005-07-11	00:41:13	012.044.103.068	1164	010.000.000.051	53	6	●

Next Page

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Information Security in Academic Institutions

Strengthening Our Infrastructure and Public Safety

Network Analysis

As of Wed Jul 27 03:22:57 2005 UTC

Summary Information | **Participant Data**

Reports Overview | **Reports Table** | Fightback | Change Profile | Logout

The **Reports Table** provides another way of viewing network activity at your specific academic institution. This table is based on data uploaded to DShield from your network, and allows you to filter and sort data in a number of ways.

Specify the report you would like using the pull-down menus for the Y and X axes in the table below. You can then drill-down within the table as you would like.

Example: View attacks on your institution's Target Ports from a Source IP for September 9
1. Go to the Date pull-down menu and select "Sept-9-2005";
2. Go to the Y axis pull-down menu and specify "targetport";
3. Go to the X axis pull-down and select "source".

Date: Jul-11-2005

Lines: 3374

Limit: 20 (lines and columns with less hits are not shown)

Submit

732503	source	012.044.103.068	061.235.154.101	065.173.218.105	083.202.133.051	210.021.230.002
targetport	totals	509	183	89	75	56
53	1765	509			75	37
49153	304					19
445	267					
1433	185					
1026	185		95			
139	136					
1027	115		88			
5269	89			89		
37852	68					
135	52					
500	40					
137	33					
113	24					

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

As of Wed Jul 27 03:22:57 2005 UTC

Summary Information | **Participant Data**

Reports Overview | Reports Table | **Fightback** | Change Profile | Logout

The **Fightback** program is sponsored by DShield.org to help users to fight back against attackers.

You have to sign up for 'Fightback'. DShield will not forward any of your log submissions unless you agree to by using the fightback option.

The user that submitted the log report will be copied on all correspondence. The ISP will receive all relevant log excerpts and we will include the e-mail address registered with DShield.org, in order to allow the ISP to contact the victim directly.

To sign up for the 'FightBack' program, go to the login page, log in and then check the 'FightBack' box. We'll do the rest.

For more information, contact fightback@dshield.org

User ID:11111
Total Fightback Messages Sent:3

This summary only shows fightback messages that included one of your logs as a sample. It is likely that we send messages to other IPs you submitted. However, we may have included some other submitters log as a sample

Reply Column: '?/N' - no reply, 'A' - auto reply, 'Y' - personalized reply, 'B' - bounced

☐ Only show personalized replies Submit Query

Currently showing lines 0 through 20

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Next Page

Report Date	E-mail	Fightback Sent	Source IP	View	Reply
2003-02-27 11:14:20	abusers@rr.com	2003-02-27 06:45:26	066.027.145.002	View	N
2002-12-30 16:44:53	Joe_Smith@McGroom.com	2002-12-30 16:44:53	198.045.019.020	View	Y
2001-10-23 08:01:58	abuse@rogers.home.net	2001-10-24 05:02:02	24.101.97.124	View	A

Next Page

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

As of Wed Jul 27 03:22:57 2005 UTC

Summary Information | **Participant Data**

Reports Overview | Reports Table | Fightback | **Change Profile** | Logout

Change Profile enables you to modify attributes related to your participation in the study (e.g., email address, name, subscription to FightBack).

Account created: N/A
Account last modified: Jul 12th 2005
Time Check: Last check: . Offset: 0 seconds.

Email Address DEMO@DSHIELD.ORG

Name DShield Demo Account - Do Not Change

Time Zone: GMT/UTC If you don't specify a time zone when submitting a report, this time zone will be used.

PGP Public Key (optional. Ignore if you don't know what PGP is)

Feedback	☑	(if you check this box, you will receive a brief e-mail response whenever you submit a log excerpt)
FightBack	☐	(**IMPORTANT!**If you check this box, we may forward selected reports you submit to ISPs where the attack originated. **WE WILL INCLUDE YOUR E-MAIL ADDRESS AND COMPLETE LOG EXCERPT!** You have to verify your time zone setting to participate!
Daily Summary Report	Text E-Mail	This will enable a daily summary of all your reports from the prior day.

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Contact E-Mail:	DEMO@DSHIELD.ORG	
Time Check	(one ip per line) 69.17.4.100	In order to participate in fightback, we need to know if your time zone is set correctly. We do recommend checking it at least once a month. You may either do it at your pace by visiting our time check page. However, if your web client is not behind your firewall (e.g. if you use a tarpit to report data, or if you are using a proxy server), the time check page will not work. If you would like us to send "time check pings" without you having to worry about, enter your IP address to the right. (DO NOT USE if you are on a dynamic IP address). These pings will be send once a week.

Submit

The Following Information is Voluntary:

We would like to understand better who is submitting data to DShield. We hope, the data you provide below will help us answer some of these questions:

- Do home users see different attack than business users?
- Do some firewall packages miss certain attacks?
- Does the number of attacks only dpend on the number of IP addresses a firewall covers, or does it also depend on the number of client computers on the network it protects?

We will not release any personalized information. However, we may use the information to compile special reports. For example, we could in the future compile a report of attacks seen in certain industries, or differences in reports submitted by home users vs. business users. We may also offer customized reports, that compare your reports to others with similar profile.

Are you reporting for a Business or Personal system?	Personal	
Where are you located (Country)	United States	Massachusetts
Are you reporting data from a firewall which protects a network or are you reporting data collected by individual hosts?	N/A	
Is your IP address static or dynamic?	N/A	
For how many hosts are your reporting? If you are sending reports from a network firewall, indicate how many hosts are on this	N/A	

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

network.

How many IP addresses are you assigned at any given time? N/A

What firewall/IDS are you using (include version number

What Operating Systems are you using?

What kind of internet connection are you using? Dialup

If you are reporting for a business, What industry are you part of:

How many people are employed by your company N/A

Any other notes/remarks we may find useful:

Submit

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.