

Transnational Criminal Internet Activity in Academic Institutions: Assessing the Issues and Developing Solutions for Policy and Practice

Steffani Burd, Ph.D., Matthew Haschak, Scott Cherkin
Information Security in Academic Institutions (ISAI)
225 East 85th Street, Suite 301
New York, NY 10028 USA

Abstract- Transnational criminal activity conducted via the Internet is an emerging area of concern for public safety and security. Incidents include identity theft, denial-of-service attacks, fraud and infiltration of government and private organizations. Increasingly, these incidents are propagated by computers infected by malicious software, creating a thriving black market for organized criminals, foreign nationals and terrorists. Adverse consequences include compromised private data and intellectual property, substantial financial losses, funding of criminal and terrorist activities, and potential compromise of critical infrastructure and national security.

As targets in private and government sectors improve protection of their information assets and infrastructure, perpetrators are shifting to softer targets. America's colleges and universities are particularly attractive due to their relatively open networks, significant computing power, diverse users, abundant private information and intellectual property, and links to government, military and research institutions. While academia's networks are generally considered more vulnerable to transnational criminal Internet activity than other sectors, little research has addressed this issue.

The purpose of this article is three-fold. First, it describes unique characteristics of academic institutions that provide opportunities for transnational criminal Internet activity (e.g., the tension between culture and security, diverse users and access methods, sensitive information, and high-risk activities on academia's networks). Second, it addresses the potential impact of transnational criminal Internet activity in academic institutions, including compromised private data, financial losses, and potential attacks on U.S. critical infrastructure. Third, this article describes how changes in policy, use of information from a variety of sources, and application of empirical data and a proposed 'roadmap' may help combat this emerging threat to public safety and security.

I. INTRODUCTION

Transnational criminal activity conducted via the Internet is an emerging area of concern for public safety and security. Incidents include identity theft, denial-of-service attacks, fraud and infiltration of government and private organizations. Increasingly, these incidents are propagated by computers infected by malicious software, creating a

thriving black market for organized criminals, foreign nationals and terrorists. Adverse consequences include compromised private data and intellectual property,

substantial financial losses, funding of criminal and terrorist activities, and potential compromise of critical infrastructure and national security.

As targets in private and government sectors improve protection of their information assets and infrastructure, perpetrators are shifting to softer targets. America's colleges and universities are particularly attractive due to their relatively open networks, significant computing power, diverse users, abundant private information and intellectual property, and links to government, military and research institutions. Although academia's networks are generally considered more vulnerable to transnational criminal Internet activity than other sectors, few data-based recommendations for policy and practice have been developed to date.

II. INFORMATION SECURITY IN ACADEMIC INSTITUTIONS

"College and university systems are a natural target for hackers. "They are large systems, often include public-use labs, and so the identity of a computer cracker can often be easily concealed within the system" [1]. Due to the unique characteristics described below, academic institutions may be disproportionately vulnerable to transnational criminal activity.

Tension between culture and security. Inherent tension exists between the academic culture and security requirements. In the private sector, company policy dictates that computers and intellectual property belong to the organization, and employees typically sign a form acknowledging this policy, thereby accepting limited functionality. The culture of academia, conversely, is built on openness, free speech, learning, information sharing and experimentation. Any attempt to limit this culture may be met with a backlash from students, faculty, staff, and university executives.

Diverse users and access methods. In an academic environment, the network is accessed by many users with different ideas, responsibilities, and access methods. Users include students and faculty on-campus (residence halls, classes, computer centers), students and faculty off-campus (remote access, sharing access), and IT staff and systems administrators (onsite and remote administration). Systems

administrators face an extraordinarily un-standardized network environment. For example, students in residence halls are typically first- and second-year students with a turnover rate of 50% per year [2].

Sensitive information. Universities house private information about faculty and students including social security number, date of birth, credit card details, driver’s license number, financial and information, and grades. In addition, academic institutions have been at the forefront of research and development efforts for most technology innovations in the country. In some cases, this intellectual property is strictly governed by security policies with the federal government, as they share information with the Defense Department (DoD), Department of Homeland Security (DHS) and Defense Advanced Research Projects Agency (DARPA). Nonetheless, huge gaps endanger the security of personal and intellectual information.

High-risk activities on academia’s networks. A critical attribute of information security in academic institutions is the high-risk activities on academic institutions’ networks, including peer-to-peer (P2P) networking, instant messaging (IM), and e-learning. Innovations in sharing information have created some of the most severe security and privacy vulnerabilities, and universities are particularly at risk due to their open cultures. The ramifications of this openness are detailed by the House of Representatives Committee on Government Reform, in which the committee discovered that via Kazaa, private information residing on users computers was readily available, including completed 1040s, military records, a living will, personal inbox, and the narcotics inventory on a Naval ship [3].

Inadequate sponsorship and resources. Academic institutions face a variety of challenges in maintaining information security at their institutions. According to a several-year study of information security in academic institutions [4], the two most widely cited high-impact challenges relate specifically to the academic environment: privacy concerns and academic freedom. Additionally, as illustrated in Fig. 1 below, of the top ten high-impact challenges, roughly two-thirds related directly to cultural issues, such as executive-level support of initiatives, executive-level awareness of issues, resistance to security measures, and insufficient awareness of information security issues. This dearth of support and awareness is clearly reflected in inadequate resource allocation. For example, according to this study and also illustrated in Fig. 1 below, over half of the survey participants do not employ a full-time Information Security Officer or person with similar responsibility and over half have zero full-time staff

Fig. 1. Top 10 challenges and number of full-time information security staff

members dedicated to information security. Further, over half of these participants indicated that the consequences for violating their institution’s policy over the past 12 months are either inconsistent or nonexistent.

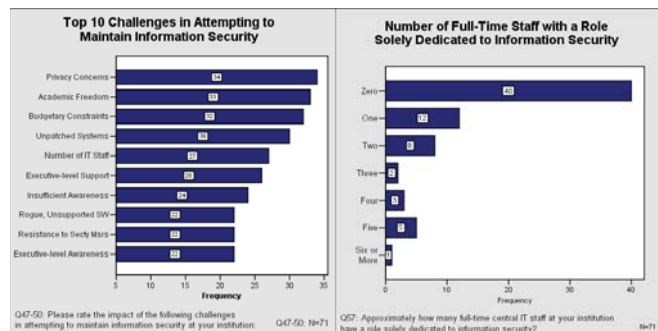
Increasing vulnerability of academic sector. The gap between academia and other sectors will continue to widen in the future, unless remediating actions are taken. The private and government sectors are improving their information security posture in response to laws and regulations such as Sarbanes Oxley (SOX), Health Insurance Portability Accountability Act (HIPAA), and Federal Information Security Management Act (FISMA). While some divisions of academic institutions may be impacted, no overall mandates are driving improvements academic institutions. Perpetrators of transnational criminal activity, such as organized and petty criminals, hackers, terrorists and experimenters are bound to exploit this emerging gap and the associated opportunity to execute their illicit Internet activities.

III. TRANSNATIONAL CRIMINAL ACTIVITY IN ACADEMIC INSTITUTIONS

America’s colleges and universities experience a broad range of information security incidents, as described briefly in the following paragraphs.

A. Types of Incidents in Academic Institutions

Hacking. Hacking has become a serious problem on university networks and may originate from “inside” (e.g., students, staff, or faculty) or the “outside” (e.g., hackers, terrorists, organized criminals). Those with malicious intent can exploit academic institutions’ vulnerabilities with little risk of detection. In an empirical assessment of two academic institutions’ network activity [4], approximately 2 million attack attempts violating their information security policy were identified in just four months. Approximately half of these attempted attacks involved international entities. Specifically, as illustrated in Fig. 2 below, of the 1,760,083 inbound attack attempts, 176 countries were associated with 88% of these attempts. Of the 82,777 outbound attack attempts, 89 countries were involved in 88% of these attempts.



Country	# Attacks	% Total	Country	# Attacks	% Total
United States	794,839	40%	United States	53,267	57%
Republic of Korea	298,986	15%	Denmark	6,578	7%
China	243,243	12%	China	5,033	5%
Netherlands	142,194	7%	Germany	4,767	5%
Canada	90,826	4%	United Kingdom	4,239	4%
Taiwan	49,356	2%	Malaysia	4,155	4%
United Kingdom	47,600	2%	Switzerland	1,844	2%
Germany	37,122	2%	Canada	1,252	1%
Sweden	34,048	2%	Unknown	916	1%
Poland	21,869	1%	Japan	726	1%

Fig. 2. Countries associated with inbound and outbound attack attempts

Espionage. Espionage and information gathering also occurs via academic institutions. The recent Stakkato incident, in which several academic and research institutions, military entities and NASA were breached by a Swedish teenager [5] demonstrates the vulnerabilities of academic institutions and critical infrastructure. Academic institutions may be particularly vulnerable to these activities. Student organizations supporting extremist agendas are increasing apace, particularly in Europe and the U.S. Table 1 below presents examples of incidents obtained from just one participant's log files on a Sunday evening from the Higher Education Network Analysis (HENA) tool. While tracking transnational criminal activity was not in the study's scope, a significant number of perpetrators were identified probing the HENA platform.

Botnets. Because of their open nature, academic networks may be disproportionately vulnerable to bot infections. In "What You Need To Know About Botnets!" [6], the Multi-State Information Sharing Analysis Center (MS-ISAC) provided three examples of botnet infections and noted that all three botnet controllers were traced back to universities. 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. In a subsequent webcast by the MS-ISAC in conjunction with the Department of Homeland Security's US-CERT, three groups were identified as most vulnerable to botnets: 1) universities and schools; 2) home broadband users; and 3) the mobile workforce. As an IT

TABLE 1.
ONE STUDY PARTICIPANT'S LOG FILES OF ESPIONAGE-RELATED ATTEMPTS

Incident	Source
An attempt from China to access a Trojan program	An account in Beijing, China – CNCGROUP Heilongjiang province network.
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
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)
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

TABLE 2:
ACADEMIC INSTITUTIONS' REPORTED BREACHES OVER PAST SIX-MONTHS

Date	Made Public	Organization	Number
Aug. 1, 2006		Wichita State University	2,000
Aug. 1, 2006		Wichita State University	40
Aug. 15, 2006		University of Kentucky	630
Aug. 15, 2006		University of Kentucky	80
Aug. 26, 2006		University of South Carolina	6,000
Sept. 1, 2006		Virginia Commonwealth University	2,100
Sept. 8, 2006		University of Minnesota	13,084
Sept. 20, 2006		Berry College (via consultant)	2,093
Sept. 22, 2006		Purdue University College of Science	2,482
Sept. 22, 2006		University of Colorado-Boulder	1,372
Sept. 29, 2006		University of Iowa	14,500
Sept. ??, 2006		Adams State College	184
Oct. 12, 2006		University of Texas at Arlington	2,500
Oct. 19, 2006		University of Minnesota / Spain	200
Nov. 1, 2006		U.S. Army Cadet Command	4,600
Nov. 3, 2006		University of Virginia	632
Nov. 17, 2006		Jefferson College of Health Sciences	143
Dec. 5, 2006		Nassau Community College	21,000
Dec. 9, 2006		Virginia Commonwealth University	561
Dec. 12, 2006		University of California - Los Angeles	800,000
Dec. 12, 2006		University of Texas – Dallas	6,000
Dec. 15, 2006		University of Colorado – Boulder	17,500
Dec. 19, 2006		Mississippi State University	2,400
Dec. 22, 2006		Texas Woman's University	15,000
Dec. 27, 2006		Montana State University	259
Jan. 11, 2007		University of Idaho	70,000

Director of a large public university stated, "We have botnets all over campus, and I'm not sure anyone wants to know that's really the case," [7].

Data compromise. Academic institutions may also serve as an effective gateway to sensitive targets with which they share information, including government and critical infrastructure entities. Terrorist, organized criminal, and espionage groups have opportunity to exploit these weaknesses and cause harm with attacks ranging from distributed-denial-of-service attacks to viruses with damaging payloads. Indeed, incidents involving the compromise of personal data from academic institutions are widespread. For example, Table 2 below lists private data compromises reported in just the past six months [8]:

B. Impact on Public Safety, Policy and Practice

Increasingly frequent and severe incidents are occurring in academic institutions, highlighting that they may not be adequately prepared to defend against attacks or detect attacks emanating from their own networks. Because network security is only as strong as the weakest link in the chain, it is incumbent on policy makers to identify and quantify the risks, help prevent incidents, and mitigate their impact after occurrence. Below is a list of potential impacts of transnational criminal activity in academic institutions on public safety, policy and practice.

Compromised private data. As indicated in the previous section, incidents involving the theft of data belonging to students, applicants, faculty, and staff are increasing at an alarming rate. For example, the names, SSNs, birth dates, home addresses, and contact information

of 800,000 individuals at the University of California Los Angeles (including current and former students, current and former faculty and staff, parents of financial aid applicants, and student applicants) were compromised when hackers gained access to a database in December 2006 [9]. Personal information for 70,000 alumni, donors, employees, and students from the University of Idaho were reported compromised when three desktop computers were stolen from the Advancement Services Office, and 331,000 individuals may have been exposed [10]. This brings the total breaches reported by colleges and universities in less than six months to 985,360 – almost 10% of quantified breaches across all sectors. This percentage is particularly staggering when one considers the volume of records routinely handled by other sectors such as banking and finance, healthcare and the government.

Financial losses. A more gradual, but certainly crippling, effect on public safety and security arises from financial losses incurred. For example, the international organization Shadowcrew traded in over 1.7 million stolen credit card numbers and incurred over \$4 million total losses before it was closed down in October 2004 [11]. According to the FTC, the economy absorbed \$52 billion in losses resulting from goods and services purchased with fraudulently obtained personal identification in 2004 [12]. All together, 9.3 million people suffering from identity theft in 2004, requiring an average of 28 hours of work to rectify the situation [13]. Beyond fraud and identity theft, financial losses result from destruction from worms and viruses. Again, this issue is of particular concerns for academic institutions: an informal survey of nineteen research universities 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 [14].

Attack on the U.S. critical infrastructure. Perhaps the most frightening incident in which networks' 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 many times. In October 2002, a DDOS attack was executed on the thirteen "root servers" which provide the basis for almost all Internet communication globally. Fortunately, safeguards built in to the system prevented slowdowns and outages, but a more prolonged or extensive attack could have caused serious damage [15]. 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. On May 5, 2006, 20-year-old Christopher Maxwell pled guilty to launching a bot network attack that compromised computers at a Seattle hospital and several universities using 13,000 distributed computers to earn about \$100,000 [16].

IV. RECOMMENDATIONS FOR POLICY AND PRACTICE

As transnational criminal activity via the Internet burgeons and perpetrators move from better-protected private and government entities to softer targets, academic institutions may represent a disproportionate vulnerability to public safety. This concern is compounded by the increasing inter-connectedness with government, military, private sector, and critical infrastructure entities. Since peer-to-peer file-sharing programs became popular in the late 1990s, college campuses have been perceived as a Wild West of profligate bandwidth use and lax security—a perfect digital haven for cybercriminals and ideal incubator for transnational criminal activities. These concerns need to be addressed with data-based recommendations for policy and practice. Following is a brief review of current policy and practice, with recommendations for addressing the issues facing academic institutions and, ultimately, public safety and security.

A. Policy

Transnational cybercrime policy. Transnational cybercrime policy is currently fragmented internationally, due to differing governments' understanding of the threats, conflicting laws within sovereign countries, and the necessity of a coordinated global effort. For example, the Convention to the Senate submitted by President Bush November 17, 2003 has faced a number of challenges. "The United States and the Commission clearly agree on many of the key principles . . . However, we believe that additional discussion is needed before we can reach broad international consensus on other core issues" [17]. The G-8's "Recommendations for Enhancing the Legal Framework to Prevent Terrorist Attacks" [18] laid out a call to the international community to join together to fight transnational crime and terrorism. Although these recommendations provide quality thought leadership, they face significant challenges in practice due to fragmented international laws. Until effective transnational cybercrime policy is established and implemented, academic institutions must rely upon U.S.-based policy and their own methods of protecting information assets and associated infrastructure.

U.S. Policy, Laws and Regulations. The U.S. government is actively addressing cybercrime and privacy issues through strategies, laws and regulations at the federal, state and local levels. For example, the President's National Strategy to Secure Cyberspace [19] Actions and Recommendations 1-7 encourage corporations to participate in industry-wide Information Sharing Analysis Centers (ISACs) that share information on technology security threats and best practices. Colleges and universities are also encouraged to consider establishing: 1) one or more ISACs to deal with cyber attacks and vulnerabilities; and 2) an on-call point-of-contact to Internet service providers and law enforcement officials, in the event that the institution's networks are discovered to be launching cyber attacks.

Federal laws and regulations are also actively addressing cybercrime through Sarbanes-Oxley, the Gramm-Leach Bliley Act, Health Insurance Portability Accountability Act, and Payment Card Industry Data Security Standards. State-level laws, such as California's SB1386, are also markedly improving accountability for reporting potential breaches. However, these policies, laws and regulations do not specifically address academic institutions.

Without legal or regulatory pressures upon the institutions, accountability at the senior executive and board of director levels will continue to founder and critical resources will not be provided. Further, as other sectors improve their protection, the potential for transnational criminal Internet activity in America's colleges and universities will continue to increase at a marked pace.

B. Practice

Organizations. The U.S. government has been creating organizations to detect and prevent cybercrime as well as developing robust research and thought leadership that is disseminated through the country. The Multi-State Information Sharing Analysis Center (MS-ISAC) is a focal point for gathering information on cyber threats to critical infrastructure among all 50 US States. It has also highlighted the potentially disproportionate vulnerability that academic institutions pose in facilitating cybercriminal activity such as botnets. The REN-ISAC (Research and Education Networking Information Sharing and Analysis), one of the ISACs established to address critical infrastructure protection, focuses on analysis, dissemination and early warning systems. The Justice Department's Computer Crime and Intellectual Property Section (CCIPS) is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. The Computer Crime Initiative (www.cybercrime.gov) is a comprehensive program designed to combat electronic penetrations, data theft, and cyberattacks on critical information systems. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.

Cybersecurity in academic institutions is also addressed by non-government organizations. ECAR, the Educause Center for Applied Research, conducts high-quality studies that explore issues of academic institutions. Several research studies, particularly "Information Technology Security: Governance, strategy, and practice in higher education" [21] provide excellent insight into cybersecurity issues of academic institutions. The EDUCAUSE/Internet2 Security Task Force is accomplishing great strides in developing next generation networking standards and protocols that embed security (i.e. IPv6).

A critical and, to date, under-utilized recommendation for improving information security in academic institutions is to leverage the funding through organizations such as the National Science Foundation. Using a method similar to

that employed by the National Security Agency in establishing and accrediting its NIETP program, the NSF could require a demonstrated baseline level of information security prior to granting funding for research.

C. Next Steps: A Roadmap for Improving Information Security in Academic Institutions

A number of data-based and focused activities, or a "roadmap", may be implemented to reduce the frequency and impact of information security incidents in academic institutions. This roadmap provides practical recommendations and 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 and executive-level support;
3. Tighten security policy;
4. Establish mandatory training;
5. Automate and institute processes; and
6. Empirically assess activity.

Each of these steps, as illustrated in Fig. 3 below, is described in the following paragraphs.

Recommendation #1: Classify Information Assets.

Asset classification involves locating information assets and their associated systems, then classifying 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, but it is a critical step to improving protection of the institution's information and infrastructure.

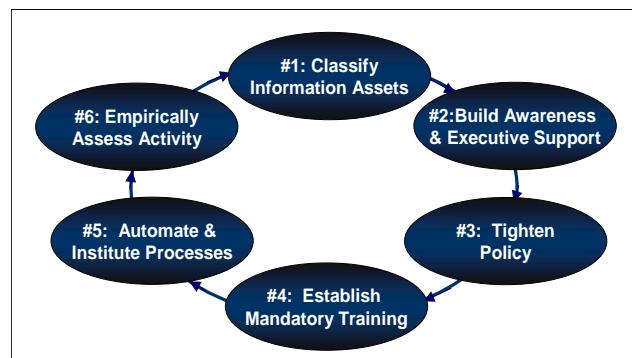


Fig. 3. Six steps in recommended information security roadmap

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;
3. Document these assets to build senior administration's awareness and to identify appropriate information security controls.

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.

Recommendation #2: Build Awareness and Executive-Level Support.

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 goals of building awareness for all of these end users are simply that;

a) they are aware of how they may affect information security;

b) they know how to respond if they suspect an incident;

and c) information security professionals within the institutions have sufficient support to accomplish their objectives. 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. Building executive-level support of information security can be particularly difficult, as it is often perceived as a threat to the culture of openness and academic freedom and a source of cost and tension. This difficulty is compounded by the current lack of accountability for breaches and compromises.

Building awareness and executive-level support 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 of this recommendation 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.

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. A 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 meaningful and consistently enforced provide incentive for end users' compliance. Tightening the policy is particularly effective in when implemented conjunction with informing end users 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 perspectives, 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.

Four steps are involved in this recommendation:

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 endusers every semester prior to granting access to the network.

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.

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.

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 antispyware 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.
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 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

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 activities. 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.

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.

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).

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.

Five steps are involved in empirically assessing activity:

1. Prioritize the most important controls, processes, and measures to be assessed, based on asset classification.
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 developing a remediation plan.
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 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.

D. Future Research.

Policy development at transnational, national, state, local and university levels should be informed by objective, independent data demonstrating the critical issues and their ramifications. Empirical assessment of actual activity, coupled with data-based recommendations for policy and practice, is needed to spur development of policy and practice for these various stakeholders in the public's safety and security. Future research should focus on the following areas:

Empirically assess transnational criminal activity in academic institutions. Meaningful empirical assessment of transnational criminal activity in academic institutions is based on two elements: 1) measuring types and levels of transnational criminal activity in academic institutions and 2) measuring types and levels of transnational criminal activity in other organizations (e.g., private sector,

government). Once transnational criminal activity for academia and other organizations outside academia have been empirically assessed, a data-driven assessment of whether academic institutions are disproportionately vulnerable to transnational crime can be derived.

Develop cost-effective, efficient tools to detect and prevent different types of transnational crime. A variety of tools to detect and prevent specific components of transnational criminal activity are currently being developed by researchers. However, they have not been integrated for a holistic perspective of transnational criminal activity.

Establish collaboration between at-risk institutions to identify and prevent transnational crime. Once tools to detect specific components of transnational criminal activity are developed, collaboration amongst at-risk academic institutions can be established. This collaboration, both within countries and across national borders, can be accomplished via ad hoc cooperation and multinational task forces. However, due care must be taken to ensure – particularly with academic institutions – to ensure the freedoms of science, research and teaching.

V. CONCLUSION

In conclusion, 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.

Although academia's networks are generally considered more vulnerable to transnational criminal Internet activity than other sectors, few data-based recommendations for policy and practice have been developed to date. It is recommended that, while effective transnational cybercrime and relevant U.S.-based laws and regulations are being developed, academic institutions implement a five-step roadmap for proactively establishing a baseline level of information security. 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 may suffer as a result.

- [1] M. Delio, "College: A cracker's best friend," *Wired News*, February 28, 2001.
- [2] S. Burd and S. Cherkin, "The Impact of Information Security in Academic Institutions on Public Safety and Security," *Presentation to the ASIS International Organization in New York City*, June 6, 2005.
- [3] House of Representatives Committee on Government Reform, "Committee staff test using Kazaa file-sharing program," April 2003.
- [4] S. Burd, "Impact of Information Security in Academic Institutions on Public Safety and Security: Assessing the Impact and Developing Solutions for Policy and Practice," *National Institute of Justice Grant NCJ 215953*, October 2006. www.ncjrs.gov/pdffiles1/nij/grants/215953.pdf
- [5] D. Sieberg, "Report: Hacker infiltrated government computers," *CNN.com*, May 10, 2005. <http://www.cnn.com/2005/TECH/05/10/govt.computer.hacker/>
- [6] MS-ISAC, "What You Need To Know About Botnets!," *Webcast*, Nov 2004. <http://whitepapers.silicon.com/0,39024759,60125590p-39001181q,00.htm>
- [7] G. Goth, "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>
- [8] Privacy Rights Clearinghouse, "A Chronology of Data Breaches," January 17, 2006. www.privacyrights.org
- [9] E. Chickowski, "UCLA notifies 800,000 of personal data hack," *SC Magazine*, December 12, 2006. www.scmagazine.com/us/news/article/609452/
- [10] S. Dininny, "University of Idaho issues data-theft alert," *The Seattle Times*, January 12, 2007. www.seattletimes.nwsourc.com/html/localnews/2003521525_idtheft12e.html
- [11] J. McCormick and D. Gage, "Shadowcrew: Web Mobs," *Baseline*, March 7, 2005. www.baselinemag.com/article2/0,1397,1774393,00.asp
- [12] United States Office of the Attorney General, "ChoicePoint To Notify Vermont Consumers Affected by Security Breach," February 24, 2005. <http://www.atg.state.vt.us/display.php?pubsec=4&curdoc=881>
- [13] United States Senate, "Statement of Senatory Patrick Leahy," April 2005. www.senate.gov/~leahy/press/200504/041305.html
- [14] A. Foster, "Colleges brace for the next worm," *The Chronicle of Higher Education: Information Technology*, vol. 50, Issue 28, Page A29. March 19, 2004.
- [15] Anonymous, "Net suffers biggest DDoS attack," *FairfaxDigital*, October 23 2002. <http://www.smh.com.au/articles/2002/10/23/1034561535264.html>
- [16] United States Department of Justice, "California Man Pleads Guilty in "Botnet" Attack That Impacted Seattle Hospital and Defense Department." May 4, 2006. <http://www.usdoj.gov/criminal/cybercrime/maxwellPlea.htm>
- [17] United States White House, "Message to the Senate of the United States," November 17, 2003. www.whitehouse.gov/news/releases/2003/11/20031117-11.html
- [18] Council of Europe ETS No. 185, "Convention on Cybercrime," November 23, 2001.
- [19] United States White House, "National Strategy to Secure Cyberspace," 2003. <http://www.whitehouse.gov/pcipb>
- [20] Institute for Security Technology Studies, "Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report," 2004.
- [21] J.B. Caruso, "Information Technology Security: Governance, Strategy, and Practice in Higher Education," *Educause*, September 2003. <http://www.educause.edu/ir/library/pdf/ERS0305/ekf0305.pdf> <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>