



Information Technology Security at MIT

Judith A. Pirani, Sheep Pond Associates and ECAR
John Voloudakis, Cap Gemini Ernst & Young

ECAR Case Study 9, 2003

Case Study from the
EDUCAUSE Center for Applied Research



EDUCAUSE

4772 Walnut Street, Suite 206
Boulder, Colorado 80301
www.educause.edu/ecar/

Information Technology Security at MIT



EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

The mission of the EDUCAUSE Center for Applied Research is to foster better decision making by conducting and disseminating research and analysis about the role and implications of information technology in higher education. ECAR will systematically address many of the challenges brought more sharply into focus by information technologies.

Copyright 2003 EDUCAUSE. All rights reserved. This ECAR case study is proprietary and intended for use only by subscribers and those who have purchased this study. Reproduction, or distribution of ECAR case studies to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior written permission is granted by EDUCAUSE. Requests for permission to reprint or distribute should be sent to ecar@educause.edu.

Information Technology Security at MIT

Preface

The EDUCAUSE Center for Applied Research (ECAR) produces research to promote effective decisions regarding the selection, development, deployment, management, socialization, and use of information technologies in higher education. ECAR research includes

- ◆ research bulletins—short summary analyses of key information technology (IT) issues;
- ◆ research studies—in-depth applied research on complex and consequential technologies and practices; and
- ◆ case studies—institution-specific reports designed to exemplify important themes, trends, and experiences in the management of IT investments and activities.

In its most recent research, ECAR has investigated the state of security practice in higher education and reported its findings in *Information Technology Security: Governance, Strategy, and Practice in Higher Education*.¹ This research was conducted by a team of researchers from ECAR and from Cap Gemini Ernst & Young. It was undertaken in five phases, described below.

Literature Review

A review of the relevant literature helped us define the study's major elements and create a working set of hypotheses.

Consultation

Researchers consulted with higher education security and policy leaders to identify and validate the most interesting research questions and hypotheses for framing the construction of a quantitative survey instrument. Those consulted include Mark Bruhn of Indiana University, Ken Klingenstein of Internet2, Mark Luker and Rodney Peterson of EDUCAUSE, Dan Updegrave of The University of Texas at Austin, and Gordon Wishon of the University of Notre Dame. The resulting research framework formed the basis for creation of an online survey.

Online Survey

ECAR conducted an online survey of more than 1,600 colleges and universities to establish the current state of computer security practices in higher education. More than 400 colleges and universities responded to the survey.²

Telephone Interviews

Researchers conducted intensive telephone interviews with more than 30 IT and functional executives, managers, and security officers at more than 20 selected EDUCAUSE institutions.

Case Studies

Researchers conducted in-depth studies of institutions regarding the state of their security efforts. To adequately capture the depth and breadth of practice, ECAR researchers chose both public and private institutions that varied in size and mission. We undertook the present case study to draw on the direct experience of those able to provide insights into policies, technologies, and practices that have worked well and those that haven't. We assume readers of this case study will also read the primary study, which provides a general context for the individual case study findings.

ECAR wishes to thank the leadership of the Massachusetts Institute of Technology for sharing their time, thoughts, insights, and records with us. In particular, ECAR thanks Michail Bletsas, director of computing at the MIT Media Lab; James Bruce, vice president for information systems; John Curry, executive vice president; Bob Mahoney, team leader, network security; Timothy McGovern, senior project manager of Stop-It; and Jeffrey Schiller, network manager.

Introduction

Managing IT security at MIT poses interesting challenges. MIT's research and academic activities are frequently on the cutting edge of technology, but the university must also protect its computing resources and information assets. The challenge is how to balance the needs of the two. "The conundrum we face is that we are an institution that has administration and administrative needs. We are also a university that engages

in research and the free exchange of ideas," explained Jeffrey Schiller, network manager. "A lot of security technology prohibits new things from happening. The challenge is how to have an open institution with the free exchange of ideas and still provide an institution that is secure."

Unsurprisingly, MIT has developed a unique solution to address this problem. At its heart is the commitment to an open network that does not rely heavily on firewalls. MIT instead focuses its security efforts on centralized authentication and authorization, developing its own solutions in these areas. And despite its robust technological environment, MIT also uses a surprisingly small, two-person department to manage its central security activities. However, its director, Bob Mahoney, has created an institutional grassroots organization of students and departmental staff to augment his central resources and to create campus-wide buy-in for IT security activities. This case study examines how MIT's technical and organizational ingenuity work together to secure the institution's IT assets.

Institution Background

The Massachusetts Institute of Technology is a world-renowned private research university organized into five schools and one college: the Schools of Architecture and Planning; Engineering; Humanities, Arts, and Social Sciences; Management; and Science; and the Whitaker College of Health Sciences and Technology, which operates 27 degree-granting departments, programs, and divisions. In addition, MIT conducted more than \$447 million in sponsored research in fiscal year 2002 and operates several major research labs, including the MIT Artificial Intelligence Lab, the MIT Media Lab, the Research Laboratory of Electronics, and the Whitehead Institute for Biomedical Research. Forty-seven alumni, faculty, researchers, and staff have

won Nobel Prizes. Currently, 10,000 undergraduate and graduate students attend MIT, and the university employs 900 full-time faculty members.

James Bruce, vice president for information systems, manages MIT's central information systems organization, which is organized into five IT processes: discovery, delivery, service, support, and telecommunications and network services. More than 275 employees currently work in the five processes. The institution operates a centrally managed network with two external connections: a 1-Gbps Internet connection and a 640-Mbps Internet2 connection. Some of MIT's research laboratories and other centers manage their own local networks, which are connected to the institutional network, although some may also have their own connectivity to external networks. More than 40,000 devices—mainly a mixture of Unix workstations and Apple Macintosh computers—run on MIT's networks.

MIT's Security Strategy

Bruce explained MIT's IT security philosophy: "This is a university. For us, this means that the network pretty much has to be an open network. And so we pretty much don't believe in firewalls. The enterprise networking environment has no firewalls in it. Some departments will run firewalls—for example, genetic data and things of that nature, and the Lincoln Laboratory, which is part of the MIT environment, has a firewall—but for the most part, since our researchers like to use all sorts of new protocols and other fancy things on the network, trying to build a firewall is a fruitless endeavor. Just as soon as you build one, somebody wants to do something different, and you keep punching holes in it, and after a while it looks like Swiss cheese. So that means for us that the fundamental proposition is that our computers and our applications need to be secure. We focus on security at the individual-machine level. We

worry a lot about operating system security, about the bugs in operating systems, and we focus a lot on ensuring that our applications have appropriate levels of security, so indeed, we know who is making the transaction when the transaction occurs.

"The key mission [of the IT security team] is to protect the ability of the faculty, students, and staff to do their work," he continued. "Computer security is not so much about protecting specific assets. What we are trying to do is to raise the level of security of all our computing assets to keep out intruders, to keep them from doing harm, so the people who do access our assets can go about their business on a regular basis without interruption. I don't stop and think which of my machines I must build a fort around because we have to build a fort around each individual machine anyway. It stands [the notion] on its side to put big doors at the front. This place has many entry doors; this place is porous; it is like a sponge."

The human element plays just as important a role as technology in MIT's security strategy. "We can govern access tightly. We can have as good encryption as possible to the desktop, but yet our vulnerability is from our people," explained John Curry, executive vice president. "MIT's network security team is responsible for the security of the network as a whole: scanning the network, looking for traffic anomalies, or people who have null passwords. However, individuals are responsible for the security of the operating system on their own machines. The network security team will turn off any infected or vulnerable machines during an attack."

Despite its complex technical environment, MIT's philosophy is to provide "as much ubiquity of computing resources in all of our facilities as possible," Bruce said. It applies the same security measures for the administrative users and the residence halls, though bandwidth use is a particular concern in the dorms. The one significant exception

is Lincoln Laboratories, MIT's high-security research facility, which sets its own data security requirements, maintains its own separate ISP and firewall, and operates its own version of MIT's SAP administrative system.

MIT's Security Environment

Given its open-network IT security strategy, MIT focuses its security efforts on protecting individual machines and applications. Central to this strategy is Kerberos, a protocol developed at MIT to allow secure authentication of users to computing resources. Kerberos, and several related applications used for authentication and authorization at MIT, developed out of Project Athena,³ MIT's campus-wide academic computing system. As Athena transitioned from a timeshare to a network computing model in the mid- to late 1980s, MIT recognized the need to provide secure authentication of users in a networked environment. Cliff Neuman, now at the University of Southern California's Information Sciences Institute; Jeff Schiller, currently MIT's network manager; and Jerry Saltzer, a now-retired faculty member, worked to develop an independent authority that certifies that people trying to access a particular resource are indeed who they say they are. This engendered the Kerberos protocol suite, where

- ◆ a user name and password travel across the network in an encrypted DES (data encryption standard) environment (now triple DES);
- ◆ the Kerberos server reviews the user credentials and verifies them to any service provider (for example, another Kerberos-aware application); and
- ◆ the user is authorized to download information to the desktop.⁴

Access, however, is just the first part of the equation. The Kerberos server provides authentication, "but there is nowhere in that environment that says who that person is," explained Bruce. "That is the whole issue of

identity management. It is 'who I am' and then 'what can I do.'" MIT built an application called Roles to provide authorization. Roles stores information on each user's authorized application functions. "It is our way of separating what you have access to from what you can do," said Bruce.

MIT's goal is to "use Kerberos and Roles more and more to secure an application in the environment because it needs to know 'who' and it needs to know 'what,'" Bruce said. Until the mid-1990s, Kerberos was used primarily within the academic computing environment. However, as MIT moved toward a commercial vendor (SAP) for its administrative systems, MIT convinced the vendor to include support for Kerberos in the product's base security module, making Kerberos a key component of MIT's administrative system security as well.

Some members of the community still operate without a Kerberos principal, but MIT is increasing Kerberos use on campus. One means is through the combined use of Kerberos principals and X.509 Web certificates for students, faculty, and staff to access the growing number of Web-accessible self-service tools or place orders on research accounts; another is by eliminating paper whenever possible. "We're twisting the screws a little more," stated Bruce. "Starting last fall, people could change their health insurance benefits only online. You need authentication to do it. When we find a pocket of people who do not [use Kerberos for authentication], we work with them and get them on board." Schiller estimated 99.9 percent penetration with the students and 80 percent penetration with staff. Faculty penetration is just 50 percent; they are the least motivated constituency, and they represent a higher percentage of computer nonusers.

Because of its open network environment, MIT encrypts all administrative data, since "at any point in time, we assume that

50 percent of our subnets are being monitored," Schiller said. To secure Web applications, MIT uses SSL (secure sockets layer) and HTTPS, which, Schiller said, "provide 80 percent of what we need." Users must register MAC (media access control) addresses for all devices attached to MIT's network to obtain IP addresses, so when a user employs a Kerberos principal to log into anything, it goes back to the appropriate RADIUS database and checks to see if the MAC address is there before it assigns the user a DHCP (dynamic host configuration protocol) address. MIT runs a port-managed network for network portions under central information services (IS) control. This provides the network security team with the ability to remotely turn off any port hosting a compromised system.

Its concentrated campus layout and the September 11, 2001, terrorism attacks prompted MIT to reevaluate its business continuity strategy. MIT operates two backup data centers, but their close proximity to the university may mitigate their effectiveness in the event of a major disaster. The institution maintains backup telephone switches. It has redundant network backbones in conjunction with Harvard University and Boston University. But some vulnerability, Curry admitted, "lies within a few key manhole covers."

One activity that MIT performs every summer in conjunction with the city of Cambridge is a simulated emergency scenario. One year, for example, they simulated a chemical spill in the lobby of the primary campus administrative building. The physical exercise enables university and emergency personnel to test their readiness, then the IS department turns it into "a tabletop exercise to determine how areas like HR or accounts receivable would function if they could not go back to work," explained Bruce.

MIT's Security Organization

IT security at MIT is funded out of the general IS budget that Bruce controls and is

paid for by network fees that IS charges to campus departments. The network security team operates within MIT's IS Telecommunications and Network Services Process Group. No particular incident prompted the team's formation about six years ago, just an increasing volume of incidents coupled with team leader Bob Mahoney's general interest in focusing more on security issues. Mahoney reports directly to the head of the telecommunications and network services team, but Jeffrey Schiller, MIT's network manager, provides technical direction for the team.

The network security team is surprisingly small to support a complex research institution. It comprises just two FTEs and a "voucher" employee who conducts vulnerability scanning. Mahoney supplements his full-time resources with a cadre of volunteers and student employees. About six years ago, Mahoney undertook the management of MIT's security mailing list, used to share information about IT security threats and coordinate responses on campus. Initially, volume was low, but its activity grew as the Web gained popularity. Soon Mahoney needed help to manage the list. He received permission to solicit help, and a team of volunteers quickly emerged.

A typical volunteer is a motivated departmental staff member who submits questions to the IT security mailing list and is already helping his or her individual organization with security issues. Members include representatives from the university's research labs and schools. Although these employees are part of the virtual IT security organization and participate in the team's activities, they continue to hold their full-time positions in their school or laboratory; they are paid by and report to these organizations, not central IS.

Successfully managing IT security requires quickly making the security team's members aware of new security issues and vulnerabilities. The security team's mailing

lists provide an effective communication mechanism. Mahoney's team manages two lists with different purposes, which the broader security team also uses. The information list provides details about new issues and vulnerabilities, while the operations list tracks specific incidents and feeds into the central IT organization's case tracking system. Nondisclosure governs information on both lists. Security team members regularly review both the information and operations/incident mailing lists and respond to issues that affect their areas of the institution. Members also attend occasional team meetings and, more importantly, provide a university-wide coalition to assist the security team in presenting security-oriented proposals to the administration.

The volunteer team builds an institutional spirit, "turning the 'us versus them' mentality often seen in the interactions between a central IT security team and departmental users into 'we,'" Schiller stated. Mahoney believes the team is a "win-win for both of us. It is often better to give them [departmental users] access to the information so they can answer their own questions. Volunteers see the activity behind the curtain, generating greater appreciation for our activities."

Mahoney also leverages the readily available supply of campus student workers. Five students, with varying amounts of commitment, currently work for Mahoney on the security team. While many students have significant technical experience coming in, some students just express an overall interest in IT security. Mahoney feels a student's ability to fit into the team is more important than technical expertise. "It is almost like an [emergency medical services] team," he explained. "Everyone you are dealing with is upset in some way, so the students have to work well under pressure."

Inexperienced students initially create Web pages or documentation for the team until they gain IT security expertise.

Sometimes computer science students will train each other, and the full-time staff also provides some training. Students may also complete IT security projects as part of their independent studies. Mahoney is cognizant of the students' special needs, designing projects in stages to plan for lack of student continuity. Student employees are trusted to deal with most IT security issues that arise, although staff members handle some senior administrators' issues and any problems with potential legal ramifications. Overall, Mahoney rates his experience in using student employees as very positive. Students receive training and experience, and Mahoney feels they frequently produce professional-grade work. Several of his student employees continue to work in the security field after graduation. "It works if you can recognize how students differ from the regular staff," Mahoney said. "And you recognize the different pressures under which they operate."

While the network security team addresses security issues related to technology, MIT's Stop-It organization handles people security issues. MIT founded Stop-It in 1992 to address "a growing campus awareness about harassment issues in general, the growing use of a distributed computing environment, and the fact that people could harass others electronically," said Tim McGovern, senior project manager. Two people devote part of their time to Stop-It, which reports to Jim Bruce, vice president of information systems.

Stop-It is "an off-the-record, confidential service," McGovern said. People report their grievances directly to the Stop-It staff, who contact the offender. It is not accusatory. "Our goal is to get people to understand the rules and the impact of their behaviors, and to prevent repeat offenses," McGovern explained. "We are not interested in litigation or disciplinary action unless it is a repeat offender. We want people to stop their actions in a way that is satisfying to all parties."

Most cases involve electronically disagreeable actions, copyright violations, spam e-mail, and occasionally viruses. There is no permanent record except for DMCA (Digital Millennium Copyright Act) complaints. Last year Stop-It handled about 1,500 cases. McGovern estimated that most cases involved disagreeable electronic content, language, and displays. Copyright-related issues constituted approximately one-third of the cases, about 20 percent were spam related, and the remainder were uncategorized.

McGovern said virus issues are not a big part of the Stop-It caseload because the MIT community is quite sophisticated about IT security overall. "People realize the Internet is unprotected, that MIT does not block things from the outside, and that you have to block them at your doorstep," he added. "The people who filter down to me are those who missed all the security announcements and publications from IS and their local system administrators. Most people know to contact the network security team for security-related problems."

But Stop-It does work with the security team in several ways. If Stop-It determines a person's machine is compromised or vulnerable, they move it quickly into the security team's queue. The security team, in turn, will hand off security-awareness-related cases to Stop-It. The Stop-It staff monitors security activity but does not work on specific cases. "We watch the security queue to help our case management," McGovern explained. "It helps determine whether the source of mischief is due to malicious intent or not. For example, we can determine whether a copyright issue stems from a compromised machine."

A Departmental View of IT Security

The network security team's jurisdiction is the centrally managed network, but many individual schools and laboratories maintain

their own networks and deal with IT security issues locally. Requirements for these local networks, especially in the laboratories, differ significantly from the enterprise network's needs. Whereas the central network is relatively static, research groups often adapt their networks more frequently to meet their evolving needs, adding hosts as needed. Research labs experience more freedom than their central IT counterpart. The central IT department follows standards more closely; the laboratories' research nature promotes experimental applications.

One example is MIT's Media Lab, which has 300 people and 1,600 nodes located primarily in one building, plus a small satellite facility. It operates a diverse computing environment: Intel-based PCs predominate, with an increasing number of Apple PowerBook laptops and some Linux and other Unix systems. The Media Lab has its own IT staff of ten full-time employees, eight of whom devote a significant portion of their time to security issues. This staff manages the Media Lab's internal network from the point where it connects to MIT's enterprise network to the desktop. Effectively responding to security incidents is an important function for the Media Lab's IT staff, as Michail Bletsas, the lab's director of computing, explained. "[Central IT's] understanding is that if we have a security incident [within the Media Lab] that puts MIT's connectivity at risk, and we don't respond quickly enough, they have to cut us off at the demarcation point. This has never happened, because we are able to respond quickly enough."

The Media Lab operates a rudimentary firewall around its network to block access to some troublesome or unnecessary services. "I drop off some ports that can cause trouble," Bletsas said. "There is no reason my SNMP [simple network-management protocol] ports need to be accessible from outside my border. There is no reason to have telnet now that there are [secure] alternatives."

They also block incoming HTTP traffic to prevent infections from Internet worms or other similar threats. The Media Lab uses MIT's central Kerberos IDs for authentication, along with a locally managed set of Kerberos IDs. Unlike the central IS organization, the Media Lab's IT staff does not require users to register their MAC addresses, since, as Bletsas explained, "It's a research environment, and people need to change their environment on a daily basis."

Bletsas characterized security as the biggest item in his area's workflow; patching the lab's 1,600 machines is his IT department's biggest security challenge. It is the users' responsibility, but the lab's IT area tries to be as proactive as possible in assisting their users. The central security team provides minimal guidelines for security activities like patching primarily because "we have better access to resources than they do," he said. "We tend to respond a lot faster than the average campus user, both because of our proximity and the availability of staff."

However, their task is also somewhat harder, given the nature of their organization. "The central side follows standards a lot closer," Bletsas explained. "We have no standards by design, because of the research nature of the facility. People are allowed to use whatever they feel like, so we have fewer stock answers for our users than they do." Bletsas would like to make security an official part of several IT department members' job descriptions and create a SWAT team of a few mid-level engineers to help users remediate problems. Researchers see security as a necessary evil. "Security is a zero-positive function," he said. "Users don't care until they get infected and lose data. Even then it is sometimes hard to convince researchers to take their computers off the network."

The Media Lab has participated in the security team since its inception in 1995. Bletsas described the benefits of participation: "Security has become our major time-

consuming task here, and every help we can get is welcomed, and so we should contribute back. The more of us who play this role, the better it is for the university. I wouldn't want to substitute the broad consensus that exists right now with the network security team with a rigid set of rules. This is a very fluid field right now, and one of the worst things you can do is set up rigid rules that everyone has to abide by."

The arrangement also enables the Media Lab to operate their research environments in a way conducive to their needs while remaining part of the overall university team. "Thus the only way the general procedures that the IT security team has established can be extended in an environment like ours is if we are an integral part of the security team." Bletsas believes the security team is extremely important because of MIT's open environment and that it is very effective. "Given their manpower and their resources, I think it is one of the most successful efforts ever in IT here," he added.

Security Culture and Awareness

MIT takes a holistic approach to security. "I tend to think of security starting first and foremost with the people and their ability to live and work here," said John Curry. "This leads in turn to the need for security personnel and technologies, from streetlights to fire protection to data protection. We want to provide [our community with] a sense that your computer is a safe thing to use. A person's e-mail will not blow up; his data will be there when he goes back to work tomorrow. We want to protect his productivity."

However, IT security's cultural aspects carry special challenges in a place where faculty members and researchers are always pushing the technology envelope. The IS department may be unaware of their activities. "You work very hard to build an environment that is transparent to people who want to

do weird and different things,” Bruce said. “We have to scramble to do things that the infrastructure does not make easy. Most of the faculty and the organizations have sufficient technology that they just go and do something. Sometimes you don’t know about it until it is done.” For example, an MIT Nobel Prize winner gave a lecture that was simulcast over the Internet in Cambridge and Singapore. Everyone assumed the network would perform correctly, and no one thought to contact the IS area beforehand to determine the impact.

A faculty member might see security as a nuisance that prevents him from completing a research project—even when his machine is compromised. “People don’t have trouble with the security—they have trouble with the rules that mandate the security,” Curry said. One faculty member refused to turn off his infected machine and reinstall his operating system. He felt that since the system’s compromise wasn’t bothering him, why should he shut it down for several days? Faculty members may not always appreciate the security measures in place. They may not understand how FERPA (Family Educational Rights and Privacy Act) regulations affect their academic activities by, for example, requiring a student’s permission to publish his work on a Web site.

But pushing awareness is difficult. “The problem we have with education around here is getting people to pay attention,” stated Jeff Schiller. “Communications in our environment are very difficult because we have many vehicles for communication, and people can ignore them all.” Schiller recalled a client who referred to the IS newsletter as “fluff and McCuteness.” “If someone asks for help to manage his data, we have won the battle,” he said. “It is all downhill from there. The challenge is how to reach the people who don’t realize there is a problem.”

IS and administrative departments do train their staff members about sensitive data issues such as the risk of leaving data on their machines or issues of downloading data from the administrative system. Individual areas are responsible for their own training, but IT will conduct training in problem areas. However, downloading data to the desktop is still routine. “If I had to guess how some confidential data at MIT will be compromised,” Schiller said, “it will be either through a server break-in or data stolen or inadvertently e-mailed from someone’s desktop.”

Security Practices and Incident Response

Jim Bruce outlined MIT’s general security practice: “We build in security mechanisms to look for weak points in the network. If there is a break-in, we isolate the problem so people can continue to do their work on the rest of the network.”

The network team uses an open-source intrusion detection system (IDS) called Snort.⁵ Mahoney relates one problem with IDS selection and use: most products assume the system administrator is behind a firewall. This methodology does not work in MIT’s nonfirewall environment. As a result, the network security team focuses mostly on outgoing attacks—indicating a compromised machine or malicious behavior—rather than on incoming scans, because the scans are continuous and not blocked by a firewall. The team generally pays attention to incoming traffic only if it is looking for something new, potentially indicating a new type of attack. The network security team scans the network constantly for null passwords and other vulnerabilities. As new exploits emerge, the security team changes the set of vulnerabilities it scans for. The staff member in charge of scanning has created proprietary scanning scripts. When the Code Red virus hit, for example, the

network security team developed its own techniques to identify the infected machines by examining the network traffic patterns an infected system generated.

MIT maintains site licenses for antivirus software for several computing platforms and makes this software, as well as significant virus-related information, available to all users on the Web.⁶ Users are strongly encouraged, although not mandated, to use it. The IS department recently installed rudimentary virus scanning on its primary e-mail system, allowing the security team to limit the institution's exposure to viruses propagated through e-mail. For example, this toolset helped the network security team filter out the Bugbear virus within a half hour.

Also saving MIT considerable e-mail virus-related grief is its relatively small Microsoft Outlook user base, but that is about to change. Previously, the IS department endorsed Eudora as the university's primary mail client, but the IS support group just issued a new recommendation for Windows users to use Outlook. While it may be easier to operate and support, Schiller believes the longer term security ramifications may be harder to address, because Outlook is often the target of virus-based attacks.

Although the security team provides monitoring and tools to protect the network, individuals must manage their own machines' security. When the network security team discovers a problem on a user's machine, the vulnerability's seriousness determines the course of action. If the scanning discovers a worm or blank administrative password, the machine is taken off the network. For example, the network security team exhibited zero tolerance for Code Red; if a user's computer had it, the team blocked its access to the network. If a machine is vulnerable, IT security tries to determine the likelihood that it will be compromised before deciding to turn it off. For a less serious vulnerability,

the team e-mails the person responsible for the machine with the appropriate CERT (Computer Emergency Response Team) or vendor advisory to fix it.

Reinstating network access for a compromised system is somewhat arduous. If a machine is compromised, the user must erase the hard drive, reinstall the operating system from known installation media, and then restore user data from a backup source. The network security team is not staffed for, and does not provide, individual recovery assistance. Instead, before discontinuing network access, they e-mail the user a detailed message about the reasons for the shutdown and how to remedy the issue. Web pages can help users restore their machines, certify that they are restored, and regain network access. As a result, many people are grateful when their network access is preemptively blocked during an attack because they avoid the recertification process.

Interestingly, Michail Bletsas believes the network security team's requirements for recertification may be a little harsh, especially given the time investment required to comply, and that worm extraction procedures are frequently documented and could be used in lieu of complete reinstallation. At the Media Lab, an IT staff member determines whether to clean up a user's infected computer or reinstall the hard drive. Bletsas, however, does concur that for users who are not technically savvy, the security team's approach appeals to the lowest common denominator.

The IS department is, however, developing new resources to help users. According to Schiller, its WinAthena, a centrally managed, security hardened Windows environment, is technically excellent but poorly marketed to the community. A review committee is about to address the marketing issue. The IS department also maintains Web pages to recommend patches and give advice on running Windows XP, as well as other commonly used systems, securely.⁷ A team also

exists that will manage an area's Windows machines for a fee.

MIT historically, and almost by intent, has fewer policies than most universities have. "Why should we have page after page of formal rules about what you can do and not do?" asked Bruce. "Nobody reads those anyway. We have always felt that we are on much sounder footing by having fewer policies at a more abstract level than down to the minutiae. I realize there are arguments on the other side, but our lack of policies has served us very well and has not gotten us into real trouble. There are very simple network rules of use, as, for example, don't use another person's Kerberos principal."

Likewise, little documentation exists for incident response procedures, though Bruce feels this may change because of the increasing number of incidents and people involved. But only a handful of people detect, remediate, and interact. They work with each other every day. Bruce feels some of the actions to follow are second nature—for example, minimizing the network impact on users as a whole.

Interestingly, MIT has called the police only twice for an IT security incident. The first involved an employee who served copyrighted software off an Athena workstation. The other involved a U.S. Customs case. "MIT prefers to solve problems internally than to pursue a full legal case," Bruce said. "Often we will notify an administrator or manager that a person is doing something inappropriate. Bob Mahoney will discuss his suspicions with a suspected student."

Occasionally law enforcement contacts the university. Bruce described how a cooperative approach paid dividends for MIT when working with them. Several years ago, the U.S. Customs Service conducted a sting operation against an employee of MIT's economics department who was suspected of using his position, and the Institute's resources, to trade warez (illegal

copies of commercial software). "When they were ready to do the bust, they came in and talked to us," Bruce recalled. "Although Customs conducted the raid, the MIT police and network staff were there. We worked with them so they wouldn't have to take any MIT machines away. We proved that cooperation means that you don't have law enforcement hauling off a truckload of your own machines. This minimized disruptions on campus."

In another incident, the U.S. Secret Service contacted MIT less than eight hours after an MIT user posted a message on a computer bulletin board threatening the first President Bush during a campaign visit in Boston. The university was quickly able to assist the Secret Service in tracking down this user.

Despite constant attacks, both Curry and Bruce believe MIT is doing a good job with its security practices. Students could break in, but they recognize the severe ramifications for their actions. "For the most part, we detect early, deal with it, and look at it as part of the cost of doing business," stated Bruce. "In this area, you can't sit on your laurels. For example, SQL Slammer infected every vulnerable machine in the world in seconds. We built our computer network with a lot of trust and with very little understanding of the devious behavior that might arise. How can we retrofit? I don't know, but it means that every one of us is going to have to continue to be on our toes for the next derivative of Slammer, Bugbear, or pick your favorite one."

MIT's Security Outreach

MIT has several IT security outreach initiatives. Jeff Schiller and Bob Mahoney both promote MIT's activities and issues through their participation in the Internet Engineering Task Force, Internet2, and EDUCAUSE. The network security team also operates a "summer camp" for 50 to 75 IT staff members from higher education institutions in the

Boston area to discuss network security issues. Representatives from law enforcement agencies frequently participate.

MIT also works closely with vendors to promote the inclusion of more robust IT security measures, including Kerberos, in their products. MIT and Microsoft developers used to hold regular conference calls to discuss Kerberos issues and compatibility. The institution was a major driver behind Apple's OS X authentication and Kerberos activities. "We believe that every time we do something and get to the point where the results come out of the box back to us, we win," Bruce said. "That was the premise when we decided to give Kerberos away rather than licensing for a return on money."

Strengths and Challenges

In our conversations, various MIT representatives outlined the institution's IT security strengths and challenges.

Strengths

- ◆ *Single sign-on through Kerberos.*

Schiller said MIT was successful because it adopted single sign-on early, before a lot of departments got involved with IT security, which has made adoption of single-sign-on tools much more difficult for later-moving institutions.

- ◆ *Web authentication through X.509 certificates.*

X.509 certificates offer several advantages, Schiller said. Students can run Web sites without impacting MIT's security exposure, because an X.509 certificate never reveals any key personal information, like user name and password, that can be used to impersonate the user to the server. For example, the MIT student government held an online election from its own Web-based system without IS having to provide access to every student's name and password. If the voting server were compromised, it could impact the voting

data but would not compromise the voters' personal authentication credentials.

MIT developed and operates its own certificate authority, saving significant cost over using a commercial product. Schiller also feels that MIT's implementation of certificates more closely aligns with an academic institution's needs, as the MIT certificate authority allows one user to have multiple active certificates on multiple machines, whereas commercial certificate authorities have difficulty supporting such a situation. In addition to on-campus uses, MIT has begun to expand its use of certificate-based authentication to its business partners. For example, an office superstore chain will display MIT-negotiated product prices in its MIT portal, once a user is authenticated as being affiliated with MIT through his X.509 certificate.

- ◆ *Running an enterprise network without a perimeter firewall.*

MIT continues to implement its security strategy using Kerberos, X.509 certificates, and strong machine- and application-based defenses.

- ◆ *An effective security response team.*

The grassroots approach creates an institution-wide network of resources and helps compensate for the limited staff and funding available to the network security team.

Institutional Challenges

- ◆ *Wireless technology.*

Wireless systems present new avenues of attack for potential hackers. While MIT does require MAC address registry for network use, there is concern that someone could surreptitiously join the network and perform undesirable activities, such as sending spam.

- ◆ *Vendors don't necessarily incorporate security in a usable way.*

Most vendors assume that users run their security applications behind a firewall or use a virtual private network (VPN). Most can't

handle single sign-on or encrypted applications. Their application developers do not consider security in application design. As noted earlier, MIT had problems selecting an IDS because of the firewall assumption. “It is a security conundrum,” Schiller said. “Vendors don’t include it because users do not ask for it [during development]. Users do not ask for it because hackers don’t attack toy implementations.” Schiller also pointed out that MIT can’t easily integrate many packaged systems into its environment because they rely on firewalls and VPNs to provide security.

◆ *Difficulty in quantifying the value of security.*

“When you read about MIT in the newspaper, you want it to be about a great breakthrough, not a break-in,” Schiller said. “That argument only goes so far.” The difficulty in quantifying the value of security makes it difficult to convince senior management to invest in security.

◆ *Resources stagnate or decline while issues grow.*

A related issue is the difficulty of justifying additional security resources during lean fiscal times. The number of attacks continues to rise monthly, and Schiller estimates the monthly attacks will triple within a year. The nature of these attacks is also changing: more are automated, and worms, bots, and zombies attack with greater frequency and at all hours. Automated worms pose particular problems because they exploit vulnerable machines in a matter of hours, requiring more manpower to respond more rapidly.

◆ *Restricted information access fosters illegally stored data on desktops.*

Schiller believes this is one of the biggest challenges facing MIT. “We don’t have a policy on campus for who owns data,” he explained. “Each department manages access for their own data.” People ask those with data access to run reports off the data warehouse, creating new files on staff members’

desktops. This sets the stage for inadvertent exposure of files from viruses or discarded hard drives. MIT needs a policy that prohibits storing confidential data on the desktop and provides easier access to the data warehouse. The problem is how to loosen access without compromising security.

Lack of data ownership standards also impacts Roles. Instead of rules-based authorization, many case-by-case determinations are made from contextual factors. Financial areas use Roles more frequently because they provide clearer rules. “When authorization was paper based, the request–response paradigm worked pretty well, but it does not scale well into the electronic space,” Schiller stated.

◆ *Response time decreases.*

With faster machines and faster networks, the security team will have less time to respond and must therefore find ways to react faster.

◆ *Speed of communication and access.*

“[We need to] retain enough power of communication to react to an incident, to assemble the right collection of brains and work the problem,” Curry said.

◆ *Prepare for the future.*

Think about what kinds of things could strike the university’s network and test rapid response capabilities.

Lessons Learned

◆ *Communicate, don’t confront.*

When there is a problem, MIT communicates about the problem rather than overtly confronting the person. “We learned that if you went to Johnny and said, ‘You did thus and so,’ Johnny would deny it,” Bruce said. “The student will blame a friend who was using his password. One of the ombudspersons suggested that we send a letter or e-mail that states that someone using your account did x, y, or z. It changes the person from belligerent defender of self to [someone who is] extremely meek about it. In the

latter case, you get an apology, the student changes their password, and the incident is unrepeated. In our 15 years of using this approach, we have had few second violators. This spring, we took the first third offender before MIT's internal judicial process."

- ◆ *Work with law enforcement to minimize disruption.*

To ensure a successful operation and to make sure they confiscated no MIT devices, MIT worked with U.S. Customs Service agents before and during their planned raid on an MIT user's illegal software distribution activities.

- ◆ *Representation facilitates buy-in.*

Mahoney's efforts to include all parts of the institution benefit him in several ways. Not only does he gain resources to help him, but he also gets buy-in to his policies and support when he presents them to senior management.

- ◆ *Firewalls breed a false sense of security.*

"A purchased firewall is not a substitute for a professional staff. They work best the closer they are to the assets they protect," Schiller said. "If a vendor says you need a firewall, that's a warning sign."

- ◆ *Maintain strong relationships.*

Since effective security is often hard to see, frequently the only time most people notice it is when there is a failure or a draconian measure implemented. "You are not maintaining good relationships if the only time the word 'security' comes up at the highest levels is when there is a problem," Mahoney said.

- ◆ *Foster a bottom-up approach to security.*

Bletsas recommends that participation be as broad as possible for security. MIT's ad hoc security team members feel empow-

ered because they directly impact security's direction at MIT. People join because they are interested and knowledgeable. This creates a lot of positive PR within the institutional community because users are participating directly in the institution's security process.

- ◆ *Security is about communication.*

Knowing whom to contact about security is especially important on a large campus. Both the network security team and Stop-It try to communicate regularly with the MIT community. Also, since the security team is so distributed, it relies on instant messaging and mailing lists rather than face-to-face meetings to communicate.

- ◆ *Port-managed networks work.*

"Managing your network to the port is really nice," said Bletsas. "It's expensive at the end of the day because you have to put managed switches all the way to the periphery, but you can make a case for lowering your costs there, because you can respond faster and a lot more surgically, as opposed to cutting off a whole work group or a whole building [in response to an incident]."

MIT's experience demonstrates the essential roles that both technology and people play in maintaining a successful IT security program. MIT's technical innovation has resulted in a robust solution that preserves openness in an increasingly unsafe network environment, but its cadre of IT security volunteers and student employees have proven just as important to its success. This latter point is particularly important because many institutions may not have the resources to emulate MIT's security architecture, but they can foster a similar cultural environment to enhance IT security institution-wide.

Endnotes

1. The scope of the security study was based on ISO17799, including system access control, system development and maintenance, compliance, personnel security, security organization, computer and operations management, asset classification and control, and security policy and its deployment, and excluding business continuity planning or disaster recovery and physical security.
2. Although this survey was not randomized or stratified, creating the risk of both survey and respondent bias, it was universal for research universities and oversampled both M.A. and B.A. Carnegie institutions. The data reflect very closely the general EDUCAUSE membership, including the relatively smaller participation of A.A. institutions.
3. For an overview of Project Athena, go to <http://web.mit.edu/afs/.athena/astaff/project/logos/olh/Welcome/Welcome.html>.
4. See <http://web.mit.edu/kerberos/>.
5. See <http://www.snort.org/>.
6. See <http://web.mit.edu/is/topics/virus/index.html>.
7. See <http://web.mit.edu/is/topics/security/index.html>.