

7

IT Security Incidents, Response Practices, and Procedures

Bandwidth spikes are rarely a result of academic breakthroughs.

—Dan Updegrave

In this chapter we address programs and practices that colleges and universities have implemented to respond to information technology (IT) security incidents. How do they identify and respond to incidents? Are some institutions more vulnerable than others, and if so, why? How does the institution respond to breaches and incidents? What is the impact on the institution?

The combination of university systems' open nature and the high-powered technology that often exists on campuses puts academic institutions in a position unique among large enterprises.¹ In addition to being the target of cyber attacks, university networks and systems sometimes serve as the source of attacks on other entities. For many institutions, being a good "Net citizen" and preventing the use of institutional resources for such attacks is nearly as high a priority as protecting their own information.

Examples of security breaches abound in higher education, and each one exposes the industry's vulnerabilities, threats, and risks. A breach is as likely to come from within as outside the institution. Cornell University graduate student Robert Tappan Morris launched one of the first worms—the

Morris Worm—in 1988. It was touted as the first worm that demonstrated the power of a self-replicating computer program across the network. The problems it caused led to the creation of the Computer Emergency Response Team (CERT) at Carnegie Mellon University, and this team remains a top organization for identifying viruses and notifying organizations and the general public about the effects of viruses and how to prevent their spread. (See the sidebar "Notable Viruses" for details about several of the most damaging viruses.) CERT also identifies security vulnerabilities, including viruses, and notifies organizations and the public about their effects and how to mitigate their exposure.

Cyber attacks are occurring with increasing frequency. A summer 2003 worm, referred to as the Microsoft remote protocol control incident, or "Blaster," hit computer users with enormous speed. Unlike many worms, Blaster did not spread via e-mail but instead scanned the Internet looking for vulnerable computers. Symantec, maker of a leading antivirus software package, gave the worm a Category 4 threat-level rating on a scale of 5. The worm hit several universities hard. The University of Texas at Austin, for

Notable Viruses

The Love Bug (I Love You) virus is one of the best-known viruses worldwide. This virus only targeted users running the Microsoft Windows operating system, attacking the Outlook e-mail program and the Internet Explorer browser. When opened, the virus attacked the computer's hard drive, deleting video and digital photography files and hiding music files. The file forwarded itself to all addresses in the Microsoft Outlook address book. The virus may have erased files from its victims' computers, but the more widespread damage was in clogging up computer networks. This virus was one of the most destructive ever developed, with effects ranging from corrupted data files to the wholesale destruction of a company's data records. Estimates of the damage caused range up to \$10 billion, mostly in lost work time.

The Melissa Virus, a widespread virus in 1999, infected more than a million computers. The virus affected only computers with Microsoft operating systems, attacking the Microsoft Outlook program to propagate itself. When a user opened the infected e-mail attachment, the virus attempted to e-mail a copy of this document to up to 50 other people. This was significant to many users, as it had the potential to compromise organizational confidentiality. While the virus did comparatively little damage to individual computers, unlike later viruses, it had graver implications for company and Web servers carrying the huge volumes of e-mail being created. The virus, believed to have been named after a Florida stripper its creator knew, caused more than \$80 million in damage.

The Code Red Worm first appeared in July 2001. Originally designed as a denial-of-service attack on the White House Web site, it had the power to infect 250,000 systems in just nine hours. The self-spreading program infected servers using unpatched versions of Microsoft's Internet Information Server software and defacing the Web sites the servers hosted. The worm spread by selecting one hundred IP addresses, scanning the computers associated with them for a hole, and spreading to the vulnerable machines. It then defaced any Web site hosted by the server. The worm could also help attackers identify infected computers and gain control of them. The effects of Code Red were devastating and widespread. It is estimated that Code Red infected more than one million of the 5.9 million Microsoft IIS Web servers. Additionally, many companies experienced internal disasters when 25 or more system infections simultaneously occurred. While the main effects were performance degradation and system instability, the Code Red worm also caused billions of dollars in damage and introduced the technol-

ogy community to the dangers of not reacting quickly to public warnings of vulnerabilities.

Called a “multiexploit” worm, Nimda used several methods to spread around the world, including e-mail and unpatched IIS servers. In 2001, Nimda was the first worm to modify existing Web sites to start offering infected files for download. It was also the first worm to use normal end-user machines to scan for vulnerable Web sites. This technique enabled Nimda to easily reach intranet Web sites located behind firewalls—something other worms couldn’t directly do. This complex virus contained a mass-mailing worm component that spread itself to Windows users in attachments named README.EXE and then quickly spread around the world. The worm created network outages worldwide, and the extent of the damage appeared throughout the Internet, causing very poor Internet connectivity, damaged Web sites, and an inability to connect to various host servers, mail servers, and Web sites. The immense volume of traffic generated by the virus either brought down network routers around the world or slowed them to a halt.

Chernobyl was the first virus to damage computer hardware. The virus struck on 26 April 1999, the anniversary of the Chernobyl nuclear disaster, and affected computers running Windows 95 and 98, striking them as they were booted up. The virus rendered hard drives unusable and, in some cases, damaged the hardware that allows computers to start up. Hundreds of thousands of computers in Asia and the Middle East had their data wiped by the Chernobyl virus, but the United States and Europe managed to escape most of its harmful effects. Estimates of damage reached into the hundreds of millions of dollars.

Happy99 has been called the first modern Internet worm discovered “in the wild.” The worm was distributed in early January 1999 as a Windows .exe file attached to an e-mail message. When run, it displayed fireworks on the screen. At the same time, it changed the machine’s network software so that every time an e-mail was sent from the machine, a copy of Happy99 was also sent to the same address. There was no other malicious payload apart from its system modifications to facilitate its propagation.

In February 2000, widespread denial-of-service attacks made headlines as they crippled the online operations of Amazon.com, Yahoo, eBay, CNN, and Buy.com. These Web sites were flooded with thousands of bogus messages, making it difficult or impossible for genuine users to connect to the site. Many of these prominent Web sites suffered major slowdowns, with some having to shut down for several hours until they could restore service.

example, scanned their network and found 5,000 machines infected. They blocked IP addresses at the border and as close to the switch as possible. They then sent a message to owners requesting that they install the patch; two days later they sent a more emphatic message, resulting in significant user community compliance.

Institutions that avoided problems had one or more of the following factors in place:

- ◆ a significant Macintosh presence on campus;
- ◆ implementation of port blocking, including permanent blocking of ports (NetBIOS protocol), or ad hoc blocking in response to notification from FIRST (Forum of Incident Response Teams) and subsequent announcements from the Department of Homeland Security and REN-ISAC;
- ◆ availability of virtual private network (VPN) service as an alternative; and
- ◆ proactive scanning and effective intrusion detection, allowing for early detection of the problem.

Border blocks plus VPNs appeared to be the most effective and desirable practice for minimizing this worm's impact on end users.

On 5 June 2003, confidential employee salary and bonus information was transmitted on the Web to some of the 35,000 computer users inside Stanford University when the Bugbear.B virus that infected the university's computer system randomly sent out files from campus PCs. Chris Handley, CIO at Stanford University, responded by temporarily blocking users from sending e-mail to the outside world.

In February 2003, a computer hacker obtained the names and Social Security numbers of about 59,000 former and current students, faculty, and staff members at The University of Texas at Austin. Dan

Updegrave, CIO, estimated that this cost the institution \$145,000 to \$150,000, including \$25,000 to print and mail letters, \$2,000 in phone bills and third-party payments for address cleanup, and \$100,000 in staff time.

In January 2003, University of Kansas officials detected suspected computer hacking into a file server that contained records of 1,450 students, mostly international students. In June 2002, the *Chronicle of Higher Education* reported the possibility that Russian mafia had infiltrated computers at Arizona State and other colleges.

Another and more recent insidious form of intrusion comes from so-called spyware—software that gets installed surreptitiously via browser hijackers, adware, auto dialers, and some freeware applications. When a user clicks on a pop-up ad, spyware resets the browser home page and inserts bookmarks that are difficult to delete. Typically, they will redirect the user to porn and gambling sites. Such attacks impede work, which is costly to the institution.

The University of Washington's Terry Gray classifies these threats to higher education institutions in seven categories:

- ◆ application-level security threats such as e-mail viruses, attachments, and IRC bots;
- ◆ threats to network infrastructure devices (switches, routers);
- ◆ threats to core network computing services (DNS, DHCP, Kerberos);
- ◆ theft of network connectivity services by unauthorized users;
- ◆ unauthorized access to hosts (both clients and servers) via the Internet;
- ◆ unintended disclosure or modification of data sent between hosts; and
- ◆ denial-of-service attacks against connected hosts.

Each has been a reality for higher education.

KPMG Consulting LLC provided the University of California with a useful analysis of hacker attack profiles.² It outlined 10 of the

most important threats and the methods used, including Internet service or software vulnerabilities, Web application vulnerabilities, social engineering (such as bribing employees or posing as a legitimate user to obtain a password), protocol infrastructure attacks, denial of service, and Internet traffic sniffing. Recommendations for mitigating risks included formulating and following institutional security policies, awareness programs, and incident management protocols; implementing a robust security architecture; and monitoring systems and networks frequently. Our study elaborates on the degree to which these strategies for mitigating risk have been adopted nationally.

The 2002 KPMG survey asked respondents what they saw as the most important security issue facing their organizations. Rated highest were viruses (22 percent), hackers (21 percent), and remote access controls (17 percent). Sixty-one percent of organizations reported having had a virus incident, 29 percent an e-mail intrusion (such as spamming), 14 percent a denial-

of-service attack, and 12 percent Web site intrusion (hacking).

These attacks rack up substantial costs. According to findings from the 2003 CSI/FBI Computer Crime and Security Survey, theft of proprietary information from businesses caused the greatest financial loss, with the average reported loss being approximately \$2.7 million. The second most expensive computer crime among survey respondents was denial of service, followed by financial fraud. Virus incidents (82 percent) and insider abuse of network access (80 percent) were the most often cited forms of attack or abuse.

IT Security Incidents

Eighty institutions (19 percent of respondents) indicated that they had an IT security incident that had been reported to the press. The larger institutions and doctoral institutions were more likely to have had such an incident (see Figures 7-1 and 7-2). Of the 19 institutions with enrollments of more than 25,000 in our study, 58 percent had an in-

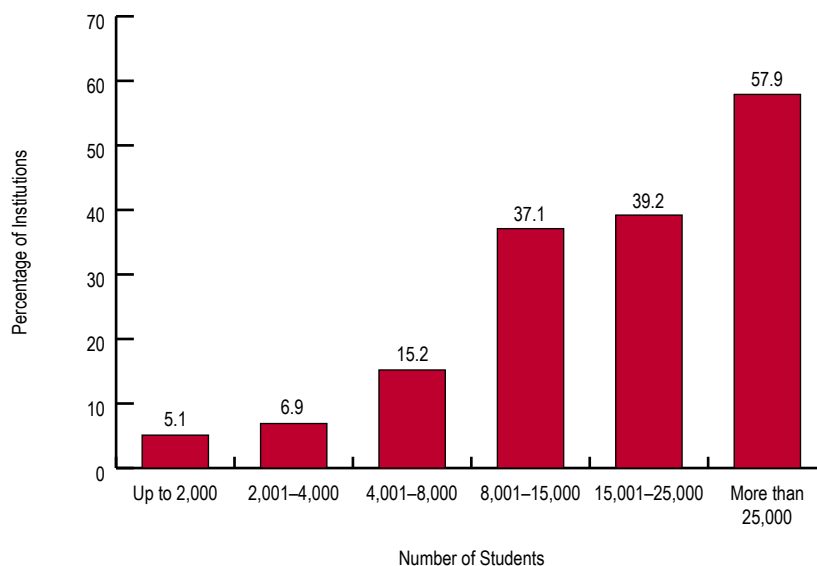
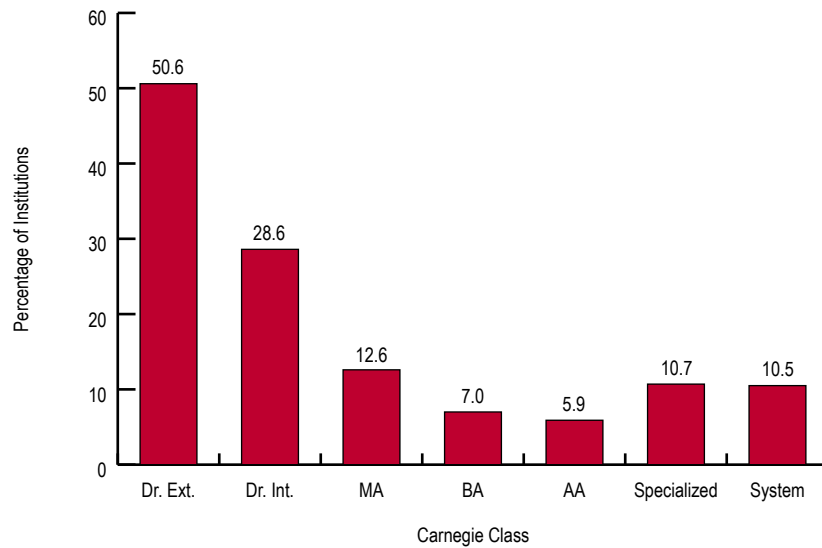


Figure 7-1. IT Security Incident Reported in the Press, by Student Enrollment

Figure 7-2.
IT Security
Incident
Reported in
the Press, by
Carnegie Class



cident reported in the press, compared with 5 percent at institutions with enrollments of 2,000 or fewer.

Of course, this does not mean that others are exempt. Of the total incidents reported in the press, 30 percent were at institutions with 8,000 or fewer enrolled students, 30 percent at institutions with enrollments between 8,001 and 15,000, 25 percent at institutions with enrollments between 15,001 and 25,000, and 15 percent at institutions with enrollments of more than 25,000.

Doctoral-extensive institutions (51 percent), followed by doctoral-intensive institutions (29 percent) and MA institutions (13 percent), had the most incidents reported in the press. And these institutions were attacked more often. Note also that 70 percent of the reported incidents occurred at public institutions, which may reflect more stringent public reporting requirements.

As the number of devices increased, the percentage of institutions that had a security incident reported in the press increased dramatically, from 9 percent to 67 percent (see Figure 7-3). The same is true for number of network users. We noted also that institu-

tions with more network devices and users are more likely to consider IT security a top institutional priority and one of three major issues facing the IT office. They are also more likely to have formal policies and awareness programs in place.

We also asked when the respondents' institutions experienced their first incident that was reported to the press. Only 71 of the 435 institutions gave us the year or period. Of that subgroup, 63 percent indicated after 2000, 28 percent during 1997–1999, and 1 percent before 1996. We found little difference by Carnegie class, size, public versus private status, or country.

Residence Halls and Incidents

Residence halls connected to the campus network are often cited as a large area of potential risk because they provide a less controlled computing environment. Consequently, they raise a potential IT security threat from within the institution and also expose the campus network to the possibility of attack on unsecured machines. According to Diana Oblinger, executive director of

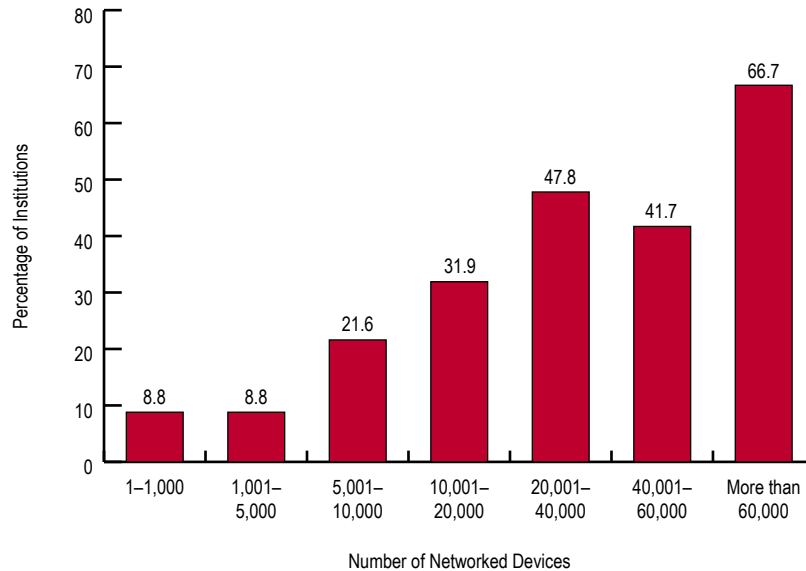


Figure 7-3.
IT Security Incident Reported in the Press, by Number of Networked Devices

higher education at Microsoft and former ECAR senior fellow, “Students are able to bring their own computer equipment and connect to the network. The software on those computers can be from a host of vendors representing an array of versions, and both students and vendors might be unaware of security problems in those products. The transient nature of the student population creates additional security challenges, while the advent of wireless capabilities generates further problems.”³

Do residence halls make a difference? Have institutions with residence halls deployed different strategies than those without residence halls? Of the institutions surveyed, 76 percent had residence halls (67 percent in Canada). Those with residence halls were more likely than those without to have policies for shutting off Internet access (89 percent versus 68 percent) and formal incident handling procedures (48 percent versus 34 percent). However, we found little difference in enforcement procedures and willingness

for administrators to take punishable action in general. While student awareness programs were more likely at institutions with residence halls (37 percent versus 22.5 percent), these percentages seem low, given the potential exposure. Moreover, the respondents did not rate their programs’ effectiveness differently. Finally, institutions with residence halls were more likely to have a security incident reported in the press (22 percent versus 8 percent). Residence-hall computing increasingly is managed differently, with many institutions setting up separate networks for them.

IT Security Incident Handling Procedures

We asked respondents whether their institution had a formal IT security incident handling procedure. Forty-five percent said they did (43 percent in Canada), compared with 66 percent of KPMG survey respondents. Institutions most likely to have formal incident procedures are public, doctoral, and those with more than 25,000 students enrolled.

Figure 7-4 shows the breakdown by Carnegie class, Figure 7-5 by student enrollment, and Figure 7-6 by number of networked devices. Clearly, as enrollments increase, so does the likelihood of having a formal procedure. Without one, many organizations cannot accurately assess damage done to the institution or effectively handle internal and external public relations.

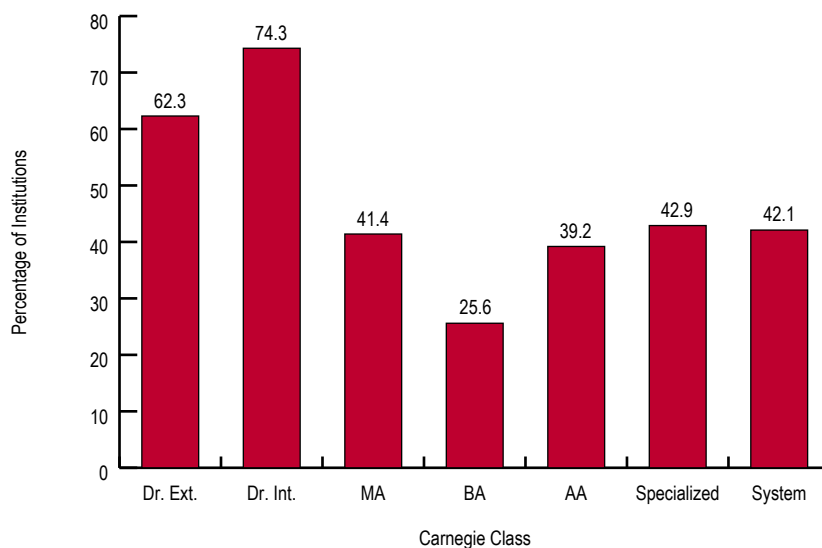
Our interviews revealed that several institutions had “incident policies” used for any incident—not just IT security ones. Typically, the press office or the Office of University Affairs handles the press, bringing in other officials—IT officers, senior management—as appropriate. The University of Notre Dame, which did have an incident reported in the local press, has a specific policy for IT security. CIO Gordon Wishon said, “We have a director of communications that coordinates with the rest of the campus. Our process involves any one or a mix of people, depending upon the nature of the incident; it depends upon the vector. If

it is an incident that is reported through the police department/public safety, I may not be involved in the front end of the process. If it is an incident that we become aware of internally, it would rise to me very quickly, and yes, we would involve the appropriate people along the way.”

According to Dick Jacobson, North Dakota University System IT security officer, “In larger institutions, departments may handle an incident response, too, since their IT security operations are decentralized. Our policy gives the individual campus the responsibility to deal with the incident. Realistically, however, we tend to find out or get involved pretty early in the process, and we have expertise that can be leveraged by the smaller institutions.”

The Georgia Institute of Technology (Georgia Tech) has a highly formalized incident response team and policies. The procedures are documented in a flowchart, which contains contact information and illustrates specific actions resulting from incident

Figure 7-4.
Institutions
with Formal
Procedures
for Handling
IT Security
Incidents, by
Carnegie Class



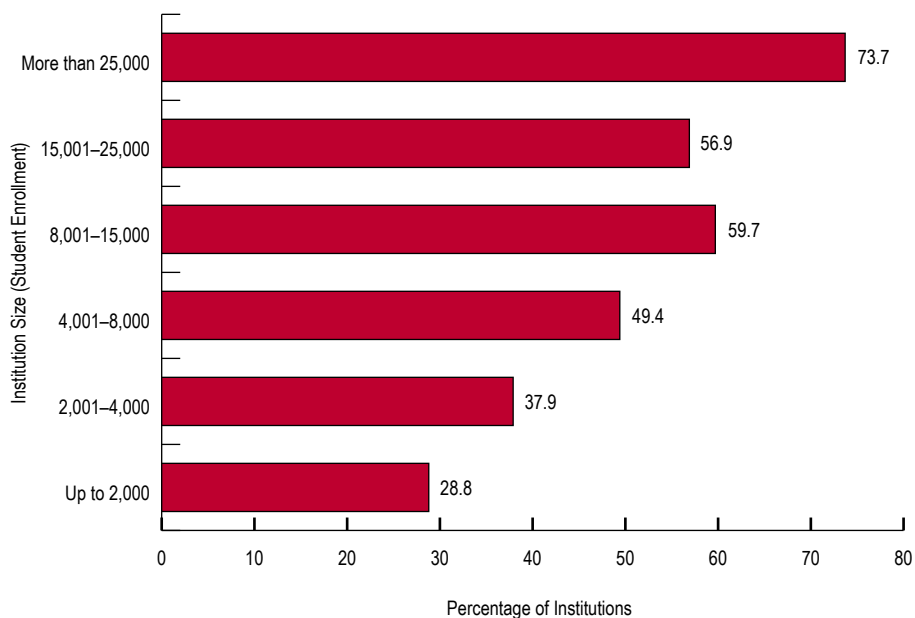


Figure 7-5.
Institutions
with Formal
Procedures for
Handling IT
Security
Incidents, by
Student
Enrollment

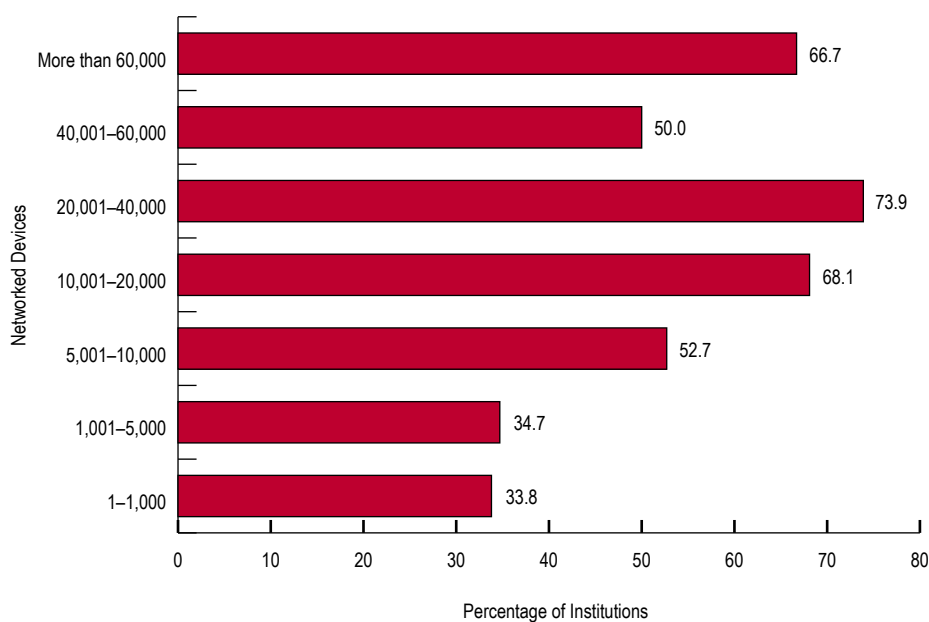


Figure 7-6
Institutions
with Formal
Procedures for
Handling IT
Security
Incidents, by
Number of
Networked
Devices

events. John Mullin, associate vice provost, associate vice president, and chief information officer for information technology, said, “Incident response policies are tools to help you deal with the incident more effectively and more quickly. We weren’t paralyzed when the incident occurred. After you get past the expletives, you have a process to follow. We tune it for the next round, and we hope we never need it—just like insurance.”

At the University of Wisconsin–Madison, volunteers participate on the BadgIRT (Badger Incident Response Team), which operates as an integral part of the Division of Information Technology’s security department. It acts as a central collection point for tracking incidents, analyzes information security trends, and works with other incident response teams worldwide. BadgIRT is a member of FIRST. “BadgIRT is very important to security efforts at UW–Madison,” emphasized Judy Caruso, director of policy, security, and planning. “As a very decentralized campus, it is imperative to have active involvement and engagement in security incidents and directions by IT staff from throughout the campus.”

Who Is Involved in IT Security Incident Handling Procedures?

We asked for further elaboration on who gets involved if an incident occurs. In descending order, 86 percent of the procedures included the police and campus security offices, 75 percent the student judicial affairs office, 74 percent the legal office (general counsel), and 65 percent the campus communications office. Among institutions that had formal procedures, we found little difference by size, Carnegie class, public or private status, or country. There was a significant difference, however, by size and Carnegie class with respect to involving the

police and legal counsel. Doctoral institutions (90 percent) and institutions with more than 25,000 enrolled students (100 percent) were far more likely than the smallest institutions (60 percent) to include the police and legal counsel.

Georgia Tech created an executive response team for incident response consisting of the CIO, the director of auditing, the director of information security, the director of financial services, the vice president of human resources, the director of campus communications, the legal counsel, and the director of campus security. In addition, the head of the affected unit joins the team for the duration of the response.

The University of Texas at Austin’s central information security office has formal interfaces to the rest of the campus community: legal affairs, public affairs, the University of Texas system office general counsel, the University of Texas police department, and the district attorney’s office. According to Dan Updegrove, vice president for information technology at The University of Texas at Austin, “When you are in the middle of a high-profile security breach, you’d better have a really good partnership among public affairs, legal affairs, the president’s office, and IT. It served us enormously well to have a very sophisticated public affairs office that had good relations with the press and a legal affairs office that understands information technology. They quickly grasped the problem and its many dimensions. We all worked together to create a systematic response.”

We also asked whether the formal procedures included central mechanisms for alerting faculty, staff, students, and the administration. Eighty-three percent of respondents answered “yes.” Among institutions that had formal procedures, we found little difference by size, Carnegie class, public or private status, or country.

Reporting Incidents to Senior Management

Asked when they report incidents to senior management, 71 percent of respondents indicated the choice “when the incident occurs.” Combined with the answer “not regularly,” the total becomes 86 percent. Only 14 percent regularly report incidents to senior management. We investigated whether institutions that are attacked most often and were among the first institutions attacked had different reporting patterns than those that were attacked less often or did not have incidents reported in the press. The numbers were so low that we couldn’t come to a conclusion. The case studies and in-depth interview data provide a better perspective.

Recent attacks and security breaches at Indiana University provided a catalyst for improving that university’s security and incident response, including adoption of a formal incident response methodology. Using a central incident response reporting system, central security staff log incidents and triage them. If they suspect a compromise, they identify the incident’s location and the system administrator for that location and ask the system administrator to respond immediately. If the system administrator doesn’t respond, central staff have the ability to isolate the machine from the network. “This is rare, though,” noted Merri Beth Lavagnino, deputy policy officer. “Maybe 5 to 10 percent of the time we don’t have records identifying the appropriate system administrator.”

Both Florida Memorial and Notre Dame report that their incidents accelerated their IT security efforts. For example, Notre Dame’s Gordon Wishon stated that after the local press reported the intrusion into a system

containing Social Security numbers of hourly wage earners, “it showed that our rollout or deployment of security provisions and best-practice implementation within the OIT and within the data center was not proceeding with enough haste, and it resulted in a substantial [acceleration] of the security program, including the erection of barriers around the data center.”

EDUCAUSE Quarterly reported an interesting case study of the ramifications of a security incident at the University of Memphis.⁴ Written by Robert Jackson, systems administrator in the information technology division at the University of Memphis, and Mark N. Frolick, Western and Southern Financial Chair in information systems at Xavier University in Cincinnati, Ohio, the article elaborated on personnel roles in the case of a security breach, detection and forensics, and policy enforcement. It also enumerated lessons learned and offered important, broadly applicable recommendations to mitigate security exposure.

IT security incidents continue to increase and are a problem industry-wide. In the next chapter, we address more directly what institutions must do to protect themselves from IT security incidents.

Endnotes

1. There is an ongoing debate about the meaning of open networks.
2. “Net Security,” topic paper for the University of California, prepared by KPMG Consulting LLC, no date.
3. D. Oblinger, “Computer and Network Security and Higher Education’s Core Values,” *EDUCAUSE Center for Applied Research Bulletin*, Vol. 2003, Issue 6, 18 Mar. 2003, p. 5.
4. R. Jackson and M. N. Frolick, “Mitigating Security Issues,” *EDUCAUSE Quarterly*, Vol. 26, No. 3, 2003, pp. 42–45.