

6

IT Security Incidents, Response Practices, and Procedures

Everything we encounter leaves traces behind.

—J. W. von Goethe

Key Findings

- ◆ The number of respondents in our survey indicating they had an IT security incident in the past 12 months declined by half since 2003.
- ◆ The primary perceived risks are viruses, theft of personal financial information, and spoofing and spyware.
- ◆ The number of reported incidents is about the same or fewer in the past 12 months, compared with the year before.
- ◆ The number of IT security incidents varies by enrollment. Respondents with higher FTE enrollments report a greater number of incidents.
- ◆ Nearly half of respondents have incident handling procedures. This percentage did not change much from 2003.

Insecure college networks get frequent press attention. The evening news abounds with reports of security breaches on our campuses. Recently, at Ohio University, data thieves may have plundered Social Security numbers and other private information—including health records—belonging to as many as 200,000 students and faculty. According to one report, the number of individuals affected at Ohio University is unprecedented for universities and colleges in the United States (Sandoval, 2006).

This pales against the spring 2006 loss suffered by the U.S. Department of Veterans Affairs when a laptop computer containing information on 26.5 million current and for-

mer members of the U.S. military was stolen from a data analyst's home. Nevertheless, widely publicized campus breaches lead to assumptions about the vulnerability of higher education's networks. William Custer, information security policy manager at Miami University of Ohio, observes, "Many states have passed bills requiring us to notify those affected about IT security breaches. As a result, there will be more reporting. So even if there are not more incidents, it will appear like there are."

The Ohio University breach is troubling because of the magnitude of compromised information. But IT security professionals in higher education consider even lesser inci-

©2006 EDUCAUSE. Reproduction by permission only.

dents serious. The recently released Computer Incident Factor Analysis and Categorization (CIFAC) study of 319 IT security incidents at 36 colleges and universities found that only 2 percent of the incidents reported were considered not at all serious (Rezmierski, Rothschild, Kazanis, & Rivas, 2005). According to the study, 26 percent were considered somewhat serious, 31 percent quite serious, and 41 percent extremely serious. Further, the study found that no region of the country is immune to such incidents, nor do institutional size and type make much of a difference. Our data do not support the latter conclusion: We found that institutional FTE enrollments do make a difference.

The security dilemma is particularly challenging for higher education. Sheri Thompson, communications and planning officer for technology at Louisiana State University (LSU), says, "It's like comparing a house with one door to a house with 40. The more doors, or access points, the more potential a door might be left unlocked or a lock may be picked. On one hand, LSU stores very sensitive data—such as medical and student loan records. But because it is a research institution, it has to make sure other types of data can flow freely. We walk a fine line between being too permissive and locking down the entire network" (Fender, 2006).

Another major dilemma is decentralization. Mary Ann Blair, director of information security at Carnegie Mellon University, notes, "Because we're a highly decentralized institution, it is difficult to know where all repositories of sensitive data reside. We know what is on our central systems, but we don't necessarily know every shadow or feeder system that has been created or what specific data they might hold. Moreover, by policy we do not look at content, and that creates discovery barriers. We need to develop methods for determining where personally identifiable data exists within our

networks. We need to be able to say that a machine was compromised but not any of its data. We need to position ourselves with logging and forensics so we can make those assertions."

In this chapter we address programs and practices colleges and universities have in place to respond to IT security incidents. How many incidents are reported to the press, what are the perceived IT security risks, what is their impact, and how are incidents responded to? Are some institutions more vulnerable than others and why? What is the impact on the institution?

The combination of university systems' open nature and the high-powered technology often present on campuses puts academic institutions in a unique position of risk, compared to other large enterprises. 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 digital assets.

IT Security Incidents

Ten percent of our survey respondents indicated that they had an IT security incident in the past 12 months that had been reported to the press (down from 19 percent in 2003—a reduction of almost 50 percent). Doctoral institutions had slightly more incidents than other Carnegie class institutions.

Nothing catches senior management's attention more than negative press coverage. Management tends to react to security breaches, like any hot topic, in a crisis mode. Georgia Tech is especially sensitive to this issue after experiencing a highly publicized compromise of credit card numbers off a server. According to director of internal auditing Rob Clark, "We don't want to be the lead story on the six o'clock news again. We sat in a meet-

ing with the president after the incident. The president looked at me, the CIO, and said, 'This will never happen again.' He made it clear that we needed to dedicate necessary resources to ensure that a high-profile incident never happened again. Everyone dropped whatever they were doing to address this because this was a matter of urgency."

The dilemma for CIOs is that most security incidents are not newsworthy and do not catch the attention of press but require resources—financial and staff. The primary perceived risks by our respondents are viruses (72.6 percent), theft of personal financial information (64.8 percent), and incidents such as spoofing and spyware (55.3 percent) (see Table 6-1). Significantly lower are denial of service (30.5 percent) and copyright issues (25.2 percent). Our respondents are least worried about fraud (2.6 percent) and embezzlement (0.6 percent). We found minor variation by Carnegie class: Respondents from doctoral institutions were more worried about intellectual property, and

those with higher FTE enrollments were more worried about theft of personal information. Baccalaureate institution respondents were more worried about unlicensed use of digital products, and those from AA institutions were more worried about vandalism and employees' misuse of computers. Note that this battery of questions was not asked in 2003, so no comparisons are possible.

A majority of respondents (74.2 percent) report that the number of incidents is about the same or fewer in the past 12 months, compared with the year before (see Table 6-2). There was little variation by Carnegie class.

Figure 6-1 shows the change in the number of incidents in the past 12 months, by FTE enrollment. The change in incident level varies, with respondents with higher FTEs being subjected to higher levels of incidents. Recent articles in the press and elsewhere have reported a growing number of incidents in higher education and a higher level of risk. Our data do not support these claims.

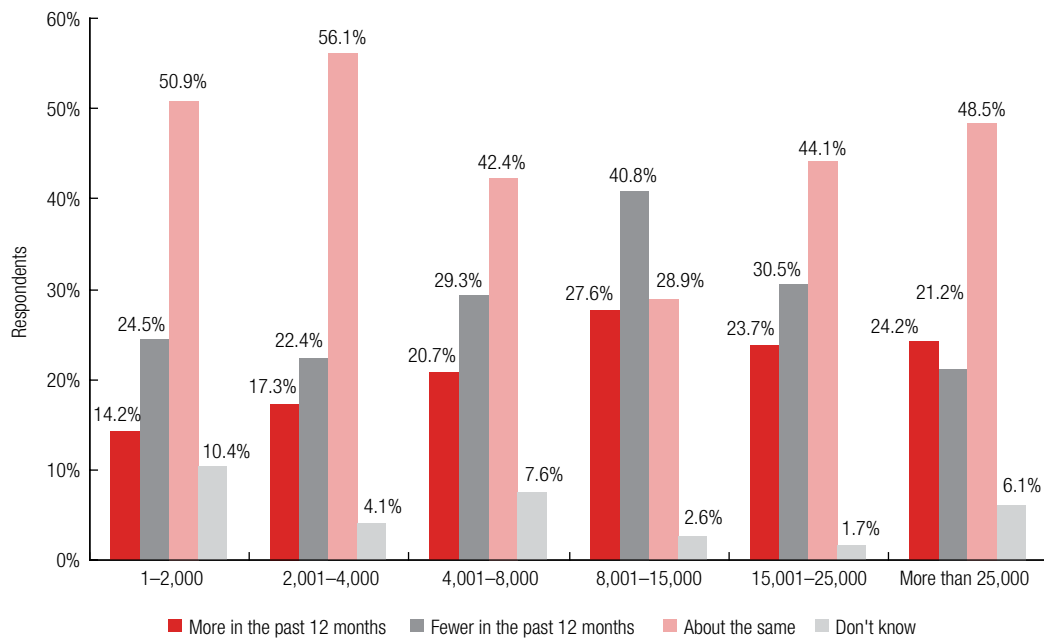
Table 6-1. Perceived Risks (N = 492)

Risk	Percentage
Computer virus, worm, or Trojan horse	72.6%
Theft of personal financial information (SSN, credit/debit/ATM card, account or PIN numbers, etc.)	64.8%
Other computer security incidents (hacking, spoofing, sniffing, ping, scanning, spyware, etc.)	55.3%
Denial of service	30.5%
Unlicensed use or copying (piracy) of digital products (software, music, motion pictures, etc.)	25.2%
Breaches resulting from information obtained from stolen laptops	11.0%
Electronic vandalism or sabotage	10.4%
Misuse of computers by employees (Internet, e-mail, etc.)	10.0%
Theft of intellectual property (copyrights, patents, trade secrets, trademarks)	7.7%
Fraud	2.6%
Embezzlement	0.6%

Table 6-2. Number of Incidents in the Past 12 Months (N = 483)

	Number	Percentage
More in the past 12 months	97	20.1%
About the same	223	46.2%
Fewer in the past 12 months	135	28.0%
Don't know	28	5.8%
Total	483	100.0%

**Figure 6-1.
Change in the
Number of
Incidents in the
Past 12 Months,
by FTE Enrollment
(N = 464)**



Moreover, our data show that one cannot generalize to higher education as a whole but must take into account enrollment size and, to a lesser degree, Carnegie class.

We asked what damage and losses were incurred in the last year and found that more than one-third of the respondents (33.7 percent) identified business applications being unavailable, followed by the network being unavailable (29.4 percent) (see Table 6-3). More than one-quarter of respondents (26.0 percent) had data compromised. Fewer than 10 percent reported identify theft, damage to hardware, and financial losses. The risk of identity theft

and compromised information confidentially is reported to be slightly higher at doctoral institutions.¹ We also find that the larger the FTE enrollment, the greater the damage (or loss) incurred, especially with identify theft and negative publicity in the press.

We reviewed CSI/FBI data that permits a limited comparison with business (see Table 6-4). The biggest differences are network unavailable (29.4 percent for higher education versus 49.0 percent for businesses), information confidentiality compromised (26.0 percent for higher education versus 16.0 percent for businesses), and financial

Table 6-3. Damage (or Loss) Incurred in the Past Year (N = 490)

Damage or Loss	Percentage
Business application, including e-mail, unavailable	33.7%
Network unavailable	29.4%
Information confidentiality compromised	26.0%
Damage to software	21.5%
Damage to data	12.5%
Negative publicity in the press	10.0%
Identity theft	8.4%
Damage to hardware	7.4%
Financial losses	6.4%

Table 6-4. Loss Experience: Comparison Between Higher Education and Business

Damage or Loss	ECAR Survey (N = 490)	Business (N = 700)
Business application, including e-mail, unavailable	33.7%	38.0%
Network unavailable	29.4%	49.0%
Information confidentiality compromised	26.0%	16.0%
Damage to data	12.5%	11.0%
Identity theft	8.4%	5.0%
Damage to hardware	7.4%	5.0%
Financial losses	6.4%	21.0%

losses (6.4 percent for higher education versus 21.0 percent for businesses). (See data from the CSI/FBI Computer Crime and Security Survey at <<http://www.fbi.gov/page2/july05/cyber072505.htm>>.)

IT Security Incident Handling Procedures

We asked respondents whether their institution had a formal IT security incident handling procedure. More than 48 percent said yes (up slightly from 45 percent in 2003). This compares with 40 percent in the CIFAC study (Rezmiarski, Rothschild, Kazanis, & Rivas, 2005). We

found that doctoral institutions (75.8 percent) are most likely to have an IT security incident handling procedure (see Figure 6-2). Also, the larger the student enrollment, the more likely the institution is to have an incident handling procedure (see Figure 6-3).

Miami University of Ohio's William Custer notes that his institution created an IT security office and hired additional staff (moving from 1.5 to 4.0 FTE): "We've adopted a five-year plan for security in the security office. We've focused on preparedness instead of simply response and detection prior to an event. We've paid attention to security components

Figure 6-2.
IT Security
Incident Handling
Procedures, by
Carnegie Class
(N = 413)

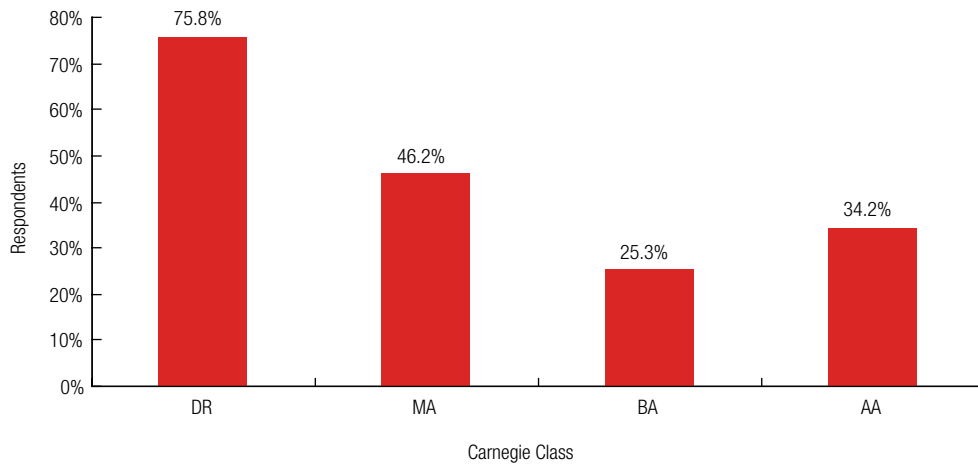
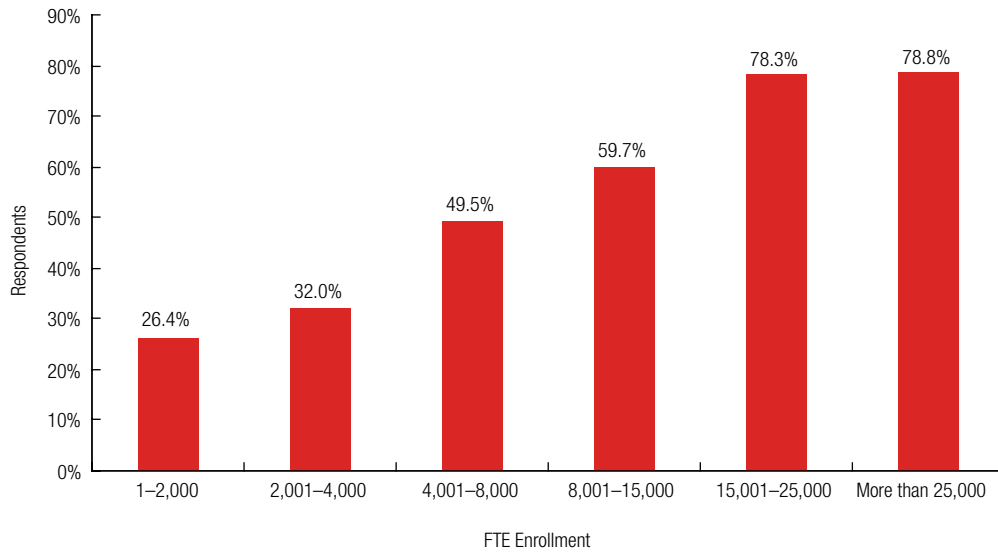


Figure 6-3.
IT Security
Incident Handling
Procedures, by FTE
Enrollment
(N = 473)



for network architecture and also server hardening. And we've focused on accountability through policy." He added, "We've upgraded our firewalls. We have incorporated intrusion detection. We have implemented a heightened password awareness program. We've done a policy gap analysis. We've increased our use of VPN. We consistently implement the latest virus protection and operating system patches."

For the 204 institutions in the 2003 and 2005 studies, doctoral institutions show the greatest change in security handling procedures from 2003 to 2005: 77.6 percent

reported having such procedures in 2005, versus 67.1 percent in 2003. The other Carnegie class institutions are virtually unchanged. The CIFAC study notes that if procedures are in place, they are well followed (81 percent of respondents) and felt to be effective (69 percent of respondents) (Rezmierski, Rothschild, Kazanis, & Rivas, 2005).

Who Is Involved in IT Security Incident Handling Procedures?

We asked for further elaboration on who gets involved if an incident occurs (see Table

6-5). In descending order, 86.6 percent of respondents included the police and campus security offices, 83.5 percent involve legal counsel, 79.7 percent involve the student judicial affairs office, 73.3 percent involve institutional relations, 71.3 percent engage human resources, and 70.3 percent involve data stewards.² The big change from 2003 to 2005 for the 204 institutions that participated in both studies is the involvement of legal counsel (88.2 percent from 77.7 percent, a change of 13.5 percent) and communications/public relations (79.5 percent from 67.0 percent, a change of 18.7 percent). Note also that doctoral institutions are far more likely than other Carnegie class institutions to involve legal counsel.³

Intrusion Detection Systems and Projected Changes

Participants at the 2005 Cybersecurity Summit at Tyson's Corner made several recommendations to improve security by means of intrusion detection systems. In Chapter 3, we noted that 55.7 percent of the respondents in the study had an intrusion detection system.

Summit participants noted that "intrusion detection systems were determined to be very

useful, and sites not deploying them should evaluate utilizing them." They also reached the following conclusions:

- ◆ Flow tools are useful as a complement to an intrusion detection system, and sites should start collecting and analyzing flows.
- ◆ Syslog data is useful as a host intrusion detection system, and sites should set up a centralized syslog server.
- ◆ Data correlation from different sensors (such as syslog and IDS data) is proving to be a valuable tool.
- ◆ Sites should have an out-of-band communication method (such as encrypted e-mail or Jabber servers), which has proven very useful in incident response.
- ◆ Site operators need to know the requirements and laws they fall under, including reporting needs, data collection procedures, and legal aspects.

Mary Ann Blair predicts that we will see a continued migration toward centralization and reduced distributed data, more encryption, and adoption of tools that let us more readily assess vulnerabilities. Today, many places have one open network. "I expect to see administrative work cordoned off from other work, and more segregation of network traffic," says Blair.

Table 6-5. Who Is Involved with IT Security Incident Handling Procedures? (N = 204)

Participant	Percentage All (N = 492)	Percentage 2005 (N = 204)	Percentage 2003 (N = 204)	Rate of Change (N = 204)
Police/public safety	86.6%	87.4%	86.5%	1.0%
Legal counsel	83.5%	88.2%	77.7%	13.5%
Student judicial affairs/dean of students	79.7%	81.8%	78.8%	3.8%
Communications/public relations	73.3%	79.5%	67.0%	18.7%
Campus human resources office	71.3%	68.0%	N/A	N/A
Data stewards	70.3%	65.7%	N/A	N/A

Note: Comparisons of changes between 2003 and 2005 are based on data from the 204 institutions that participated in both studies.

Summary

Higher education continues to improve its ability to respond to security breaches. It has done so by involving more senior campus officers and establishing incident handling procedures. Security incidents as perceived by the respondents do not seem to have increased in the two years of analysis covered by this study, and higher education incidents and their consequences are not unlike what is reported for the business sector.

Endnotes

1. The CIFAC study categorizes incidents into three broad groups: 29.3 percent are people-focused, 26.5 percent are data-focused, and 44.2 percent are systems-focused (Rezmierski, Rothschild, Kazanis, & Rivas, 2005).
2. These percentages are comparable with the findings in the CIFAC study (Rezmierski, Rothschild, Kazanis, & Rivas, 2005).
3. The CIFAC study concluded that interdepartmental response teams are increasing on U.S. campuses (Rezmierski, Rothschild, Kazanis, & Rivas, 2005).