

1

Executive Summary

It is my ambition to say in ten sentences what other men say in whole books.

—Friedrich Wilhelm Nietzsche

Longitudinal data on IT security in higher education affords us an opportunity to better understand change and stability in our industry. In contrast, cross-sectional data and its analysis give us a 10,000-foot snapshot of the state of the practice at a particular time. This ECAR study does both: it provides a cross-sectional perspective of the state of higher education's IT security practice in 2005 as well as a longitudinal and empirical perspective of change and trends in higher education's IT security environment. Both analyses are intended to help guide the improvement of information security for higher education.

ECAR's 2003 study established a security baseline for higher education. It identified what security policies, products, and procedures were currently in place. This second study shows what has happened in two years, and the findings are exciting. We are witness to a sea change in the practice and management of IT security in higher education.

Providing secure IT services to colleges and universities is a special, if not unique, challenge. Unfettered and timely access for all to enormous quantities of information is higher education's lifeblood and is key to its success in educating its students and generating new ideas and know-how. Insensitive, political, or casual attempts to check and control

this dynamic transmission and consumption of information are problematic at best and potentially deleterious to the academic mission. On the other hand, thoughtful and mission-minded implementation of IT security can and will ensure, protect, and facilitate the requisite flow of information so necessary for higher education's continued success. What we find remarkable is that in just two years, many institutions participating in our study appear to have struck a balance—or perhaps more accurately, an acceptable compromise—between these competing interests.

Methodology

We addressed the issues using a multifaceted research methodology. We gathered quantitative data from 492 higher education institutions (459 U.S. institutions and 33 Canadian institutions). Four data collection and analytical initiatives were undertaken.

- ◆ We began with a review of literature published in the period 2003–2005. We paid particular attention to IT security surveys undertaken by various IT security organizations and online IT newsletters.
- ◆ Consultation with members of the EDUCAUSE/Internet2 Computer and Network Security Task Force was undertaken

to align the survey with their initiatives and to identify and validate the most interesting research questions and hypotheses that would frame the construction of a quantitative survey instrument. A major purpose of this study is to inform the agenda of this task force. In addition, we interviewed senior IT leaders at 17 higher education institutions and at EDUCAUSE for further insight into IT security (see Appendix B).

- ◆ A quantitative Web-based survey first constructed in 2003 was modified for use in 2005. It recognizes new technologies in use and adheres to policy and practice recommendations of the EDUCAUSE/Internet2 Computer and Network Security Task Force.
- ◆ A longitudinal analysis compared 2003 findings with those for 2005. Fully 204 institutions responded to our survey in both 2003 and 2005, and we highlight the changes that occurred in that subset of respondents recognizing that different individuals may have completed the survey. Also discussed are contrasting data on IT wireless security from ECAR studies in 2001 and 2005.

Key Findings

The worm attacks of late 2003 and changes in the nature of threats seem to have driven many institutions to improve their defenses. Among many interesting findings in this study was the growth in firewall use, which many respondents said they were not fond of in 2003. Of particular note was the 22 percent growth in research universities' use of perimeter firewalls since 2003. Many research institutions ardently stated that perimeter firewalls would not be an effective solution in their environment when we spoke with them during the 2003 study. Also significant was the 27 percent growth in the use of interior firewalls across all Carnegie classes. Other rapidly growing technologies included virtual

private networks, up more than 65 percent, and intrusion detection and prevention systems, each up more than 30 percent. We also saw a 55 percent jump in the use of enterprise directories and nearly a doubling in the use of active filtering technologies. These statistics show that respondents have taken the threat of attack seriously and taken steps to protect themselves.

Although our statistics show that higher education has made significant progress in advancing its use of security technologies, some areas still could be improved. Despite the high growth rates, fewer than half of the respondents to this survey were using intrusion prevention systems, 34 percent did not use interior firewalls, and nearly 25 percent did not have centralized data backup capabilities. Also telling was the lack of change in the authentication methods used by our 204 respondents since 2003. Fully 95 percent of respondents reported still using traditional username and password combinations. While almost 60 percent indicated they also use strong passwords within their organizations, only 27 percent were using Kerberos, and fewer than 10 percent reported the use of any multifactor authentication mechanism such as hardware tokens (SecureID), biometrics, or PKI. This is an area where higher education continues to lag broader industry benchmarks.

In 2003, our respondents were, as a whole, more focused on technical solutions and put less emphasis on the "softer" aspects of IT security such as planning, training, auditing, and codifying policies and procedures. The current study shows tremendous growth rates in the cultural aspects of security. More than 34 percent of respondents now have a chief information security officer, up from 20 percent in 2003, and 62 percent of respondents now report having a centralized IT security function, up from only 39 percent in 2003. The number

of respondents offering IT security awareness programs jumped by 26.5 percent, with the largest reported program growth targeting faculty. In the area of planning, we saw a huge change from 2003 to 2005, with a 49 percent increase in respondents reporting either a partial or complete security plan in place. The number of institutions that had conducted a risk assessment increased by 77 percent. We also found a substantial reported increase in senior management's interest in IT security issues.

Despite the quantum leap forward in many of the cultural aspects of security, there is room for improvement. Although most respondents had some security policies and procedures in place, their coverage lacked uniformity. For example, nearly 11 percent did not cover data backup, nearly 15 percent did not cover authentication and authorization, nearly 20 percent did not cover physical security, nearly 28 percent did not document individual employee responsibilities for security, and more than 30 percent did not cover disaster recovery. More than 50 percent did not report having formal incident response procedures in place, nearly 50 percent don't test new applications for security, and nearly 70 percent had not established security standards for application or system development. Fully 20 percent of respondents indicated that no plan of any type was in place for IT security. Fewer than 10 percent of respondents indicated they had undergone a comprehensive risk assessment in the last two years, and more than 40 percent still had not performed any type of risk assessment.

On the whole, we found that respondents rated the success of their IT security programs lower in 2005 than in 2003, although they did rate some aspects of their programs more highly. Some key indicators, such as the barriers facing institutions as they deal with security, improved significantly. For example, 15 percent fewer respondents cited lack of

awareness as an issue in 2005. There was a much higher assessment of the security of central applications, networks, and data than of those that are locally controlled.

We feel that several factors influence this lower rating of overall success. First is the changing nature of threats. Because attacks target data rather than systems and networks, the defenses deployed to date are inadequate; they are generally weaker in decentralized areas where many new attacks are targeted. Also, institutions may have a greater awareness of the complexity of developing a comprehensive security program to combat these changing threats. Added to this is the complexity of managing security in the higher education environment, where many systems are not centrally controlled.

In the 2003 study, one of the key findings was that institutions needed to balance their use of technology with their use of cultural tools to better combat IT security threats. In this study, we certainly see that higher education made significant strides in this area, as well as in technical improvements, and that defenses are more robust than they were several years ago. However, the disparity in perceived security between central and local systems found in this study, along with the other areas highlighted as possibilities for improvement in this chapter, now put the spotlight on a new need: development of enterprise security programs that are designed to protect the entire institution—not just the central systems—in a coordinated, flexible manner.

The higher education community has come a long way in the last two years in accepting prescribed behaviors to make its environment more secure. The culture has changed, and dramatically. Overall, respondents feel more secure today than two years ago despite being in a perceived riskier environment. Respondents feel that the academic community has become more sensitive to security and privacy in the last two years. They feel that the security of centrally

controlled assets has risen somewhat but that locally controlled assets are still at significant risk. This finding indicates that while numerous specific measures have been implemented to help make institutions more secure, such efforts have not come together into institution-wide programs designed to address the spectrum of threats an institution faces across the full range of institutional IT assets.

The study identified several factors driving the need for more comprehensive IT security programs. These include the changing nature of threats—from attacks on servers and networks to attacks seeking personal data—as well as demands from external parties, including government agencies and financial institutions seeking consistent, effective security practices from their partners.

To help institutions move forward on an enterprise security program, the study lays

out a set of leading practices, including the development of governance, requirements, controls, training, assessment, monitoring, and remediation, that work in the context of the institution's culture and structure.

Organization of the Study

The study begins with an explanation of the methodology used. It then proceeds to look at the hard side of IT security, that is, technologies used. This is followed by a discussion of the soft side of IT security—organization, staffing, planning, policies, policy enforcement, awareness programs, and budgets. It then examines IT security incidents, discussing incident rates, challenges, and proposed solutions and determinants of success. Lastly and in summary, it outlines the evolution of technology practices.