

2

Methodology

*There are two kinds of statistics, the kind you look up,
and the kind you make up.*

—Rex Stout

Key Findings

- ◆ From 2003 to 2005, respondents to the IT security survey moved toward the senior IT leadership—the CIO or specially designated IT security professionals—and away from less senior IT managers.
- ◆ The average number of years of experience with IT security self-reported by our respondents was 13.9 years, and 24.3 percent reported over 20 years of experience. Comparative data suggest that our respondents appear to have more IT security experience than their private sector counterparts.

Using a multifaceted research methodology, this ECAR study gathers quantitative and qualitative data from 492 higher education institutions (459 U.S. institutions and 33 Canadian institutions). One-third of the respondents are ECAR subscribers.

The data provide a comprehensive view of higher education's collective experience with IT security and the state of the practice in 2005. Equally important, having 2003 and 2005 data permits comparisons of the state of the practice over a two-year period. Also, data from the ECAR 2001 wireless study (Arabasz & Pirani, 2002) are used to demonstrate rates of change over four years in the use of IT wireless security.

We show that an organizational, technological, and behavioral sea change has occurred in virtually every aspect of IT security

in higher education. Equally significant are findings that IT security has been significantly improved in an environment that is far more diverse and complicated than what confronts many other industries, public and private.

What Do We Mean by Information Security?

By far the most commonly used meaning for information security in the literature is the preservation of the following characteristics:

- ◆ *Confidentiality*, by which we mean protection from unauthorized use or disclosure of information.
- ◆ *Integrity*, by which we mean ensuring the accuracy and completeness of the data through protection from unauthorized, unanticipated, or unintentional modification. Included here are *authenticity* (the ability of

a third party to verify that the content of a message has not been modified in transit), *nonrepudiation* (the origin or receipt of a specific message must be verifiable by a third party), and *accountability* (an action can be traced to a unique entity).

- ◆ *Availability*, by which we mean making data available to authorized users on a timely basis and when needed.

This was the definition we used in 2003, and we see no reason to change it. Each of these five protection categories (confidentiality, authenticity, nonrepudiation, accountability, and availability), in turn, can be categorized by a level of sensitivity: high (grave injury to an institution), medium (serious injury to an institution), and low (minor injury to an institution). These injuries occur when a category is compromised.

The above nuance is significant for higher education. Much of higher education's information that is used for teaching and research requires the highest level of integrity and availability but a low level of confidentiality. For public institutions, this is also true for much of their financial information. However, in areas protected by FERPA (Family Educational Rights and Privacy Act), HIPAA (Health Insurance Portability and Accountability Act), and Gramm-Leach-Bliley, and with sensitive research, for example, all five protection categories must be at the highest level. A compromise in any one area potentially puts the institution at significant risk.

A challenge, then, is to build information systems that can support the institution's public and open missions and the academy's intellectual curiosity while protecting the privacy and intellectual property of the institution and its community. Higher education's information systems must be both open and closed, depending on what kind of information is being viewed and used, and for what purpose. Flexibility is key here and it must accommodate both security needs and the values of the

campus culture. Our study is designed to address these potential contradictions and to assess the ability of higher education to resolve these matters. It may well be that these problems no longer have a basis in fact despite reports to the contrary.

Newspaper reports and other studies that use less robust data and methods often portray higher education as less secure than other industries, in part because of its values such as academic freedom and freedom of expression, its decentralized organization, the *mélange* of hardware and software in use, and its unique mission and user base. Indeed, in many collegiate environments, particularly larger ones, a decentralized culture is the norm. As a result, individual schools, laboratories, and departments may control a portion of any or all of their IT assets, making the job of the institution's IT security administrator much more difficult. Rather than being able to automatically push new security patches out to all devices on the network, or mandating the use of security tools like virus protection software, many university IT security officers are put in a position of having to educate and persuade their user community to keep their machines secure.

Also, a higher education institution's technology environment, even in a small institution, varies significantly from the typical corporate structure. One of the biggest differences is that a large percentage of machines on a university's network are not actually owned by the institution but may belong to students connected to the institution's network in a dorm room, classroom, or other location. Having machines not owned by the institution connected to the network means that the security administrator must assume there will always be insecure systems inside the institution's perimeter, and additional protective steps may be required that would not be necessary in a more controlled corporate environment.

A typical university engages in a wide range of business activities as part of its mission. In addition to teaching, many institutions conduct a wide range of research, provide hospitality services (dorms and dining halls), serve as an Internet service provider, act as a phone company, engage in retail sales (bookstore, food concessions), manage financial accounts, provide entertainment (athletics, arts), and conduct many other diverse activities. As a result, the IT environment of all but the smallest colleges is by necessity complex and is constantly changing. And at many institutions, the selection and maintenance of the systems used to support these functions is left to the individual campus units.

Institutions that attract significant research funding have some unique issues of their own. By their nature, research labs encourage experimentation and often have extremely diverse computing environments. Managing an IT security environment that incorporates a large research community therefore poses some special challenges for administrators.

But none of these issues is insurmountable, and we will show that in the last several years, IT security administrators in higher education have found effective ways to move forward in these complex environments.

Research Approach

Four data collection and analytical initiatives were undertaken: a review of literature, consultation, a quantitative Web-based survey, and a longitudinal analysis.

A review of literature published from 2003 to 2005 complements the literature review undertaken for the 2003 study. This effort further identifies and clarifies issues of concern to the higher education community and creates additional hypotheses to be tested. Note that the extant work focusing primarily on higher education and IT security continues to be minimal. The vast majority of the electronic magazine literature focuses on business.

Books and articles in professional journals provide analysis of available technologies. Exceptions are the publications and task force reports of EDUCAUSE and the *Chronicle of Higher Education*. The federal government's publications and the professional organizations place great emphasis on planning, policies, preparedness, and awareness, which have informed the design of our survey.

ECAR again paid particular attention to IT security surveys undertaken by various security organizations and online IT newsletters. When appropriate, ECAR included questions that mirrored those in these surveys, which makes possible a limited but useful comparison of higher education with other sectors of the economy.

Because IT security technologies and practices are undergoing such rapid change, the most up-to-date information available is on the Web. A short list of references (Appendix C) and other resources (Appendix D) accompany this study, providing addresses for the Web sites we used and found helpful. The references are not intended to be comprehensive. Also, because the terminology used can be confusing to a lay reader, we have again added a glossary (Appendix E).

Consultation with members of the EDUCAUSE/Internet2 Computer and Network Security Task Force and others was undertaken to align the survey with their initiatives as well as 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 survey is to inform the agenda of the EDUCAUSE/Internet2 Computer and Network Security Task Force. We also interviewed professionals recognized for their expertise in this area and added their critical insight to the text of the study (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 is informed by policy and practice recommendations of the EDUCAUSE/Internet2 Computer and Network Security Task Force.

EDUCAUSE staff sent an e-mail invitation with the survey's Web address and access code information to EDUCAUSE member institutions. Senior college and university administrators, the majority of whom were CIOs and other IT leaders, from 492 institutions responded to the survey. Their responses provide a detailed understanding of how higher education approaches IT security. The survey's questions appear on the ECAR Web site, <http://www.educause.edu/ir/library/pdf/ecar_so/ers/si/ESI05G.pdf>. Appendix A lists the survey respondents. We note that the information collected is confidential. No data from the quantitative survey are presented that would make it possible to identify a particular institution or respondent, and the data files we use for analysis have been purged of any data that would have similar consequences.

A longitudinal analysis comparing findings for 2003 with those for 2005 was completed. Fully 204 institutions responded to our survey in both 2003 and 2005, and we highlight the changes that have occurred in that subset of respondents recognizing that different individuals may have completed the survey (see Appendix A for a list of these respondents). Also discussed are contrasting data on IT wireless security from the 2005 and 2001 ECAR studies.

Most ECAR studies involve cross-sectional analysis, which provides us with a snapshot of a sample of a population at a single point in time. Longitudinal analysis lets us examine change over time, although it does not necessarily provide us with insight as to how or why the changes have taken place. Most IT security studies, such as the CSI/FBI studies, do trend analysis, a type of longitudinal analysis based on different populations. These are useful but not anywhere near as sound as a panel study. In a panel study, the same

people (in our case, representatives from the same institution) are interviewed at two or more points in time. Since the sample is the same, any changes we observe are not a result of sampling error and the change noted is statistically of greater interest.

The following topics are not included in depth in this study, because they are very important and large enough to warrant separate study:

- ◆ business continuity or disaster recovery,
- ◆ ID management,
- ◆ physical security,
- ◆ legal and ethical issues such as copyright violations,
- ◆ legislative mandates such as FERPA and HIPAA, and
- ◆ academic freedom and privacy.

Analysis and Reporting Conventions

ECAR study tables and figures typically depict numbers and percentages to the first decimal place. Percentages in some tables and figures do not add up to 100 percent because of rounding.

Carnegie Class as a Distinguishing Factor

The study grouped the sample by a modified Carnegie Classification of Institutions of Higher Education (see <<http://www.carnegiefoundation.org/classifications/index.asp>>). The Carnegie taxonomy describes the institutional diversity in U.S. higher education. Most higher education projects rely on the classification to ensure a representative selection of participating individuals and institutions. We also believe that IT security strategies will differ by Carnegie class because missions, academic culture, and size vary significantly for each Carnegie group. Note, however, that the Carnegie classification is undergoing significant change, and it is too early for this study to respond to the

proposed changes. As a consequence, we will use Carnegie class basically to help institutions compare themselves with similar institutions as appropriate and not use it as an independent variable for analysis purposes. Note, too, that the 2005 study shows far less difference in IT security practice by Carnegie class than was the case in 2003.

The study collapsed the Carnegie categories as follows to obtain larger numbers for descriptive purposes:

- ◆ Doctoral/research universities (DR)—doctoral extensive and doctoral intensive. Doctoral-extensive institutions typically offer a wide range of baccalaureate programs, and they offer graduate education through the doctorate. They award 50 or more doctoral degrees per year in at least 15 disciplines. Doctoral-intensive institutions are similar with respect to baccalaureate education. They award at least 10 doctoral degrees per year in three or more disciplines, or at least 20 doctoral degrees per year overall.
- ◆ Master’s colleges and universities (MA). The study grouped both Master’s Colleges and Universities I and Master’s II together. These institutions typically offer a wide range of baccalaureate programs as well as graduate education through the master’s degree.
- ◆ Baccalaureate colleges (BA). The study

grouped the three baccalaureate college groups into a single BA group. Baccalaureate colleges are primarily undergraduate colleges with major emphasis on baccalaureate programs.

- ◆ Associate’s colleges (AA). These are institutions that offer an associate’s degree and certificate programs but, with few exceptions, award no baccalaureate degrees.

We also provide data where appropriate on higher education system offices and for the 33 Canadian respondents in our study, recognizing that they too vary by size and mission. Because the N is too small for meaningful analysis of institutions classified by Carnegie as “system” or “other,” they are excluded from analysis when Carnegie class is used as a variable.

Thirty-eight percent of the respondents in our study are private; 62 percent are public. We found little difference along this dimension.

Institutions in the Survey and Their Characteristics

Figure 2-1 compares the distribution of the institutions that responded by their Carnegie class, EDUCAUSE membership, and the universe of higher education institutions in the United States. The responding schools mirror much more closely the EDUCAUSE membership than the national population

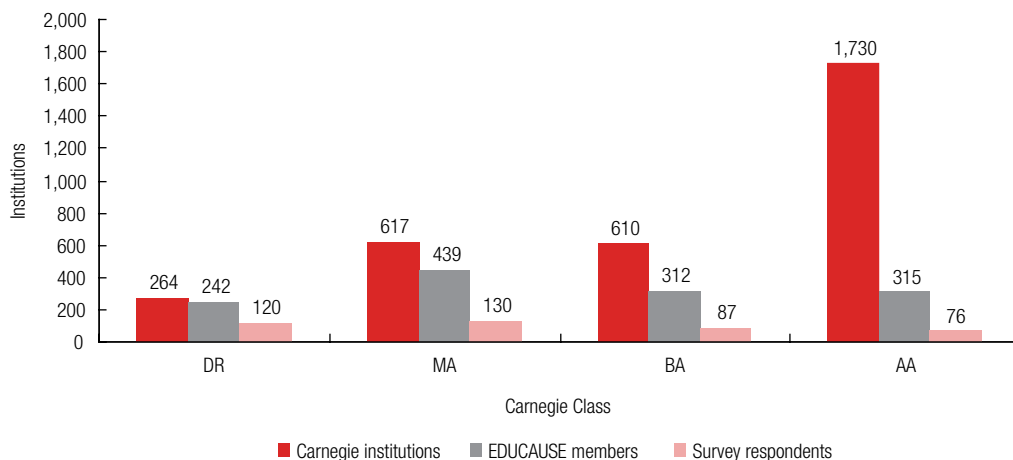


Figure 2-1. Survey Respondents, by EDUCAUSE Membership and Carnegie Class

of institutions by Carnegie class. Note that the 204 institutions used for comparison between 2003 and 2005 are weighted slightly higher (less than 5 percent) toward DR and MA institutions.

The study relied on volunteers to complete the survey rather than a random sample, and this limits the statistical conclusions that are possible. Nevertheless, the overall 30 percent response rate from EDUCAUSE member institutions gives us confidence that the study's respondents portray a reasonable image of the EDUCAUSE institutional membership.

A statistical analysis of the representativeness of the data proved to be inconclusive. On the one hand, the findings do not support the conclusion that the institutions surveyed represent the population as whole. Nor do they support the opposite conclusion that the respondents fail to represent the EDUCAUSE membership. Neither is statistically significant.

Size of Institution: Number of FTE Students

The IT security literature on the business sector uses size as a significant variable that explains, in part, how much corporations are willing to spend on security. The larger the corporation and the greater the number of users, the lower the per capita expenditure on security. Does number of FTE enrollments

make a difference in higher education? In 2003 FTE enrollments made a difference. In 2005 FTE enrollments were less significant, but we do see differences, especially in areas of planning and awareness programs. Smaller institutions apparently lack the necessary staffing resources to address comprehensive awareness programs and needs.

The mean student enrollment of the institutions in our study was 8,375 in 2005, compared with 7,169 in 2003. The distribution of responding institutions appears in Table 2-1.

Smaller institutions dominate our study, just as they dominate U.S. higher education. Forty-four percent have 4,000 or fewer enrolled students. Fewer than 20 percent of the institutions in the study have more than 15,000 students. This distribution is very similar to that of 2003. Note that system enrollments are not included in Table 2-1.

The Respondents: Position in the Organization and Experience

The survey was completed largely by CIOs (52.6 percent) and chief IT security officers (21.1 percent) and reflects their experiences, observations, and opinions on IT security (see Figure 2-2). Academic, financial, and other administrative officers represent 2.4 percent of the respondents. We emphasize that this

Table 2-1. Size of Institution, by FTE Student Enrollments (N = 473)

Student FTE Enrollment	Number	Percentage
1–2,000	110	23.3%
2,001–4,000	100	21.1%
4,001–8,000	93	19.7%
8,001–15,000	77	16.3%
15,001–25,000	60	12.7%
More than 25,000	33	7.0%
Total	473	100.0%

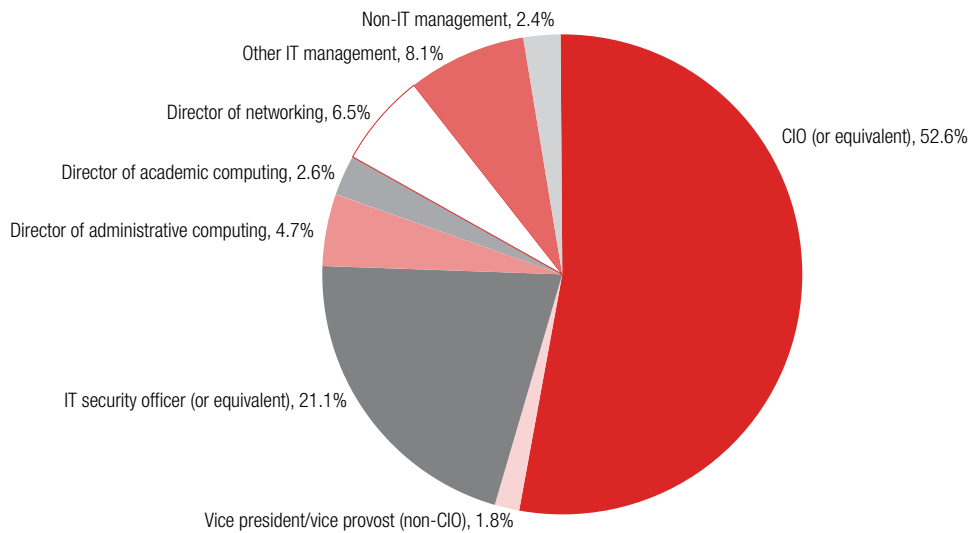


Figure 2-2.
Respondents'
Administrative
Titles (N = 492)

study is largely a CIO/IT management view of IT security moderated by observations of other institutional leaders obtained through complementary in-depth qualitative surveys and the study's IT security advisors.

We note significant differences in the respondents' positions in 2005. We compared the titles of individuals who completed the survey in 2005 and 2003 at the 204 schools that were in both surveys (see Table 2-2). CIOs and IT security officers have replaced directors of networks and of academic and administrative computing both as respondents and, we suspect, as individuals responsible for IT security. Note especially the rate of change for IT security officers (96.7 percent). As IT security has increasingly come to the forefront of senior management's attention, it appears that responsibility for IT security has moved to the senior IT leadership or specially designated IT security professionals.

The respondents are, as a whole, very experienced with IT security. Their average experience was 13.9 years, and 24.3 percent reported more than 20 years of experience with IT security. These numbers did not change significantly between 2003 and 2005.

One interesting comparison is with the years of experience found for IT professionals globally in the IDC 2005 Global Information Security Workforce Study (see <http://www.securitymanagement.com/library/globalinformation_itsecurity0206.pdf>). Fully 4,305 private and public entities from around the world responded to their survey. Individuals responsible for IT security in higher education self-reported more experience than what IDC found. In both studies, about 25 percent of individuals responsible for IT security self-reported experience of five years or less. However, 47.7 percent of the IDC study respondents had five to 10 years' experience, compared with 27.3 percent for our respondents. Noteworthy is that 40 percent of the IDC respondents had more than 10 years' experience, in contrast with 48.2 percent for the respondents in our survey. When comparing the IDC numbers for the Americas only, our U.S. and Canadian respondents scored higher.

Our respondents bring a great deal of experience to our study as well as a view of IT security from a variety of IT positions and institutions within higher education. We are gratified by the number of respondents, which makes the findings more than simply

Table 2-2. Change in Respondent's Title (N = 204)

Title	2005	2003	Percentage Change	Rate of Change
IT security officer (or equivalent)	29.9%	15.2%	14.7%	96.7%
CIO (or equivalent)	49.5%	43.1%	6.4%	14.8%
Director of academic computing	1.5%	2.5%	-1.0%	-40.0%
Director of administrative computing	4.9%	6.9%	-2.0%	-29.0%
Vice president/vice provost (non-CIO)	1.0%	3.4%	-2.4%	-70.6%
Other academic management	0.5%	3.0%	-2.5%	-83.3%
Director of networking	5.4%	8.8%	-3.4%	-38.6%
Other IT management	7.4%	17.2%	-9.8%	-57.0%

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

the observation of a small subset of the industry. In the chapters that follow, we present their collective view of IT security in higher education. We begin in Chapter 3 with an overview of IT security technologies

in use at 492 institutions. In Chapter 4 we describe the security culture—the human side of IT security, by which we mean leadership and organization, values, and policies and procedures.