

Foreword

The EDUCAUSE Center for Applied Research (ECAR) was launched on January 1, 2002, to create a body of research and analysis on important issues at the intersection of higher education and information technology. ECAR is fulfilling its mission through a program of symposia and through the publication of

- ◆ biweekly research bulletins oriented to senior campus functional executives;
- ◆ detailed studies designed to identify trends, directions, and practices in an analytically robust fashion; and
- ◆ case studies designed to showcase campus activities and highlight effective practices, lessons learned, and other insights from the practical experience of campus leaders.

Since ECAR's inception, two symposia have been held and close to 60 research publications have been issued.

IT Security in Higher Education

For well over four decades, providing secure IT services to their constituents has been a top priority for college and university administrators. Institutions have invested money and human resources to protect their information assets and those of faculty and students. With no end in sight

to security threats and breaches, their efforts are growing. Rapidly increasing bandwidth demands, the evolution of distributed computing architectures (and governance), and an incredible rise in computer crimes place increasing stresses on higher education's institutions and their computing infrastructures. Even institutions famous for their IT security investments and policies are at risk and have suffered newsworthy break-ins, resulting in the theft of student Social Security numbers, medical records, and other confidential information. Colleges and universities have also been the launch pads for numerous virus and denial-of-service attacks in recent years, creating high public relations, financial, and regulatory problems for higher education as a whole.

EDUCAUSE efforts in this arena have been noteworthy. EDUCAUSE has long been recognized as a major participant in national efforts to secure higher education's communications and computing infrastructure. It has participated with Internet2 to conceive, develop, and deploy technologies, techniques, and standards that enhance identity services and other middleware elements essential to IT security. We especially commend the work of the EDUCAUSE/Internet2 Computer and Network Security Task Force. Mark Bruhn of Indiana University, Ken Klingenstein of Inter-

net2, Mark Luker and Rodney Petersen of EDUCAUSE, Dan Updegrave of The University of Texas at Austin, and Gordon Wishon of the University of Notre Dame deserve particular attention and thanks. In addition to helping secure higher education, these busy people advised us throughout this research. Of course they bear no responsibility for our findings or conclusions. This study's authors also owe thanks to EDUCAUSE for data from the 2002 EDUCAUSE Core Data Service survey.

The EDUCAUSE/Internet2 Computer and Network Security Task Force has identified several issues for further study. These include making IT security a higher and more visible priority in higher education; doing a better job with existing security tools by, for example, revising institutional policies; and designing, developing, and deploying improved security for future research and education networks. In the spirit of the Bush administration's national security goals, the task force is working to raise the level of security collaboration among higher education, industry, and government, and to integrate higher education work on security into the broader national effort to strengthen critical infrastructure.

Despite the national attention and ongoing efforts of EDUCAUSE, Internet2, and other organizations to develop and foster a modern and secure IT infrastructure in higher education, our knowledge of the current state and future plans of colleges and universities vis-à-vis IT security has been largely anecdotal to this point. Leadership is purported to be reactive rather than proactive, with a lack of clearly defined goals. Similarly, the academic culture often finds the goals of security, academic freedom, and intellectual freedom to be antithetical.

This ECAR study is designed to provide a fact-based and national perspective of higher education's security environment that

can lead to the improvement of institutions' cybersecurity. It establishes a security baseline for higher education. It identifies what security policies, tools, and procedures are currently in place. Institutions will be able to compare their own investments and practices with those of similar institutions. Emphasis is placed on both the benefits and risks of implementing security solutions, including trade-offs and future trends.

Important Contributions

ECAR research studies are the result of a team effort. Robert B. Kvavik, ECAR senior fellow and professor at the University of Minnesota, and John Voloudakis, CTO of Cap Gemini Ernst & Young's (CGE&Y) Higher Education Practice, authored this report. Their intellectual leadership is evident in the work itself. Their work was fostered by Judith Caruso, ECAR fellow and director of policy, security, and planning at the University of Wisconsin–Madison, who managed the research project, authored the executive summary, and coauthored the case study of IT security at Indiana University. Judith Pirani led the design, execution, and analysis of this study's qualitative aspects, adding a richness and texture that survey data alone can rarely supply. Former ECAR Fellow Paula King was instrumental in the creation and deployment of the quantitative survey whose results form the backbone of this study and supported the University of Washington case study. Robert Albrecht coauthored the case study of IT security at Indiana University and provided thoughtful commentary on drafts and research design throughout this project.

Of course, the real team in any ECAR study is the EDUCAUSE community. Our ability to develop a good understanding of practices, policies, and directions in higher education depends on our associates' goodwill. Hundreds of busy CIOs and security officers shared their experiences and expertise

on our quantitative survey, and dozens more generously gave their time in interviews. Jim Bruce of MIT, Ron Johnson of the University of Washington, and Michael McRobbie of Indiana University gave our researchers access to their staff for intensive discussions during on-site case visits. We cannot thank them enough.

The EDUCAUSE staff is also part of our community, and our ability to conduct this research depends on their provision of a myriad of services big and small. The EDUCAUSE team is always there when you need them, and their commitment to excellence is evident in all that they do. Thank you.

Finally, ECAR, while now enjoying the support of more than 200 college and university subscribers, continues to depend on the generous support of a small and dedicated cadre of corporate sponsors. Cap Gemini Ernst & Young, Collegis, Datatel, Hewlett-Packard, Microsoft, PeopleSoft, SCT, and WebCT not only provide direct financial support but are also generous with their advice and skilled resources. John Voloudakis of CGE&Y, for example, coauthored this report and was instrumental to the project.

This study reminds us that the opportunities and challenges posed by networked information demand responses that are at once technological and cultural in nature. The story of IT security in higher education is ultimately a story of people—people on the outside and inside of our academies who may have sinister motives, and people on the outside and inside with good intentions but incomplete knowledge of or attention to good practice. These people, good and bad, converge in, on, and around our virtual Commons, which we have optimized to facilitate communication and the free exchange of scholarly ideas. In the end, higher education's potential to secure its stakeholders and their information assets will depend on our IT leaders' creativity, vigilance, investment, and technical sophistication on the one hand and on communication, education, awareness training, and collaboration among institutional subunits on the other. IT security, it seems, is everyone's responsibility.

Richard N. Katz