

Preface

You don't have to look very far to find a president, chief information officer, or public relations director in higher education who can recount a recent incident in which information security was compromised at his or her institution. The stories often contain similar themes: a wide range of problems for victims whose data are lost or exposed, bad publicity for the institution, threats of lawsuits and legal liability, and significant expenditure of energy and resources in recovery and cleanup. Contributing factors often, but not always, include careless behavior by employees or students, faulty system administration by overworked and inadequately trained personnel, inadequate preventive measures, absence of risk analyses and testing for vulnerabilities, outdated policies and procedures, and insufficient supervision or leadership. With such a bleak outlook, is there any hope for a remedy or possible cure?

Although the obstacles and challenges for improving computer and network security in higher education may seem daunting, we have reason for optimism and hope. Significant progress has been made in the past few years by a number of colleges and universities, many of which will be highlighted in this book. This book is designed to provide both a conceptual framework and a launching point for the development of comprehensive information security programs to address risk factors such as these in the college and university environment.

Higher Education and the Protection of Critical Infrastructure

The information and communication resources of the Internet, now considered a critical part of the national infrastructure, are indispensable to research and education. The educational mission of most campuses now requires direct access to computing and the Internet for every student. Issues of student turnover, evolving technology, technical diversity, decentralized management, funding, and the sheer size of the populations involved present special challenges for cybersecurity in the “wired” as well as the “wireless” campus.

Higher education and officials in the White House and the new Department of Homeland Security are understandably nervous about the vulnerabilities in computer systems and networks on which many of our critical infrastructures depend. There is also recognition of the interdependence among government, industry, and higher education in the reliability and performance of computer networks (Computer Science and Telecommunications Board, 2003). Therefore, a national effort was initiated following the attacks on America on September 11, 2001, to examine cybersecurity along with the physical, chemical, and biological threats to our homeland.

The resulting *National Strategy to Secure Cyberspace* was signed by President George W. Bush in February 2003. According to the *National Strategy*, “The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact” (*National Strategy*, 2003, p. vii). A cover letter from the president to the American people summarized the issue and corresponding national policy as follows: “In the past few years, threats in cyberspace have risen dramatically. The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act

to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible" (*National Strategy*, 2003).

The EDUCAUSE/Internet2 Computer and Network Security Task Force, representing higher education, participated in the development of the *National Strategy* directly with staff from the White House and other federal agencies. One of the outcomes of this recent engagement between the security task force and key players within the federal government is government recognition that higher education plays an important role in the cybersecurity of America. Through its core mission of teaching and learning, it is the main source of our future leaders, innovators, and technical workforce. Through research, it is the source of much of our new knowledge and subsequent technologies. And finally, colleges and universities operate some of the world's largest collections of computers and high-speed networks.

Any successful national response to the threat of cyber terrorism must include steps to strengthen and protect the security of college and university networks and information resources. Institutions of higher education have a responsibility to ensure that their computing and networking facilities are not used to launch attacks on critical infrastructure beyond the campus.

Higher education represents a great national resource with which to explore solutions and develop strategies for cybersecurity in an open and free society. The values of higher education are, in the end, those of the nation. The computers and networks of higher education represent, in many cases, the emerging systems of the future. Successful security implementations in higher education can serve as guideposts for related developments in the nation at large.

The final version of the *National Strategy* encourages colleges and universities "to secure their cyber systems by establishing some or all of the following as appropriate":

1. One or more information sharing and analysis centers to deal with cyberattacks and vulnerabilities
2. An on-call point-of-contact to Internet service providers and law enforcement officials in the event that the school's IT systems are discovered to be launching cyberattacks
3. Model guidelines empowering chief information officers (CIOs) to address cybersecurity
4. One or more sets of best practices for IT security
5. Model user awareness programs and materials
(*National Strategy*, 2003, pp. 25, 41)

The Commitment to Cybersecurity in Higher Education

Higher education has completed a number of significant, concrete steps to move forward with cybersecurity on a national basis. The locus of discussion and planning has been the EDUCAUSE/Internet2 Computer and Network Security Task Force, organized in the summer of 2000. In early 2002, the task force drafted a five-part *Framework for Action* that pledged the following:

1. Make IT security a higher and more visible priority in higher education.
2. Do a better job with existing security tools, including revision of institutional policies.
3. Design, develop, and deploy improved security for future research and education networks.
4. Raise the level of security collaboration among higher education, industry, and government.
5. Integrate higher education work on security into the broader national effort to strengthen critical infrastructure.

The *Framework for Action* was ratified by the American Council on Education and the remaining members of the Higher Education Information Technology Alliance in April 2002. It was then presented to Richard Clarke, formerly special advisor to the president for cyberspace security, when he addressed Networking 2002, an annual national policy meeting for campus information technology leaders. The *Framework for Action* continues to guide the efforts of the task force, and the first three items are addressed in considerable measure by the authors of this book.

Overview of the Book

The chapters in this book are designed to give readers a broad view of the most important ingredients to a successful information security program. Each of the chapters covers topics on which entire books could have been written. Therefore, the content identified and included in this book is designed to provide higher education leadership and management with the necessary overview and stimuli to improve the state of computer and network security at their own campus. The book's authors, however, are practitioners whose experience and insights will also inform IT security professionals responsible for program implementation.

The first chapter examines the unique mission of higher education and values of the academic community. There is sometimes concern that efforts to improve computer and network security will compromise important academic values. There is the mistaken belief that the introduction of better security practices and new institutional policies will be at the expense of privacy or will result in loss of academic freedom. This chapter introduces general principles established during a workshop sponsored by the National Science Foundation that should guide efforts to improve computer and network security in the academic environment.

Initiating a program to improve the security of college and university computers and networks can be both intimidating and

overwhelming. The second chapter provides a road map for organizing to improve security. The author discusses the challenges of finding resources and establishing leadership for security and the evolving role of the IT security officer.

The third chapter describes one of the first steps for improving IT security in a college or university setting: conducting a security assessment and risk analysis. Security assessments may be conducted by using internal resources or by employing an external organization that specializes in vulnerability testing and other techniques that measure the extent of an institution's exposure to known threats. This information can be combined with corresponding estimates of potential institutional losses to yield a prioritized list of preventive actions. The author describes a successful technique, Security Targeting and Analysis of Risks (STAR), used at the Virginia Polytechnic Institute and State University.

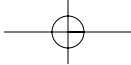
Another important aspect of risk analysis is consideration of legal liability that could result from a security incident. The fourth chapter explores the potential for a college or university to be found negligent in its application of information security. The lack of legal precedent and contemporary experiences with actual IT security incidents mean that there is little direct evidence for making informed choices about the level of risk to tolerate and the payoff that comes from instituting preventive measures. It is inevitable that a combination of incidents of legal liability, based on issues of negligence and business continuity among other things, and new government regulation will make attention to legal issues an important consideration.

Information technology has become an issue of strategic importance for colleges and universities. Chapter Five describes the importance of including cybersecurity in planning and the necessity of developing appropriate institutional policies and procedures. The authors provide an overview of policy development to address the increasing complexity of security issues.

Chapter Six describes how the development of a security architecture and use of an array of technology tools can enhance the security of campus systems. College and university computer systems and networks have evolved in response to innovations and perceived needs of the education and research communities. However, the evolution has resulted in IT infrastructures that are seldom coherent and rarely cost effective, where attention to security has often been an afterthought. An opportunity for a renewed focus on IT security awaits us as colleges and universities attempt to overhaul their network and application architectures, and focus on strategies for life-cycle replacement of hardware and leveraged software licensing.

Finally, experts in computer and network security usually cite people as both the most significant source of IT security problems and the most important element of any program that seeks to improve security. Therefore, no treatment of computer and network security would be complete without a chapter that describes the importance of education and awareness in an overall campus information security program. As discussed in Chapter Seven, short-term efforts must be made to raise the awareness of senior executives, IT professionals, and end users regarding the severity and criticality of IT security issues. Long-term solutions will require persistence and ongoing professional development of system administrators and other IT professionals.

Tactics for improving computer and network security will evolve and change along with the technology over time. Accordingly, the authors and editors recognize the importance of providing readers with general information that is likely to survive the test of time and a sufficient number of specific suggestions to stimulate near-term campus initiatives. Each of the topics can benefit from the sharing of effective practices and solutions on an ongoing basis. For this reason the EDUCAUSE/Internet2 Computer and Network Security Task Force will continue to promote information



xxii Preface

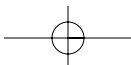
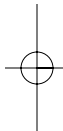
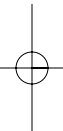
sharing and identification of useful resources through its Web site, periodic publications, and outreach at conferences and other professional development events. For more information, consult www.educause.edu/security.

October 2003

Mark Luker
Rodney Petersen

References

- Computer Science and Telecommunications Board, National Research Council.
Cyber Security Today and Tomorrow: Pay Now or Pay Later. Washington, D.C.: National Academy Press, 2003.
- National Strategy to Secure Cyberspace*. [www.securecyberspace.gov]. Feb. 2003.

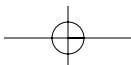
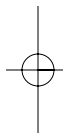
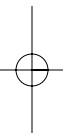
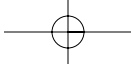


Acknowledgments

A book of this kind is made possible through the expertise, hard work, and dedication of authors, the leadership of the EDUCAUSE/Internet2 Computer and Network Security Task Force, and the EDUCAUSE staff. We would like to thank the authors for their insights and unique perspectives. We are also grateful for their devotion of time and energy—above and beyond other job duties—that will provide higher education executives and IT professionals with critical information that will support campus efforts to improve computer and network security.

We want to acknowledge the wisdom and underlying contributions of the leadership of the Security Task Force and participants of the security workshops funded by the National Science Foundation. The workshop discussions helped formulate many of the ideas contained within Chapter One (“IT Security and Academic Values”). The Security Task Force leadership continues to provide expertise and direction in the overall strategy and agenda for cybersecurity on behalf of higher education.

Finally, we are also indebted to the support and assistance received from Cynthia Golden of EDUCAUSE. Cynthia supported the editors by working directly with some of the authors and carefully proofreading multiple drafts. We are grateful for her dedication and help with this project, in particular, and appreciate her continuing support of the Security Task Force in her role as executive director of professional development.



The Authors

Mark Luker is vice president of EDUCAUSE, where he heads the Washington, D.C.-based policy program as well as Net@EDU. He is a leader in the EDUCAUSE/Internet2 Computer and Network Security Task Force, the Higher Education Bridge Certification Authority, and the National Science Foundation (NSF) program in Advanced Networking with Minority Serving Institutions. Previously, he was program director for advanced networking and the Next Generation Internet project at the NSF. Luker also served as chief information officer at the University of Wisconsin-Madison and as a faculty member and acting dean at the University of Minnesota Duluth. He received his doctorate from the University of California, Berkeley.

Rodney Petersen is the project director for the EDUCAUSE/Internet2 Computer and Network Security Task Force and a policy analyst with EDUCAUSE. He previously served as director of IT Policy and Planning in the Office of the Vice President and CIO at the University of Maryland. He was the founder of Project NEThics at the University of Maryland, which was established to educate the community about responsible use of computing resources and enforce acceptable use policies. Petersen has authored numerous publications and is a frequent speaker on the topics of information security, copyright, privacy, and institutional policy development for the

appropriate use of information technology in higher education. He received his law degree from Wake Forest University.

Mark Bruhn is chief IT security and policy officer at Indiana University. In this role, he advises the administration on technology deployment, usage, and security issues, and directs the efforts of the University IT Policy Office and the University IT Security Office. He is also associate director of the Indiana University Center for Applied Cybersecurity Research (CACR), and recently was appointed acting director of the Research and Educational Networking Information Sharing and Analysis Center (REN-ISAC) based at Indiana University. Bruhn is a member of the EDUCAUSE/Internet2 Computer and Network Security Task Force. He has a bachelor's degree in computer science from Park College and is a Certified Information Systems Security Professional.

Randy Marchany is director of the Virginia Tech Security Testing Lab. He is also the coordinator of VA-CIRT and a member of the White House Working Group for Critical Infrastructure Security. He is the author of numerous computer security documents, including the standard acceptable use policy used in the Virginia State University system, is co-author of the FBI/SANS Institute's "Top 10/20 Internet Security Vulnerabilities" list, and is currently working on a SANS publication on Internet security audit programs. Marchany has taught professional development seminars and has spoken at both national and international conferences on a variety of security topics. He is the recipient of the SANS Institute's Security Technology Leadership Award for 2000.

Diana Oblinger is the executive director of higher education for Microsoft Corporation and adjunct professor at North Carolina State University. Previously, she served as the vice president for information resources and the chief information officer for the sixteen-campus University of North Carolina system. Oblinger has

been a consultant and senior fellow for the EDUCAUSE Center for Applied Research, led the Institute for Academic Technology for IBM, and served on the faculty at Michigan State University and the University of Missouri–Columbia. A frequent keynote speaker, Oblinger has authored and edited numerous books and publications, including the award-winning *What Business Wants from Higher Education*. She is a graduate of Iowa State University.

Shirley Payne is director for security coordination and policy at the University of Virginia. In this capacity she focuses on the continuous enhancement of information technology policies and security of the university's diverse and decentralized computing environment. She works across the university to formulate policies, assess security risk, establish strategic direction, and provide security education and training and related activities. She has thirty-two years of experience in information technology, most of which has been in higher education. She holds a bachelor's degree in computer science from Winthrop University and a master's degree in management information systems from the University of Virginia.

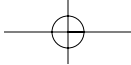
Jeff Recor is president and CEO of the Olympus Security Group, Inc., where he advises clients on the topics of security strategy, return on investment (ROI), and risk mitigation. He has more than eighteen years of experience in the security field, including positions as director of Nortel Networks' Global Professional Services Security Practice and president of the Sargon Group, Inc. An adjunct professor at Walsh College, Recor is the author of three books and numerous articles on this topic. He is currently assisting the White House on infrastructure protection and security research issues. He is a graduate of Michigan State University.

Nancy E. Tribbensee is deputy general counsel at Arizona State University. She advises the university in the areas of intellectual property, technology transfer, research, student affairs, free speech, risk

management, and computer use and security. She is a member of the National Association of College and University Attorneys (NACUA) and serves on the NACUA Publications Committee. She is a founding member of the board of directors for the Association for Interdisciplinary Initiatives in Higher Education Law and Policy. Prior to joining Arizona State University in 1989, Tribbensee was an associate with the law firm Evans, Kitchel, and Jenckes. She received her doctorate in counseling psychology from Arizona State University.

Jack Suess is chief information officer at the University of Maryland, Baltimore County (UMBC). Previously, as a systems programmer, he led projects that developed the Unix and network infrastructures and the campus Web development strategy. He was principal investigator for UMBC's very high-speed Backbone Network Service (vBNS) award and has served on multiple NSF and National Institutes of Health panels related to advanced networking. He is an active participant in the Internet2 Middleware Initiative and a member of the EDUCAUSE/Internet2 Computer and Network Security Task Force. Suess is an adjunct professor at UMBC, as well as a presenter at numerous Internet2 and EDUCAUSE conferences on middleware, security, Web technology, and portals.

Daniel A. Updegrove is vice president for Information Technology at the University of Texas at Austin. He is the co-chair of the EDUCAUSE/Internet2 Computer and Network Security Task Force and serves on the higher education advisory committees for Apple Computer and Dell. Updegrove is a consultant, an author, and a frequent speaker on IT strategic planning, networking, computer-based planning models, and computer gaming simulation. Previously he served as director of Information Technology Services at Yale and associate vice provost for Information Systems and Computing at the University of Pennsylvania. Updegrove studied industrial engineering and urban planning at Cornell University.



Gordon D. Wishon is chief information officer at the University of Notre Dame, where he leads all campus technology efforts. Previously he served as associate vice president and associate vice provost for Information Technology at the Georgia Institute of Technology. Wishon spent twenty years in the U.S. Air Force and ended his military career as CIO of the Air Force Institute of Technology. He is the co-chair of the EDUCAUSE/Internet2 Computer and Network Security Task Force. Wishon holds degrees in computer science from West Virginia University and Wright State University in Ohio.

