Preface

Mark Luker and Rodney Petersen

Computer and Network Security in Higher Education

Mark Luker and Rodney Petersen, Editors

A Publication of EDUCAUSE
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trained personnel, inadequate preventive measures, absence of risk analyses and testing for vulnerabilities, outdated policies and procedures, and insufficient supervision or leadership.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 cyberterrorism 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.
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
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