Foreword

Daniel Updegrove and Gordon Wishon

Computer and Network Security in Higher Education

Mark Luker and Rodney Petersen, Editors

A Publication of EDUCAUSE
College and university executives are increasingly aware of the importance of computer and network security in their institutions. The *Chronicle of Higher Education* and other national and local media regularly report on information security incidents at colleges and universities. A letter was sent in February 2003 to all college and university presidents from the president of the American Council on Education stressing the importance and urgency of cybersecurity in higher education and the need for campus leadership and engagement (www.acenet.edu/washington/letters/2003/03march/cyber.cfm).

Has this awareness been translated into institutionwide policy, well-understood authority, and adequate resources to secure campus information technology resources? Are campus information security officers employing and sharing effective practices and solutions? Is higher education doing its part in securing the Internet, which is increasingly a mission-critical tool to education, business, government, and national security?

The EDUCAUSE/Internet2 Computer and Network Security Task Force was established in the summer of 2000 to address these issues. One impetus for this collaborative effort was the widely publicized distributed denial-of-service (DDOS) attacks that had occurred earlier that year on such key Internet sites as Amazon.com, CNN, eBay, and Yahoo. These attacks were traced to insecure computers at two universities. Another was the realization that Internet2,
higher education’s flagship networking initiative, needed to ensure that high-performance connections and next-generation collaborative applications did not carry with them advanced security risks. Aided immeasurably by a grant from the National Science Foundation, the security task force has developed awareness and best practice seminars, created an information resources Web site, launched an annual conference for campus information security professionals, supported establishment of the Research and Educational Networking Information Sharing and Analysis Center (REN-ISAC) at Indiana University, and orchestrated higher education’s contribution to the recently published National Strategy to Secure Cyberspace (www.securecyberspace.gov).

Two observations from the National Strategy bear repeating here. First, colleges and universities are targeted for exploitation because they possess vast amounts of computing power and because they allow relatively open access to those resources. This open access takes many forms: weak Internet gateway firewalls, lest essential interinstitutional collaboration be impeded; minimal standards for attaching and configuring computers and other devices to networks; a long-standing commitment to remote access and emerging deployment of wireless access; and a culture of innovation and trust. Second, much of the computing power at colleges and universities—servers and workstations in research laboratories, desktops and laptops in wired residence halls—is not managed by IT professionals, if it is managed at all. These are not hypothetical vulnerabilities—high-profile security breaches have occurred in several universities, exposing student, employee, and patient records.

Creation of the REN-ISAC, inclusion of the higher education sector in the National Strategy, and establishment and funding of information security offices in numerous universities and colleges are all positive signs, but much remains to be done. Too many software and hardware products are delivered with insecure configurations or with coding errors that can be exploited to gain unauthorized access. Too many of our academic colleagues believe
that “no one would be interested in my fruit fly database,” not realizing that the computing power of the underlying server, not the data, is often the resource prized by intruders. Too few of our IT organizations have the authorization, expertise, and staff resources to scan their networks for vulnerabilities, even as the frequency and sophistication of hostile network scans increase. In addition, just as we are facing up to the magnitude of these problems, most of our institutions are facing budget difficulties.

Nearly three years after the first large-scale DDOS, an even more potent attack, the so-called “SQL Slammer,” hit the Internet in early 2003. From an unknown origin, this attack proliferated worldwide around the Internet within ten minutes, penetrating tens of thousands of computers with vulnerable software (that is, software to which available patches had not been applied) and causing, by some measures, a 20 percent reduction in Internet accessibility. Colleges and universities responding to a task force survey reported that 75 percent were affected, with some effectively unable to access the Internet for hours—or days—either because their systems had become overloaded or because their Internet service providers had disconnected them to stop the rogue traffic emanating from the penetrated systems.

Every college and university needs a strategy to secure its information resources, a top-level commitment to establish and enforce policies, and an organization that can provide leadership, expertise, and real-time incident response. We must protect our intellectual property and critical records, the privacy of our constituents, and the integrity of our systems, lest they be used against us or our neighbors on the Internet. And we must accomplish this without sacrificing our mission and core values.

The expert contributors to this volume address all of these issues and more. They write from long experience on the forefront of cybersecurity and from heated discussions about the most technically viable, most cost-effective, or most culturally appropriate approaches to securing our college and university networks. They have been,
Foreword

and will continue to be, key contributors to the ongoing work of the security task force. We hope you will join us in this important national effort and will find the resources contained in this book of assistance as you seek to improve computer and network security at your campus.

_Daniel Updegrove_, co-chair of the EDUCAUSE/Internet2 Computer and Network Security Task Force and vice president for Information Technology, The University of Texas at Austin

_Gordon Wishon_, co-chair of the EDUCAUSE/Internet2 Computer and Network Security Task Force and chief information officer and associate vice president/associate provost, University of Notre Dame