

Security: Progress and Challenges

The Homepage column in the March/April 2003 issue of *EDUCAUSE Review* explained the national implications of security vulnerabilities in higher education and the role of the EDUCAUSE/Internet2 Computer and Network Security Task Force in representing the higher education sector in the development of the National Strategy to Secure Cyberspace. Among other things, the National Strategy called for higher education to implement the following: one or more Information Sharing and Analysis Centers to deal with cyber-attacks and vulnerabilities; an on-call point-of-contact on each campus for Internet Service Providers (ISPs) and law enforcement officials in the event that the campus IT systems were discovered to be launching cyber-attacks; model guidelines empowering Chief Information Officers (CIOs) to address cybersecurity; one or more sets of best practices for IT security; and model user-awareness programs and materials.

Since that time, the Task Force has mounted a multipronged attack on the many problems of cybersecurity in higher education, with concrete initiatives in outreach and awareness, training and development for security professionals, tools for risk assessment, legal issues and institutional policies, federal and state public policy, effective practices and solutions, and a more formal engagement with vendors. As part of the national effort, the Task Force is participating in the implementation process of the new National Cyber Security Summit and is coordinating communications regarding all these efforts with the National Cyber Security Division in the Department of Homeland Security.

One result is that security has been

promoted to a featured position in nearly every conference of EDUCAUSE and Internet2 and their partners. Task Force members have contributed a corresponding number of articles to the most relevant publications and Web sites. A letter from David Ward, president of the American Council of Education, to college and university presidents represents a milestone of executive awareness. The second meeting of a new annual conference for security professionals in higher education will be hosted in Washington, D.C., on May 16–18, 2004 (<http://www.educause.edu/conference/security/>). And Internet2 has organized corresponding meetings on the research issues of security for advanced networks.

The Task Force has organized and commissioned a strong collection of leadership resources on security (<http://www.educause.edu/security/resources.asp>). Included, for example, are a white paper on legal issues, a critical analysis of firewall strategies, analyses of the requirements and penalties of the new Gramm-Leach-Bliley Act, guidelines on risk assessment and disaster recovery, links to academic education and training centers on campuses, and a large collection of relevant campus policies. A new book in the EDUCAUSE Leadership Strategies Series, *Computer and Network Security in Higher Education*, provides context for the entire area of cybersecurity in higher education and an executive-level introduction to each of the major issues that must be addressed. More recently, the Task Force has published an online collection of Effective Practices for Security (<http://www.educause.edu/security/ep.asp>) in response to the oft-heard plea, “I now believe that improving security is very important, but how do I do it?”

In the corporate arena, the Task Force has opened a high-level channel of communications to the security architects and others in the vendor community for desktop operating systems, network components, and other technologies that play such a critical role in the security of campus networks and systems. At the institutional level, a Research and Educational Networking Information Sharing and Analysis Center (REN-ISAC) has been established at Indiana University, and many campuses have made improvements in their security policies, systems, and operations over the last year.

Campus leaders who have been on sabbatical for the past year might take these achievements as a sign that we are well on our way to a solution to the cybersecurity threat. During this same time period, however, higher education and all other sectors have suffered from an unprecedented level of attack by worms, viruses, and hackers at the same time that the federal and state governments are increasing the civil and criminal liabilities for institutions that fail to secure their networks and to safeguard personal information protected by law (e.g., health, financial, and educational records). The silver lining of these attacks, if there can be said to be one, is that awareness of the problem has been raised through every level of higher education institutions and, indeed, society. Clearly, there is no simple, “silver bullet” solution. Much work remains to be done in the EDUCAUSE/Internet2 Computer and Network Security Task Force and on college and university campuses.

Mark A. Luker, Vice-President of EDUCAUSE, heads Net@EDU, a “thought-leadership” coalition of college and university CIOs and state network directors.