

Information Security Technology

Common-sense advice on the big-picture security issues college presidents and their administrators should be thinking about now – before they see their institution in the headlines. by Thomas Keith Meier



Some college presidents are well-versed in many of the internal aspects of information technology, while others, like me, merely admire the many benefits it offers. However, recent widespread and well-publicized security threats, as well as the opportunity to contribute this chapter, have raised my own level of awareness of information technology (IT), and I wish to thank two of my tutors in the field who are the principal contributors to this discussion: Scott Lowe, director of Information Technology, and Michael Rogers, director of Communications, both at **Elmira College** (NY).

There was once a day when a college could connect its campus—along with every student—to the Internet, and not have to worry much about security. The primary threat was from students who attempted to hack the college administrative systems in an effort to boost their (perhaps lackluster) grades. Those days are gone.

Of course, a college still needs to worry about the occasional computer-savvy underachiever, but today's threats to campus information security are much more serious and sophisticated. Among the threats to college campuses today are:

Identity theft: a crime in which an imposter gains access to someone's personal information and uses it to impersonate the innocent victim. This crime is of particular concern to college campuses, either due to historically lax policies or the use of unprotected social security numbers as student identification numbers.

Hacking and data theft: a crime in which a person gains unauthorized access to key systems, and steals sensitive data. This is sometimes followed up by actual identity theft.

Viruses and spyware: Viruses have been around for a long time, but spyware—generally, tracking software that watches what users do and reports activity to a home base—is a relatively new phenomenon that can have serious security consequences if left unchecked.

Because of these issues and the explosion of all things Internet, IT security has quickly moved from a back-burner, “would-be-nice-if” task to a critical and ongoing investment for any campus that relies on technology for its services. Information security often is compared to a war in which the allies need to stay one step ahead of the enemy. Presidents and other senior leaders must take steps to ensure that the college is always one step ahead. What are some ways to achieve this evermore elusive goal?

IT Security Goal: One Step Ahead

Probably the most important security goal is identifying the campus risk areas. Most college administrators have read about the unfortunate situation at **George Mason University** (VA) in early 2005. In short, attackers gained access to sensitive campus systems and may have snatched as many as 30,000 personal student and employee records, including social security numbers. This is not the kind of publicity that any institution seeks. In this case, one major risk area for George Mason was its administrative system's use of the social security number as a student identifier. Ironically, the university was in the process of converting to an unrelated student identifier at the time of the security breach.

Key areas that need to go through a risk analysis include administrative servers, e-mail systems, institutional desktops, and the student residential network, for a start. The simple truth: Every area on campus that has stored electronic information needs to be secure. Even the office computer in the Department of Buildings and Grounds could be a risk. How? Consider this: Suppose a student submits a request to Buildings and Grounds and that department uses the student ID number to track the request. Further suppose that the institution still is using social security numbers as a student identifier—the conclusion is obvious.

Second, institutions need to make sure they have the appropriate policies in place and that those policies are enforced. For example, does the campus have an acceptable use policy as well as an enforced password policy? If not, those policies should be in place, and IT must have the means and the authority to enforce them. For help creating or revising such policies, Educause and the Cornell Institute for Computer Policy and Law have compiled hundreds of information policies from dozens of campuses and made them available on the [Educause Web site](#).

Target Student and Employee Threats

A study conducted by the US Secret Service and the [Carnegie Mellon Software Engineering Institute](#) found that 78 percent of computer crimes carried out at financial institutions were accomplished by authorized users—that is, users who had the right to access the affected systems. While not operating a financial institution, colleges and universities do house information that is compelling for data thieves, including social security and credit card numbers.

An information security policy should limit access to key systems to only those who require access in order to perform their jobs. Too often, campuses provide access to almost every system to every employee—without determining who has a “need to know.” Unfortunately, every person with access to a key system becomes a potential threat to the institution’s information security.

Some universities provide inappropriately wide access in the mistaken belief that to limit access is to communicate that the institution distrusts its own employees. With today’s high stakes in IT, common sense dictates restricting access. After all, colleges do not make explosive laboratory chemicals or the institution’s checking accounts available to everyone on campus.

Another part of an information security policy should detail exactly what kind of data is stored and why. For example, colleges may need to store social security numbers for financial aid reporting, but are they storing other information that leaves the institution at even greater risk? Maybe it doesn’t have to be that way. For instance, instead of storing student credit card numbers for tuition payment, one might consider outsourcing this activity to a competent third party with a security infrastructure designed to handle this kind of activity, thus avoiding the liability of storing credit card numbers.

A further feature of a solid security practice lies in the technology the college uses. To implement effective security policies, the technical environment must, of course, be conducive to security. Not very long ago, this meant placing a firewall (a device that blocks unwanted and uninvited visitors from the Internet) between the campus network and the Internet. With this firewall in place, the theory went, unauthorized visitors could not gain access to critical information systems and cause damage. Today, while a firewall is still critical, it is but one cog in the security wheel. There are additional hardware and software components that are required to protect systems.

The first technical solution relates back to the point made earlier about the judicious control of access to key systems. One should make sure this is enforced through a technical solution as well. For example, on some campuses, student computers can “see” key administrative servers, but the students do not have accounts to access these systems, so they may be deemed “safe” when in fact they are not. For every key system on campus, ask the question, “Who needs to access this service?” and make sure that IT takes the technical steps necessary to lock others out. In the example above, no student computer should even be able to see an administrative system.

The seemingly mundane task of keeping virus scanners current also is important to preventing problems. Some viruses take advantage of vulnerabilities on the computer to allow access by a third party. By keeping the virus away, one also keeps the third party away, so institutions should insist on a current virus scanner across the board—on all institutional machines, as well as on all student computers, without exception.

Education and Oversight

The final areas on which to concentrate security efforts lie in education and oversight. Educate users about the risks of lax practices, such as writing passwords on sticky notes and posting them on their monitors, and about sharing passwords with others. A password shared with the wrong person can lead to data theft that could make the institution a case study in systems security mismanagement. Make sure the IT staff has the skills necessary to keep the university's information safe. One might even consider having an IT staffer whose responsibility it is to question, learn, and advise the campus community about potential security threats. After all, the college is most assuredly not the last place in which students will need to be armed with knowledge they can use to protect themselves from fraud. On the oversight front, consider contracting with a third-party company that performs information security audits. The results of such an audit can help quickly identify weak areas in information security infrastructure and may avoid serious problems.

IT has become a strategic component for many campuses. Along with the benefits of IT inevitably come the dangers, including the security threats outlined here. Using some of the information discussed herein, college leaders could certainly reduce the risk of succumbing to security threats—and keep their institutions out of the headlines.

*Thomas Keith Meier has served as the 12th president of **Elmira College** since 1987. Previously, he was the 17th president of **Castleton State College** (VT) for eight years. SunGard SCT (www.sungardsct.com) is publisher of *President to President: Views of Technology in Higher Education* (2005), from which this article is excerpted, and is corporate sponsor of the New Presidents program. Marylouise Fennell, co-editor of *President to President*, is coordinator of the New Presidents program, and senior counsel to the Council of Independent Colleges (www.cic.edu). Scott D. Miller, also co-editor, is president of Wesley College (DE), and chair of the program.*

This article originally appeared in the November 2005 Issue of Campus Technology