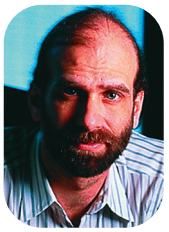
University Networks and Data Security

In general, the problems of securing a university network are no different than those of securing any other large corporate network. But when it comes to data security, universities have their own unique problems. It's easy to point fingers at students—a large number of potentially adversarial transient insiders. Yet that's really no different from a corporation dealing with an assortment of employees and contractors—the difference is the culture.



Bruce Schneier
Counterpane Internet Security

Universities are edge-focused; central policies tend to be weak, by design, with maximum autonomy for the edges. This means they have natural tendencies against centralization of services. Departments and individual professors are used to being semiautonomous. Because these institutions were established long before the advent of computers, when networking did begin to infuse universities, it developed within existing administrative divisions. Some universities have academic departments with separate IT departments, budgets, and staff, with a central IT group providing bandwidth but little or no oversight. Unfortunately, these smaller IT groups don't generally count policy development and enforcement as part of their core competencies.

The lack of central authority makes enforcing uniform standards challenging, to say the least. Most university CIOs have much less power than their corporate counterparts; university mandates can be a major obstacle in enforcing any security policy. This leads to an uneven security landscape.

There's also a cultural tendency for faculty and staff to resist restrictions, especially in the area of research. Because most research is now done online—or, at least, involves online access—restricting the use of or deciding on appropriate uses for information technologies can be difficult. This resistance also leads to a lack of centralization and an absence of IT operational procedures such as change control, change management, patch management, and configuration control.

The result is that there's rarely a uniform security policy. The centralized servers—the core where the database servers live—are generally more secure, whereas the periphery is a hodgepodge of security levels.

So, what to do? Unfortunately, solutions are easier to describe than implement.

First, universities should take a top-down approach to securing their infrastructure. Rather than fighting an established culture, they should concentrate on the core infrastructure.

Then they should move personal, financial, and other comparable data into that core. Leave information important to departments and research groups to them, and centrally store information that's important to the university as a whole. This can be done under the auspices of the CIO. Laws and regulations can help drive consolidation and standardization.

Next, enforce policies for departments that need to connect to the sensitive data in the core. This can be difficult with older legacy systems, but establishing a standard for best practices is better than giving up. All legacy technology is upgraded eventually.

Finally, create distinct segregated networks within the campus. Treat networks that aren't under the IT department's direct control as untrusted. Student networks, for example, should be firewalled to protect the internal core from them. The university can then establish levels of trust commensurate with the segregated networks' adherence to policies. If a research network claims it can't have any controls, then let the university create a separate virtual network for it, outside the university's firewalls, and let it live there. Note, though, that if something or someone on that network wants to connect to sensitive data within the core, it's going to have to agree to whatever security policies that level of data access requires.

Securing university networks is an excellent example of the social problems surrounding network security being harder than the technical ones. But harder doesn't mean impossible, and there is a lot that can be done to improve security. □

Bruce Schneier *is one of the world's foremost security experts and chief technical officer of Counterpane Internet Security. His most recent book is* Beyond Fear: Thinking Sensibly about Security in an Uncertain World. *You can subscribe to his email newsletter,* Crypto-Gram, *at www.schneier.com.*