



## University Networks and Data Breaches

*Bruce Schneier, Chief Technology Officer  
Adam Rice, Director, Professional Services*

Ohio University fired their director of communication network services and their manager of Internet and systems for the school, in the wake of a June data breach that exposed the personal information of 137,000 alumni.

Theft of personal information from computer networks has been a serious problem for years, due to the increasing tendency of criminals to target centralized networks to steal personal identifying information for identity theft. The public has only become aware of the problem since 2003, when California mandated public disclosure of these sorts of thefts. Since then, 22 states have followed suit.

Targets are varied: retailers, large corporations, financial institutions, and so on. Colleges and universities have also been a target, a surprisingly big one. In addition to the [Ohio University](#) incident, in the last three months we've seen data breaches at [Purdue University](#), [Georgetown University](#), [Sacred Heart University](#), [Western Illinois University](#), [University of Tennessee](#), and the [University of Texas](#). And these are just the data breaches we've heard about; not every institution is required by law to make these sorts of crimes public.

In general, the problems of securing a college or university network are no different than the problems of securing any other large corporate network. But universities have their own unique problems when it comes to data security. It's easy to point fingers at the student body: a large number of potentially adversarial transient insiders. But that's really no different than a corporation dealing with the usual assortment of employees and contractors. The difference between a university and a large corporation is the culture.

Universities are very edge-focused; central policies tend to be weak, by design, with maximum autonomy for the edges. This means that they have natural tendencies against centralization of services. Departments, research groups, and individual professors are all used to being semi-autonomous. These institutions have been in place since long before computers. When networking began to infuse universities, they grew up within the administrative divisions that were already in place. Some universities have academic departments with totally 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 have policy development and enforcement as one of their core competencies.

The lack of central authority makes the enforcement of 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—and generally operate with limited authority. This leads to an uneven security landscape.

There is also a cultural tendency for faculty and staff to resist restrictions,

*"Security and compliance requires specialized expertise, and it makes more sense to outsource that so my staff can stay focused on the core business objectives... Counterpane can survey all the potential threats worldwide. They can provide a much wider, more current view of the threats. That's something we can't do as efficiently, given our current staff levels."*

**John Lambeth, CSSP, CISA**  
VP Information Technology  
Blackboard Inc.

*"Because Counterpane gives us only the information we need when we need it, we can concentrate on the attacks that matter. The value of that kind of service is enormous."*

**David MacLeod, Ph.D. CISSP**  
CISO  
The Regence Group

*"By outsourcing monitoring and management of established security systems to managed security service providers, most enterprises can increase security while reducing operational costs, and free up internal security resources to deal with changing business needs and new threat."*

**John Pescatore**  
VP Distinguished Analyst  
Gartner, Inc

## **Contact Us**

(888) 710-8175  
sales@counterpane.com

www.counterpane.com

1090A La Avenida  
Mountain View  
CA 94043  
U.S.A.



especially in the area of research. Since today most research is done online—or, at least, involves online access—restricting use or deciding on appropriate uses for information technologies can be difficult. This resistance also leads to a lack of centralization and an absence of such IT operational procedures as change control, change management, patch management, and configuration control.

The result is that there is rarely a uniform security policy. The centralized servers—the core where the database servers live—are generally more secure, while the periphery is a hodge-podge of better and worse security.

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

First, universities should take a top-down approach to securing their infrastructure. Rather than fighting a culture that can be hundreds of years old, they should concentrate on the core infrastructure.

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

Next, enforce policies for those 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 and saying it cannot happen. All legacy technology gets upgraded eventually, and it probably doesn't even make sense to upgrade anything that will be replaced within a few years.

Finally, create very distinct segregated networks within the campus. Treat those networks that are not under the direct control of the IT department as untrusted networks. Student networks, for example, should be treated like the Internet and 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 cannot 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.

Of course, the core should be similarly zoned.

One last piece of advice: universities should look to the outside for guidance and help. Universities tend to be a bit incestuous about knowledge. They sometimes believe that because they are academic institutions they don't need guidance. That's simply not true.

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 – or at least the personal identifying information of students and faculty.