

Payment Card Information Security for Higher Education

Executive Summary

While headlines may indicate that the majority of security breach victims are counted among the Fortune 500, in our work we've found that universities and colleges are at least as, if not more, vulnerable to attack. The several instances of compromises we've seen at higher education institutions over the past few years support this claim. These cases range from individuals breaching a university's administration system and accessing student records, to the theft of credit card information from a campus book store's point-of-sale (POS) system illustrated below:

- ❖ **The Environment** - *A university book store used a high-speed Internet connection to process credit card transactions. High speed Internet access at this campus – like many other campuses - was ubiquitous and available to all users from various locations including students in their dorm rooms and professors in the English Department. In essence, the Internet connected the entire campus network with itself and the outside world. For institutions of higher education, this set-up is commonly used to facilitate the open sharing of information in an environment of higher learning.*
- ❖ **The Incident** – *An investigation identified the book store as the location of a data security breach through which an unauthorized individual accessed thousands of students' (and their parents') credit card information. The individual then used the information to execute fraudulent transactions and all affected cards had to be cancelled and re-issued.*
- ❖ **The Cause** – *The investigation revealed that a number of security flaws within the book store's environment lead to the breach. First, the POS system ran on an outdated version of Microsoft Windows and was connected to the Internet. Second, no effective perimeter defense, such as a firewall, monitored traffic on the network. This combination of old software and a lack of security hardware controls created a dangerous situation that ultimately resulted in data compromise.*

The scenario outlined above may sound familiar because, unfortunately, it's becoming a more and more common occurrence at colleges and universities across the country. Many institutions of higher education have yet to sufficiently address the balance between an open-access environment and the latest protections against an ever-growing fraud business poised to exploit it.

Colleges and universities that fall victim to a data compromise will attest to the complications and anxiety that result. Before a breach, they operate assuming their system is secure. But as detailed above, these compromises typically take place on systems outside the direct periphery of the core IT structure and not usually monitored for suspicious activity. Along with the stolen or corrupted data itself, the aftermath of a breach includes unwanted network disruption and downtime, burdensome and often significant financial costs, major resource constraints, and, perhaps most damaging, the degradation of an institution's brand fueled by media coverage.

When credit card information is involved, the attention to a security breach increases exponentially. But no matter how innocuous a data compromise may seem, every time an attacker foils an institution's security measures and the public is informed, addressing the balance between open-access and security becomes even more urgent.

Preventing data security attacks is not a simple issue to address for any organization, higher education or otherwise. Organizations with a stake in the flow of electronic commerce respond to this threat in a variety of ways. For example, major credit card brands like American Express, Discover, MasterCard, and Visa joined together in 2004 to create a common set of data security requirements—the Payment Card Industry (PCI) Data Security Standard. Visa and MasterCard require *all* merchants and service providers that store, transmit or process credit card holder information comply with the PCI standard. To ease enforcement, the

card associations make merchant banks and acquirers responsible for ensuring that their merchants and service providers meet the PCI standard. Service providers and merchants that process credit card transactions must validate their system's PCI compliance through assessments performed on a recurring basis by an approved independent third-party assessor.

Target-Rich Environment

In the data security field, protecting a higher education institution's data presents a unique situation. As with all merchants and service providers, a university can find itself under attack from the Internet. However, while a merchant or service provider can restrict internal access to a select few, an education institution has a vested interest in nurturing the free transfer of ideas over their network by giving access to as many users as possible. While thus far higher education institutions have mostly avoided detrimental press coverage, with the difficulties inherent in securing an open-access network the breach that breaks the fold is probably not far away.

A number of characteristics common to many higher education institutions make them a prime target for data compromise more so than the average corporation. Specifically:

- Attackers view higher education networks as target-rich because these institutions typically function in a decentralized manner with regard to their IT infrastructure, operations, budgets, compliance management, and decision-making.
- Higher education networks contain vast amounts of data an attacker may find valuable such as social security numbers, credit card and other personal financial information.
- The threat of an internal attack from a pool of technologically-savvy individuals (primarily students) makes protecting the network an expensive and time-consuming project that attackers know many institutions aren't willing to undertake.
- Higher education's desire to cultivate the free exchange of ideas and provide open access to online resources makes sufficient protection difficult.

The following are a few key issues mentioned by our higher education clients when we discuss vulnerabilities in their network environments:

"We may have credit card transactions on our network that we don't even know about" – We find this is a pervasive concern with most of our higher education clients. In many cases, they often don't know the number and types of merchants conducting commerce on their campus or the various access methods used to call and connect to their processors. This type of information has not been centrally managed and maintained.

"We don't know where all the critical data is on our network" If you don't know where your critical data is stored, processed and transmitted, you can't protect it. Many organizations need to explore their networks to determine where their critical information assets exist. Given the nature of higher education, most institutions are storing not only large volumes of credit card data, but also other sensitive financial and personal profile information such as social security numbers.

"We run open networks" - The philosophical core of most higher education institutions includes the belief that the technology environment must be designed and maintained to encourage the open exchange and availability of ideas, information and files. Therefore most environments were established, grown, and maintained in a culture that, however unintentionally, makes information security a low priority. Unfortunately, this philosophy tends to create a natural resistance to appropriate security measures and most information security personnel today find themselves trying to protect critical information in an environment where data security was previously only an afterthought. Albeit slowly, this philosophy is changing primarily due to liability issues involved when higher education systems or networks are hijacked and used to perform attacks against a third party. Court rulings have upheld the notion that the owner of a system must take reasonable and customary precautions in protecting their systems from exploitation by a third party attacker.

“We allow and invite personally-owned computers on our network” – College and university computing and network environments are generally highly populated with servers and student-owned computers that have high bandwidth Internet connectivity. These characteristics bring with them a host of challenges from a security management perspective. Because most higher education institutions don’t control whether a student’s PC has anti-virus software installed and running or what software a student has downloaded that may contain bugs or malicious code (enabling hijackers to use the system to spawn attacks), allowing student-owned PCs to connect to internal network segments greatly increases the risk that a network could be devastated by a virus or worm.

“We operate a decentralized environment” – It’s quite common to find higher education entities geographically dispersed and decentralized, especially with physical controls, policies and procedures. Most specifically, credit card data controls are rarely in place, and this sensitive data may reside in any number of locations or on numerous systems. Managing sensitive data in this situation becomes burdensome as it is difficult to secure all areas of the network where it exists.

“We manage on very thin budgets which can barely support what we have” – This is a very common obstacle mentioned by our clients. Most higher education institutions have not made or committed to the financial investment in security initiatives, personnel and technology necessary to supporting these types of environments.

“We typically don’t use formal software development disciplines” – This response is particularly relevant when it’s shown that many of the compromises investigated today result from software that is implemented incorrectly or inherently weak with respect to security. Software developers must be trained in secure coding techniques and integrators must be graded based on performance criteria that emphasize security in addition to standard performance metrics. (For example, did the integrator change the default passwords?).

“We don’t know how to defend our infrastructure” – The scope of this issue transcends just one or two departments. It’s a technical and business issue that requires interdepartmental participation and the full support of executive management to address. It’s a real problem that requires a real solution and a commitment from the entire organization.

Suggested Best Practices

Despite the security challenges faced by institutions of higher learning, there are simple, cost-effective solutions when it comes to the protection of sensitive data. While all of the recommendations below may seem obvious, they are lacking at many colleges and universities.

- **Vulnerability Management & Intrusion Detection** – In most environments, systems and applications are used in every area of a campus network. These networks are often connected to the Internet with hundreds of access points across the campus. While monitoring every system user is very difficult (if not impossible), detecting just unauthorized access and improper activity is manageable. Most universities do not have intrusion detection systems in place to tell them if an attacker is attempting to gain access to their environment. To implement such a system cost-effectively, an institution must identify critical systems within the campus (such as those that contain student records or financial information) and build a system of sensors to alert security personnel when something out of the ordinary occurs. For example, if a sensor detects an FTP connection made between a database system within a financial aid office and a system outside of the campus network, security personnel need to be notified in order to prevent a possible breach. In addition, run a vulnerability scan on your IT environment to identify security gaps. This will help you decide where to focus your security resources.
- **Asset Inventory** - Identify your critical information assets including all hardware and software. This will help you identify the devices and applications that are the most important when it comes to securing information. There are several technologies on the market that can identify the assets on your network.

- **Policy & Procedures** - Develop written security policies and procedures for protecting all data. A primary obstacle to achieving compliance within a higher education institution is that institution's security policies and procedures. Many times certain university staff practice appropriate security measures, but often these policies and procedures are not documented sufficiently (if at all). If a security-minded network administrator or engineer leaves an institution, their standards and practices leave with them. This leaves unknown holes in the university's network environment and can negatively impact the overall security structure. Documenting a university's security policies and procedures, will help ensure that when an employee leaves or adopts a new role, their replacement can easily learn and incorporate standardized policies and procedures into their daily routine.
 - **Communicate** - Conduct security awareness education and training for all departments. It's common for an individual to develop a work routine to complete their daily assignments and forget to consider the impact their actions have on the organization's overall security posture. Sending regular security alerts to and educating all staff members on various security topics will increase security awareness among all individuals and departments. These efforts will provide the information staff members need to keep in mind when making decisions that may change the network environment. Even the smallest tactical change can have a negative impact if not implemented correctly.
 - **PCI Compliance** - Validate compliance with IT security requirements including the PCI Data Security Standard mandated by all the credit card associations. Ask your acquiring bank about your compliance requirements and what resources they may have available to assist you in your compliance efforts. For example, they may have a relationship with a Qualified Data Security Company (QDSC) – a firm sanctioned by the credit card associations to provide PCI compliance validation services.
-

Conclusion

Experts predict that the number of attacks on various institutions' network systems, and the resulting security breaches, will continue to increase.

Higher education institutions need to ensure that their systems are protected and need to do so immediately. Anyone that utilizes the electronic payment network is vulnerable to attack, and it is incumbent on the leaders of higher education institutions to raise their standards when it comes guarding their students' financial and personal information and ensuring compliance with the latest regulatory mandates. In fact, with over a dozen pieces of legislation regulating the protection of sensitive personal information pending in Congress, the issue will only require more resources for oversight and personnel. Fortunately there are a number of ways to proactively address these issues and get on with real business.

AmbironTrustWave is available to assist you in these efforts to reduce your exposure to security incidents and loss of sensitive information, enhance your organization's security posture, manage your institution's complex credit card processing environment, improve substandard merchant network security, and demonstrate compliance against industry and regulatory standards.

About AmbironTrustWave

AmbironTrustWave is a leading provider of information security and compliance management solutions to businesses in the Fortune 2000 and the public sector. The company's flagship products, TrustKeeper® and TrustMinder™, serve more than 25,000 businesses throughout the world to validate compliance with a variety of industry standards and regulations. For the payment card industry, AmbironTrustWave helps banks, merchants, service providers and software developers mitigate their risk by validating compliance with industry best practices for safeguarding information endorsed by American Express, Discover, MasterCard, Visa Canada and Visa USA. AmbironTrustWave clients include financial organizations, global electronic exchanges, educational institutions and business services firms. The Company also provides services to several government agencies. AmbironTrustWave is headquartered in Chicago with offices throughout the United States.