

Straight Talk About DATA SECURITY

By Walter Conway and Dennis W. Reedy

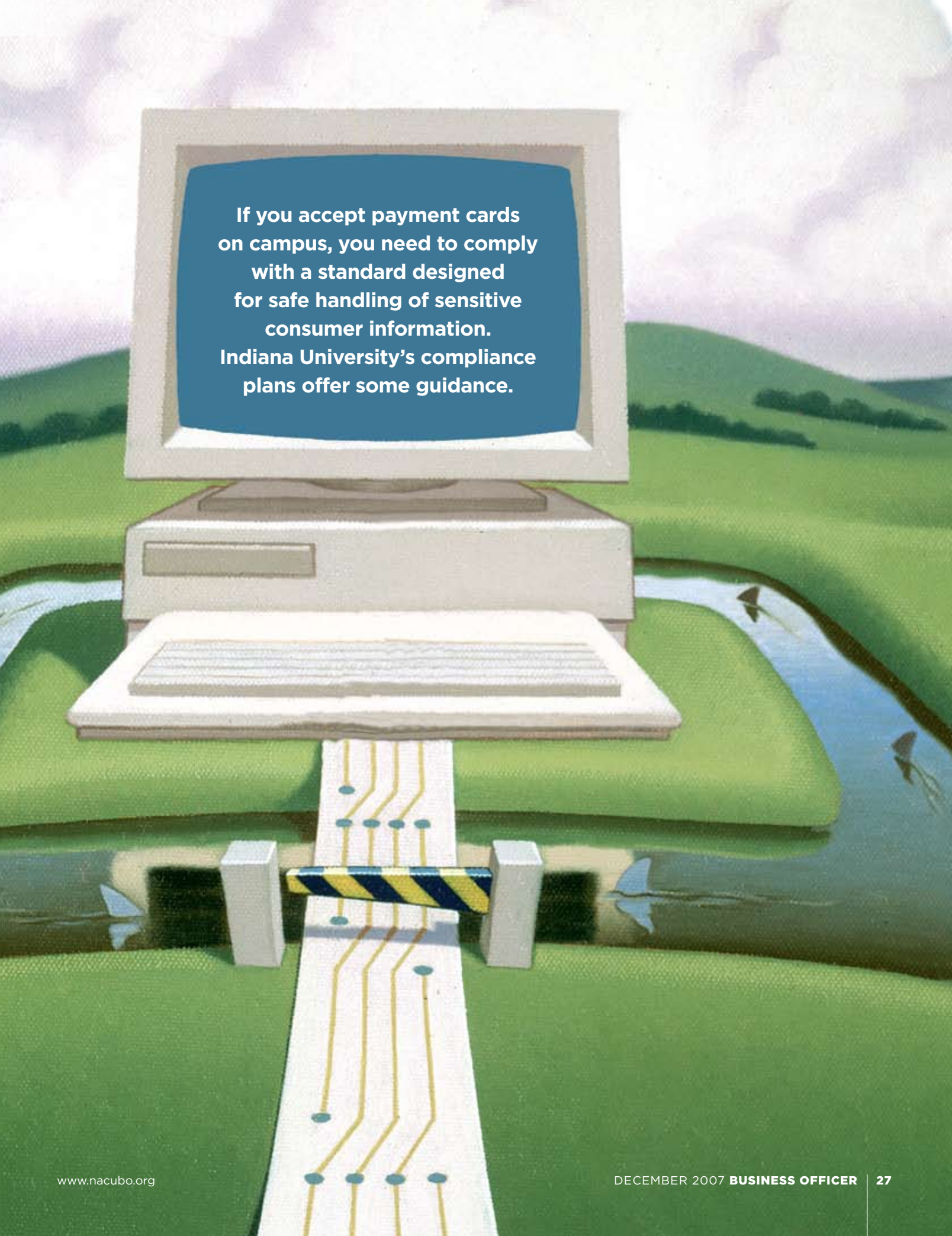
Plan for the worst. Every institution, regardless of size, is vulnerable to a security breach that can lead to the compromise of sensitive information. The incident may be accidental, caused by a stolen laptop, lost storage device, or mishandled paper record. Or, it may be malicious—the result of phishing, malware, or database hacking by outsiders.

Unfortunately, our research indicates that educational institutions are particular targets of intentional attacks (see Figure 1). Drawing on our database of more than 650 publicly reported security breaches from early 2000 to July 2007, we found that the largest source of data compromise for educational institutions was hacking or related intentional attacks. These purposeful actions accounted for 41 percent of all breaches. In comparison, the biggest data security problems for businesses originated with lost or stolen laptops and storage devices, which accounted for nearly half the total incidents. Hacking represented only 18 percent of breaches for these businesses—less than half the figure recorded for colleges and universities.

The cause of such problems, however, is less important than the reality that your institution is vulnerable. The only *uncertainty* is how much the inevitable breach will cost when it happens. Direct financial costs can mount when you must notify individuals that their data have been compromised, pay for credit monitoring, and repair faulty systems and procedures. For breaches related to payment card information, potentially significant liability—and even fines—may be involved. It's not unusual for these overall direct costs to total \$1 million for even a relatively small breach.

The financial price tag pales when compared to the much larger cost: the damage to your college's reputation when people think that the institution has violated the trust of students, parents, and alumni.

Fortunately, a new data security standard shows promise in protecting payment cardholder information—a large area



**If you accept payment cards
on campus, you need to comply
with a standard designed
for safe handling of sensitive
consumer information.
Indiana University's compliance
plans offer some guidance.**

of data vulnerability, given that higher education represents roughly a \$40-billion market for card issuers. Following are an explanation of the standard and a description of compliance plans that Indiana University, Bloomington, is in the process of implementing.

A Standard Comes to the Rescue

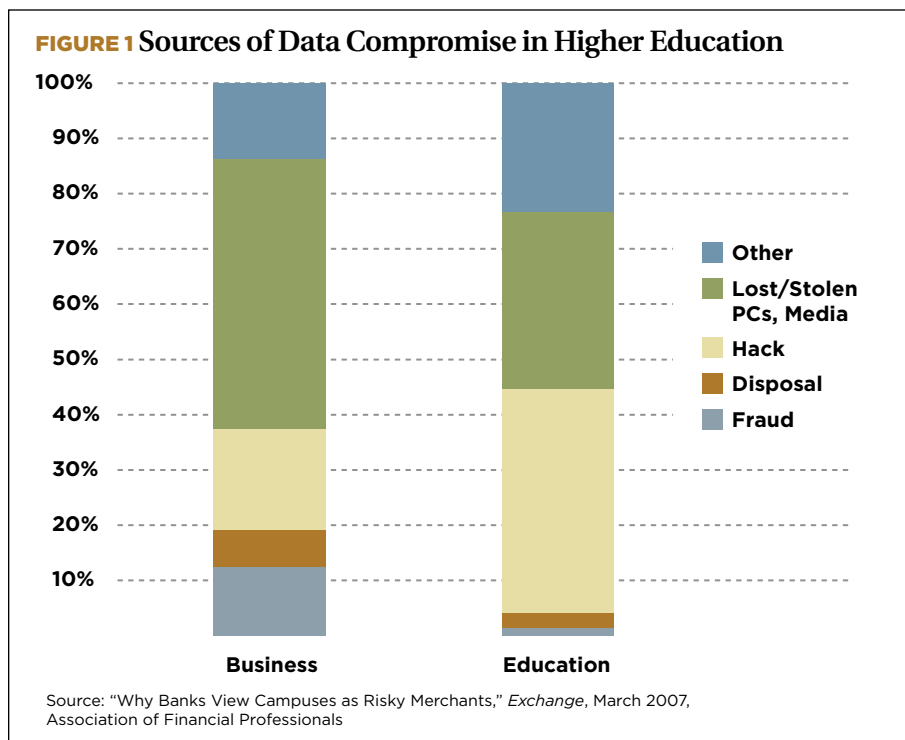
The Payment Card Industry (PCI) Data Security Standard (DSS) is rooted in 2001 data security efforts: Visa's Cardholder Information Security Program and MasterCard's Site Data Protection plan. In 2004, the two standards were combined into a single standard, with American Express, Discover Card Services, and the Japan Credit Bureau joining in support. In 2006, the five payment brands formed the Payment Card Industry Security Standards Council (PCI SSC), an independent body to promote adoption and global management of the standards.

The primary objective of PCI DSS is to protect cardholder data. Compliance with the standard is required of all merchants that process, store, or transmit cardholder data. This definition includes almost all campuses. The volume of payment card activity combined with institutions' vulnerability to attacks will undoubtedly attract the attention of people who see value in institutions becoming PCI compliant as soon as possible. Payment card associations and issuers have reinvented efforts to achieve such compliance of *all* organizations by the end of 2007, with an emphasis on merchants handling large volumes of transactions.

While it's true that PCI DSS compliance is required, we think that it is also good business practice for all colleges and universities taking payment cards.

Expectations and Recommendations

The PCI DSS contains 12 requirements that can be divided into six logical groupings, as shown in Figure 2. Each requirement includes additional details that can make the standards appear daunting and technical in nature. The



objectives, however, are really business processes, not merely technology issues. Since PCI DSS is a fact of life, you'll need to devote resources to achieving and maintaining compliance. This calls for a team approach that includes financial, audit, legal, and information security experts from throughout the institution. While the lead most often—and appropriately—rests with the business side, it takes a multidisciplinary, institutionwide team to create an effective data security process.

Our experience tells us that it works best to resist the inclination to tackle standards compliance in a linear fashion, starting with number one and proceeding through the list. Rather, the most important part is to start with controlling cardholder data (requirements 3 and 4) by finding where it is stored and, subsequently, managing that data. The compliance team then can proceed to strengthen systems (requirements 5 and 6) and ensure that activity logging and audit systems are in place (requirement 10). Whatever the approach, the objective is to assist all campus operations involving credit card processing to fulfill the

requirements of the standard.

Indiana University Commits to Compliance

As this article went to press, Indiana University, Bloomington, was in the process of validating its compliance. Following is a description of the approach IU has used for each of the PCI DSS requirements. Meeting the standard involves applying technology, policies, procedures, and business practices.

I. Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Indiana University has a separate server for credit card transaction processing. This server is segregated from our other servers and is protected by a firewall.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

All systems that interface with credit cards are being reviewed to ensure that vendor-supplied default accounts are deleted or changed.

II. Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

It is against Indiana University policy to electronically store cardholder data. Cardholder data in paper format is required to be kept in a secure location for a maximum of two years.

Requirement 4: Encrypt transmissions of cardholder data across open, public networks.

We currently use the PayPal PayFlow Pro SDK and require transactions that are processed via the Internet to use secure sockets layer (SSL) protocol. We also outsource some processing to a PCI DSS-approved vendor.

III. Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update antivirus software.

We are requiring merchant locations to provide screen shots of the antivirus protection from each machine involved in credit card processing. We are looking into providing a central antivirus server that merchants will be required to use.

Requirement 6: Develop and maintain secure systems and applications.

We require that all systems put in place or developed at Indiana University undergo extensive testing prior to deployment.

IV. Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by the business's need-to-know.

The systems in place at Indiana University do not allow users to view the entire credit card number.

Requirement 8: Assign a unique ID to each person with computer access.

Each Indiana University staff member is assigned a unique ID upon hiring. The ID grants access only to the systems that the individual needs to do his or her job.

Requirement 9: Restrict physical access

FIGURE 2 The Payment Card Industry (PCI) Data Security Standard (DSS)

I. Build and Maintain a Secure Network

REQUIREMENT 1: Install and maintain a firewall configuration to protect cardholder data.

REQUIREMENT 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

II. Protect Cardholder Data

REQUIREMENT 3: Protect stored cardholder data.

REQUIREMENT 4: Encrypt transmission of cardholder data across open, public networks.

III. Maintain a Vulnerability Management Program

REQUIREMENT 5: Use and regularly update antivirus software.

REQUIREMENT 6: Develop and maintain secure systems and applications.

IV. Implement Strong Access Control Measures

REQUIREMENT 7: Restrict access to cardholder data by business need-to-know.

REQUIREMENT 8: Assign a unique ID to each person with computer access.

REQUIREMENT 9: Restrict physical access to cardholder data.

V. Regularly Monitor and Test Networks

REQUIREMENT 10: Track and monitor all access to network resources and cardholder data.

REQUIREMENT 11: Regularly test security systems and processes.

VI. Maintain an Information Security Policy

REQUIREMENT 12: Maintain a policy that addresses information security.

Source: Payment Card Industry Security Standards Council

to cardholder data.

Access to paper documents is restricted at the merchant location to those who "need to know" to conduct business.

V. Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

We track access to network resources by unique user ID. No access to cardholder data is provided.

Requirement 11: Regularly test security systems and processes.

We run internal scans on a regular basis for those systems that interface with credit card data.

VI. Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security.

Indiana University has an information technology department that is responsible for maintaining policies that relate to security and information technology.

Beyond the Standard

Achieving compliance with the standards can go along way in protecting payment card information. However, it still doesn't guarantee that you'll never experience a data breach. In fact, educational institutions represent a disproportionate share of security breaches: Drawing on our database of publicly reported security breaches, we found that fully one third of all breaches took place at educational institutions (see Figure 3). The disproportionate numbers take on another dimension when you consider

that higher education institutions number about 4,000, compared with roughly 14 million businesses involved in credit card transactions.

If a data breach is virtually inevitable, the logical approach is to make sure that, when the worst happens, no sensitive data are compromised. The objective becomes how best to achieve safe harbor to protect the institution. In this context, “safe harbor” means that the institution reduces or eliminates its notification requirement and financial liabilities under state law. It also means no fine is likely from the card issuers.

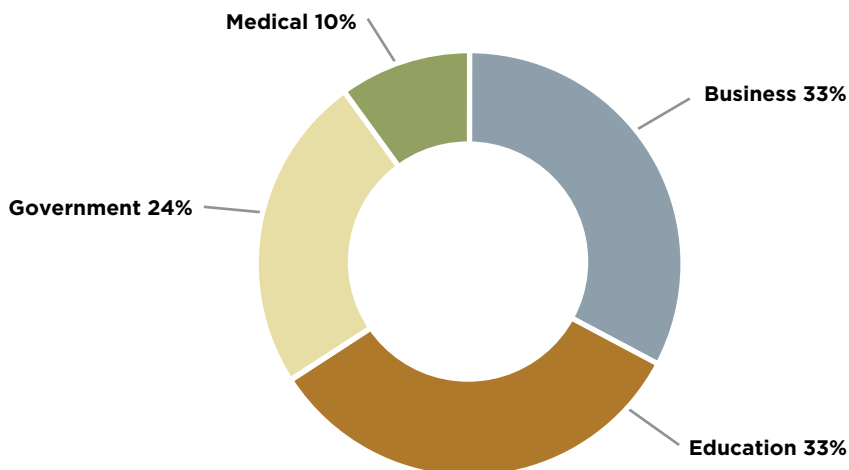
Here are two ways to achieve safe harbor:

Make it a practice not to retain sensitive cardholder data. For example, refrain from storing the cardholder’s primary account number (PAN) anywhere on your systems. (In this case, achieving safe harbor has more to do with policies and procedures than with technology.) Don’t confuse the need to keep transaction data (which you should) with the need to keep cardholder account data (which you should not). There is little need to keep any more than the last four digits of a cardholder’s PAN. Then, should a breach occur, the institution is in safe harbor: No sensitive data are compromised. Or, as they say in sports, “no harm, no foul.”

If you feel you must retain the PAN to process exception items, such as charge backs and refunds, at least purge those data after a defined period of, say, 90 days. By that time you will have processed most of your exception items, and you no longer need the account numbers. This approach has worked at the University of Notre Dame to help limit the scope of its PCI compliance effort.

Not retaining the PAN may appear extreme, and it may lead to additional back-office work. At IU, we requested that our merchant processing bank update all our terminal programs so that the PAN was no longer printed on any receipts or reports. The only cost was for staff time to request the changes and then to track progress and follow through to ensure campus merchants had implemented the changes.

FIGURE 3 Reported Security Breaches 2000–July 2007



Source: “Why Banks View Campuses as Risky Merchants,” *Exchange*, March 2007, Association of Financial Professionals

While the process is ongoing, we estimate the total staff time to complete the project is roughly three person-weeks of effort.

Encrypt all sensitive data stored on the institution’s systems. This alternative approach to securing information is consistent with PCI DSS, and it can achieve safe harbor—up to a point. Relying on protection alone, however, will not be sufficient; once staff copy transaction data to laptops, spreadsheets, and other media, such devices are rarely encrypted and can be lost or stolen.

Addressing this latter issue to some degree is the requirement in PCI DSS that calls for institutions to limit severely the number of staff with access to sensitive data. We suggest that you implement this vigorously.

A Word About Compensating Controls

Meeting each PCI DSS requirement in precisely the defined way is either impossible or impractical for most merchants. Recognizing this, provisions exist for “compensating controls,” whereby institutions can make the case that they have achieved the control objective by other means. For example, many institutions use automated voice response systems for payment card transactions.

Under PCI DSS, the sensitive cardholder data, such as security codes and passwords that cardholders provide during the taping, may not be retained. However, it is not practical to review each tape and delete the sensitive information. Since the tapes are not searchable electronically, the institution can meet the control requirement with the compensating control of ensuring that physical recordings are stored securely and that access to them is severely limited.

It is difficult to provide a guideline for compensating controls. Each institution is unique. The final decision as to what is acceptable rests with your “acquirer,” that is, the bank that processes your Visa and MasterCard transactions or the company—such as American Express, Discover, or Japan Credit Bureau—that issues the card. What may be acceptable for one university with one bank acquirer may not be acceptable in another situation. Keep in mind, though, that it is rare for a merchant that processes a large volume of transactions to achieve PCI compliance without at least applying one compensating control.

Gaining your acquirer’s approval for a compensating control is as much an art as a science. As technology costs decline, compensating controls are becoming less acceptable in some areas. In the meantime, work with your acquirer, while recognizing

that most compliant merchants (and vendors) use at least one compensating control.

Considering Outsourced Compliance

It can be attractive to use third parties to process payment card transactions, especially those transactions that are Web-based. Many vendors are PCI DSS compliant and offer fine products (go to www.visa.com/cisp for a list of PCI DSS compliant service vendors). Outsourcing such work, however, does not absolve your institution from its own PCI DSS compliance requirements. Since you are responsible for protecting your customers' data, ensure that your service providers are and remain PCI DSS compliant. Furthermore, establish that your communication gateways to the outside vendor are secure. You will also *receive* transaction reports from your acquirer that are likely to contain cardholder data that need to be protected.

Bottom line: While outsourcing can be a good decision, it is not a panacea for proper PCI DSS compliance.

Other Vulnerabilities

PCI DSS covers *all* transactions, not just electronic commerce. For that reason, other areas of risk come into play.

Older equipment. Many integrated point-of-sale systems, particularly older models, retain full magnetic stripe data. These devices can be vulnerable to hacking. Other terminals and POS devices use wireless communications that may not be strongly encrypted, making transactions containing magnetic stripe data easy to intercept. In both cases, sensitive cardholder data can be compromised.

Include your POS systems in your PCI DSS compliance scope. Security standards and good business practices may indicate the need to replace noncompliant POS systems and devices with more secure versions.

Shared networks. In addition to campus organizations and affiliates, many institutions have commercial operations that use their networks. For example,

campuses work with food service corporations that use their own POS systems together with the institution's network. If this is the case for your institution, implement contract language requiring the merchant to be PCI DSS compliant to minimize the additional risk of a network breach.

Ongoing Compliance and Security Vigilance

Adhering to PCI DSS requirements—and establishing other related business practices—is a significant accomplishment. Still, recognize that it is the beginning of an ongoing process. You'll

likely need to continue developing new policies and procedures along the way. They might include:

- informing merchants and potential merchants on campus about what is expected of them and how to achieve established objectives (IU has revised its Payment Card Merchant Agreement to reflect the additional duties and responsibilities placed on card-accepting campus organizations. One provision that was not changed, however, is that the office of the treasurer may revoke the ability of any campus merchant to accept payment cards, if the merchant violates proper procedures.)
- minimizing the number of staff with access to sensitive data
- training supervisors and keeping them updated
- developing and testing a response plan to deal with an information security breach

You'll still need to plan on surprises. It's possible that you could discover, for example, a merchant you didn't know about, or you might learn of a new card processing contract signed by a faculty member or auxiliary organization. Either situation

exposes the institution to risk.

A more subtle vulnerability can be found in older laptops, servers, and even paper records containing sensitive cardholder data. These collections of pre-PCI DSS data are like time bombs waiting to explode; they have been the cause of data compromises at some institutions. Work with your security team to scan all likely sources for 16-digit numbers (and maybe 9-digit Social Security numbers, too). Finally, make sure to electronically scrub those old laptops before they are recycled, donated, or sold on eBay. Data thieves shop online, too, and they are ever on the lookout for data-storage and older POS

Since you are responsible for protecting your customers' data, ensure that your service providers are and remain PCI DSS compliant.

devices that might contain caches of magnetic stripe data.

At the same time, new equipment can pose some risks. For example, new laptops for staff and faculty might lead to the transfer of sensitive data from previous computers. Make it standard practice to screen for and eliminate such information.

By implementing these information security practices, you'll not only bring your institution into compliance with the new standards, you'll also be creating business processes that will serve you well in many other areas of campuswide operations. In other words, achieving PCI DSS compliance is not only required, it makes good business sense for your institution.



WALTER CONWAY

is president of Walter Conway Associates, LLC, San Francisco, and

DENNIS W. REEDY is the managing director of treasury operations for Indiana University, Bloomington.

walt@walterconway.com

dreedy@indiana.edu