



E-Guide

# PCI DSS Compliance Overview and Best Practices

Any company that accepts credit cards for its business is subject to the Payment Card Industry Data Security Standard (PCI DSS). Yet an estimated 60% of merchants using credit cards aren't PCI compliant. Though PCI is an industry standard—not a government regulation—it can still be enforced with equal weight as a regulation by the credit card industry. A credit card company can cut a business off at the knees for noncompliance. A business can be fined, or worse—cut off completely from being able to process credit cards.

This SearchCIO.com and SearchSecurity.com E-guide offers an explanation of the requirements of PCI DSS and best practices for ensuring compliance with it.



E-Guide

# PCI DSS Compliance Overview and Best Practices

## Table of Contents:

[PCI compliance a good start, but not enough](#)

[PCI compliance without costly consultants](#)

[PCI standard still packs little punch](#)

[PCI Data Security Standard compliance: Three steps to success](#)

[PCI is about eliminating data, not securing it, former QSA says](#)

[Compliance recycling: Combining compliance efforts to manage PCI DSS](#)

[The 'security standards dilemma': Network segmentation and PCI Compliance](#)

[PCI compliance and Web applications: Code review or firewalls?](#)

[Midmarket CIOs turning to log management for compliance](#)

[Version 1.2 of Payment Card Industry \(PCI\) Data Security Standard answers questions, raises others](#)

---

## PCI compliance a good start, but not enough

By Linda Tucci, Senior News Writer  
SearchCIO.com

The news from Hannaford Bros. Co. was ugly: 4.2 million credit and debit card numbers stolen by a cyberintruder over three months. The breach affected 271 stores in the Hannaford supermarket chain, 23 independently owned markets and 70 banks nationwide. Some 1,800 fraud cases have already come to light. Within a week, the first of possibly many class-action lawsuits was filed against the Scarborough, Maine-based grocer.

The theft pales in comparison with 2007's massive data breach at The TJX Cos. involving 94 million cardholders, but the Hannaford intrusion marked another worrisome milestone. The heist occurred when customer data was in transit, as opposed to in situ in a database—the first known time that has happened on such a large scale.

Even scarier, unlike an estimated 50% of retailers out there, the company was in compliance with the Payment Card Industry Data Security Standards (PCI DSS) established by the major credit card companies, including Visa Inc. and MasterCard Inc., to ensure the privacy of stored customer information.

"PCI compliance is not enough," said Steve Rowen, partner and PCI expert at Retail Systems Research LLC (RSR), a Miami research firm specializing in technology and business challenges in the retail industry.

"Visa is a bank, not an IT company. The notion that Visa should be telling retailers, particularly retail IT-ers, how to secure their information is really a bit silly," Rowan said.

Visa, to its credit, was quick to identify the problem associated with the collection, retention and use of customer financial data by retailers, said Brian Kilcourse, managing partner at RSR and co-author with Rowen of "Customer Data Security, PCI and Beyond," a 2008 benchmark study of how retailers are approaching the PCI mandate.

Retailers, however, are collecting all kinds of customer data to customize and fine-tune their product offerings and improve customer service.

"PCI focuses exclusively on credit card payment data, but there is other stuff collected that is just as dangerous," Kilcourse said. "A good portion of the breaches are Social Security numbers. PCI has nothing to say about Social Security numbers."

The point? Looking at PCI compliance as a "checkbox project is not enough," Kilcourse stressed. Security is a fluid process that requires proactive measures to minimize the risk associated with the capture and retention of customer data.

Retailers who wish to tackle customer data security from a proactive standpoint "must successfully incorporate their payment-specific security measures into larger business initiatives."

## PCI pain points

The most common mistake retailers make in becoming PCI compliant, Kilcourse said, is to “map their applications to the mandate.”

“Retailers will come up with to-do lists, so, for example, ‘We have customer data in this application, therefore let’s map it over the mandate,’ as opposed to looking at all their applications through the lens of the mandate,” Kilcourse said.

But there are myriad places where data can be grabbed by a shadow or external process, Rowan said, and retailers know this—even if they can’t quite face up to it.

When Kilcourse and Rowen asked retailers to name the most difficult aspect of complying with PCI, the No. 1 hurdle cited by most was the ability to monitor access to the network. “There are so many points of data transmission in the network, they could not monitor them.”

In the case of the Hannaford breach, it is believed the credit and debit card numbers were stolen while in transit from the pin-pad device (where the card is swiped) back to the database—a weak spot firms like RSR have been warning retailers about since before PCI was instituted.

Retailers need to encrypt the data in all of its forms, not just in its in-state form, Rowan said.

“A lot of retailers cringe when you say this, because there are so many littler discreet handoffs of this data between Point A and Point B, that it can seem like a daunting task,” Kilcourse said.

---

## PCI compliance without costly consultants

By Joel Dubin, CISSP  
SearchCIO.com Contributor

Any company that accepts credit cards for its business is subject to the Payment Card Industry Data Security Standard (PCI DSS). As it is with other regulations, such as the Sarbanes-Oxley Act, the biggest component of being compliant is *proving* you're compliant.

Though PCI is an industry standard—not a government regulation—it can still be enforced with equal weight as a regulation by the credit card industry. The PCI Security Standards Council LLC is governed by the five largest credit card companies: Visa International, MasterCard International Inc., American Express Co., Discover Financial Services LLC and JCB Co.

A credit card company can cut a business off at the knees for noncompliance. A business can be fined, or worse—cut off completely from being able to process credit cards.

Better to have and not need, than to need and not have.

A PCI audit is something you can do without hiring an outside consultant. Your secret weapon: Documentation.

Auditors have a mystical attachment to paperwork, and if it isn't in writing in front of them, they won't see it. The only way to prove to an auditor that your company is compliant with PCI is to document every control required by the standard. In the eyes of the auditor, if a control isn't documented, it isn't compliant.

First, appoint someone to be the contact person for PCI auditors. This isn't a full-time job and doesn't necessarily even have to be someone from the IT department. The important thing is that this person has a sufficient background in IT and understands the technical terminology in the standard.

Next, go to the PCI Security Standards Council website and download three documents: the standard requirements, the self-assessment questionnaire and the security audit procedures.

PCI defines four levels of merchants. Any merchant processing fewer than 6 million transactions annually falls into the lowest three categories (levels two, three and four). Only level-one merchants are required to have an on-site audit. All the others can complete the self-assessment questionnaire annually on their own.

The standard documentation is to be used as a guide and final reference to how you fill out the questionnaire. The questionnaire is a series of check boxes that you must fill out and have on hand if the credit card companies come calling. The security audit procedure is a 50-page manual that instructs you on what to do and how to do it.

Going through these three documents thoroughly, checking off each item and providing documentation for each item will soothe even the most aggressive auditors.

There are 12 overarching requirements you will have to meet when filling out the documentation. Some of the requirements are no-brainers. But there are some that might need some explanation:

**Requirement: Install and maintain firewalls.** Make sure to have a network diagram documenting all connections to cardholder data. Also, make sure to have a firewall configuration standard that outlines all users and groups with firewall access, all services and ports open on the firewall and justification for the use of protocols other than HTTP, such as FTP, SSL, SSH and VPN.

**Requirement: Protect cardholder data.** Make sure to have a written policy describing data retention and disposal policies and procedures. This should include how long data is held, for what purpose and how often it's disposed of.

Another pain point here is encryption of cardholder data. Be able to produce documentation describing encryption methods and systems with the names of algorithms and their bit strengths.

**Requirement: Develop and maintain secure systems and applications.** Keep lists of security patches installed on systems and be able to show they are current with the patches issued by vendors. Be able to document software development practices and prove that they include security reviews during the development lifecycle.

**Requirement: Restrict access to cardholder data.** Be ready to produce a written policy showing that access to systems is based on the principle of least privilege and that there are systems in place for auditing provisioning of user access.

**Requirement: Require users to have unique IDs to access the system.** Documentation should be available describing authentication methods. Auditors may even ask for verification of all user IDs to make sure they're unique and have the appropriate level of privileges.

**Requirement: Track and monitor access to networks and cardholder data.** The requirement states that audit trails be turned on for network systems. Be able to produce copies of these trails for auditors.

**Requirement: Schedule quarterly security scans by an outside vendor.** This is a cornerstone of PCI. These vendors, called approved scanning vendors by the PCI council, conduct vulnerability assessments. Have copies of the last four assessments available for review by auditors.

**Requirement: Maintain an information security policy.** The policy should define responsibilities for employees and contractors. Also, make sure to have documentation of a security awareness program and an incident response plan.

Note that if you outsource any functions, such as processing and transmission of card data, you should identify those specific functions and who is handling them. Those vendors will be responsible for their own PCI compliance.

Ultimately, the key to PCI audits for companies of any size is to have documentation available of processes, policies and procedures. So, when auditors call, make sure to have your documentation in order.

---

**About the author:** *Joel Dubin, CISSP, is an independent computer security consultant. He is a Microsoft MVP specializing in Web and application security, and is the author of The Little Black Book of Computer Security, available from Amazon.com. He has a regular radio show on computer security on WIIT in Chicago and runs The IT Security Guy blog at [www.theitsecurityguy.com](http://www.theitsecurityguy.com).*

---

## PCI standard still packs little punch

By Linda Tucci, Senior News Writer  
SearchCIO.com

On June 30, 2008, retailers that accept payment card transactions were required to protect all Web-facing applications against attacks by either installing application-level firewalls in front of Web-facing applications or by doing application code reviews.

The requirement is spelled out in section 6.6 of the Payment Card Industry Data Security Standard (PCI DSS), established by the major credit card companies, including Visa Inc. and MasterCard Inc., to ensure the privacy of customer information. On June 30, the recommendation went from best practice to requirement.

What does the mandate mean? It means vendors are swooping in with products that promise to automate code review and make you PCI compliant. For example, Solidcore Systems Inc., a change control system provider in Cupertino, Calif., offers an embedded PCI product for point-of-sale (POS) devices that promises to protect against attacks like the Hannaford Bros. Co. breach in March.

Research houses are cranking out warnings on the risks of not complying. Typical is a study from Pleasanton, Calif.-based Javelin Strategy and Research showing that 40% of consumers change their relationship with a business affected by a security breach. The study also found that 56% of breach victims wisely prefer a solution that prevents fraudulent use of their information, over a credit-monitoring system that notifies them when their information has been stolen.

Of course, security experts are at the ready for comment. The eminently quotable Gartner Inc. security analyst Avivah Litan has observed (everywhere) that most of the Stamford, Conn.-based firm's clients were indeed not ready by June 30. And that most clients are opting for the application firewall rather than taking on the more onerous job of auditing their applications for flaws and fixing them.

But the important thing to note about the June 30 mandate, say many experts—including Litan—is that what is true about 6.6 is what has been true of PCI standards in general: The mandate is insufficient. Neither fix alone—the firewall or the review code—is enough to protect consumer data in Web-facing apps against attacks and, consequently, neither is sufficient to protect your company's reputation.

Critics of the PCI standards point to the Hannaford, which was PCI-compliant when secret malware installed on servers compromised more than 4 million credit and debit cards.

The PCI rules are written as standards, not laws, but noncompliance may pose legal risks for retailers, nevertheless. David Navetta of InfoSecCompliance LLC, writing in SC Magazine, believes standards such as PCI, set by a private body, could pose more risk than traditional government regulations. He advises merchants to engage their legal teams on PCI compliance.

Still, security expert Joseph Miller, an engagement manager in the technology risk management practice at Jefferson Wells International Inc. in Milwaukee, said the 6.6 requirement is important, even “though it may or may not be enforced by the merchant banks or card brands.” (Another hallmark of the PCI standards is that the group hasn’t gone after offenders.)

“I think it is good to become PCI compliant, but you need to assure that you have your own best practices in place and test your own processes,” Miller said.

He recommends to clients that they definitely take the PCI self-assessment questionnaire but also do their own internal testing. For example, restaurants would want to look at their process for accepting credit cards and use a data diagram that shows the actual path the cardholder data takes into the point-of-sale (POS) system, as well as the optimization of the transaction itself as it goes to the merchant bank or card company for processing, Miller said.

Test the whole process, Miller said, “and make sure that you are showing evidence that you are protecting cardholder data.”

At the core of good practice is the protection of cardholder data, as well as the card’s authentication data during the transaction, said Miller, who is a certified PCI assessor. He offers three recommendations for companies that accept payment card transactions for protecting cardholder data:

- Minimize storage time as much as possible. To do that, “you need to determine in the course of doing credit card transactions how long do I really need to keep the cardholder data,” he said. In the hotel industry, where Miller has done considerable consulting, the data needs to be kept for the duration of a guest’s stay. There are also regulatory considerations. Nevada, for example, requires retailers and casinos to keep credit transactions for as long as two years, in the event of disputes.
- Always store the primary account number in unreadable format (masked, except for the last four digits).

Encrypt the data if it needs to be stored for any length of time. Encrypt the data while it is transit, using protocols like Secure Sockets Layer and IPsec.

## PCI Data Security Standard compliance: Three steps to success

By Joel Dubin, CISSP  
SearchCIO.com Contributor

When Visa International, MasterCard International Inc., American Express Co., Discover Financial Services LLC and JCB Co. banded together in 2005 to draft the Payment Card Industry (PCI) Data Security Standard (DSS), they wanted to improve credit card security among merchants, retailers and banks that issue, use and process credit cards. For some businesses, the burden to comply can be onerous.

With 12 requirements, PCI compliance strikes fear even among larger companies with established information security departments and staffs equipped for handling compliance.

It's no wonder, then, that an estimated 60% of merchants using credit cards aren't PCI compliant. But noncompliance can be costly, if not fatal, to a business. Noncompliance can result in fines or, at worst, being barred from processing credit cards through a PCI council member.

There are three ways to stay PCI compliant:

1. Follow industry best practices for network and IT security.
2. Use tools and services geared toward PCI compliance.
3. Align with a larger partner for credit card processing.

### Industry best practices

The PCI standard, for all its critics, covers many common-sense approaches to IT security that most companies should already be following. These include requirement eight, which requires a unique ID for everyone with computer access, and requirement nine, which places restrictions on physical access to cardholder data. Most authentication systems require unique user IDs and passwords, and servers holding card data are often in isolated locked rooms or facilities.

Other requirements most companies may already be following include requirement one, which calls for firewalls around credit card data, and requirement two, which calls for changing vendor-supplied default passwords on systems. These are often routinely done by IT and network managers.

The toughest requirements can be requirement three, calling for the protection of credit card data, and requirement four, seeking encryption of data transmitted across networks. Requirement three states that cardholder data can be kept only as long as needed for the business, or for legal and regulatory purposes. But companies like to store data for customer convenience, bringing it up from a database rather than having to ask customers every time they buy something. Under PCI, not only does the transaction have to be encrypted, but the database holding the data must also be encrypted.

In addition, particularly at retailers, wireless devices are used so sales clerks can move around the store helping customers. Wireless networks open a whole new range of access to networks that require PCI compliance under requirements three and four.

Companies can comply with requirements three and four easily and cheaply by doing two things: isolating the portions of their networks that handle card data, and using what are called in PCI parlance “compensating controls,” rather than full-blown encryption. By isolating data on the network, only that network segment needs to be scanned and reviewed for PCI compliance. Otherwise, the company’s entire network must be compliant, adding costs for the scanning and auditing required for PCI.

Truncating card and account numbers, or obscuring them with one-way hash functions, qualifies as a compensating control for purposes of the standard. Encryption and key management can be costly and may require additional hardware. Truncating and hashing are cheaper shortcuts.

## PCI tools

The second approach covers a broad category of products. There has been some controversy about this, with complaints that vendors are coming out of the woodwork claiming to be PCI saviors. While there isn’t a PCI panacea, there are products on the market that can ease the compliance burden.

An interesting technology is tokenization, developed by Shift4 Corp. in Las Vegas. Tokenization replaces the credit card number on the point-of-sale (POS) device at the retailer with a token, or a reference number. The reference number is useless if sniffed in transit, as happened in The TJX Cos.’ breach, since it can’t be traced back to the cardholder or his or her account. Shift4 sells a driver for POS devices that generates and accepts tokens at a fraction of the cost of the expensive upgrades PCI would require to encrypt data sent and received by POS devices. Since the token isn’t the actual card or account number, under PCI it isn’t sensitive customer data and doesn’t need to be encrypted.

## Partner with a larger organization

Companies can use a third party to process their credit card. But this is recommended only for small retailers; medium-sized businesses will not benefit. This doesn’t absolve a storefront from minimum security precautions to protect its customer data. But the headache of being fully compliant with PCI will rest with the service handling the card transactions, not the small business.

While created for a good reason, there are some criticisms of the standard. One is it’s changing too rapidly for companies to remain compliant.. Another criticism, along the same lines, is PCI auditors sometimes provide contradictory answers on what constitutes legitimate compliance

**About the author:** *Joel Dubin, CISSP, is an independent computer security consultant. He is a Microsoft MVP, specializing in Web and application security, and is the author of The Little Black Book of Computer Security, available from Amazon.com. He has a radio show on computer security on WIIT in Chicago and runs The IT Security Guy blog at <http://www.theitsecurityguy.com>.*

## **PCI is about eliminating data, not securing it, former QSA says**

By Robert Westervelt, News Editor  
SearchSecurity.com

Forrester analyst John Kindervag says he's sick of hearing people whine about the payment card industry data security standard (PCI-DSS). A former qualified security assessor (QSA), Kindervag said companies often drag out compliance issues instead of dealing with them head-on.

"A lot of times you just have to get down in the mud and get it done," Kindervag said.

In his presentation at the Forrester Security Forum 2008, "The Inside Story of PCI: Confessions of a QSA," Kindervag presented ways companies can have a much smoother experience assessing their security systems and ultimately complying with PCI-DSS. He said PCI takes a different line of thinking from IT security pros and company executives, because it goes against the project-based culture of IT.

"Compliance is a marathon; A never ending marathon," Kindervag said.

To narrow down the scope of PCI, companies should first segment out network systems that contain credit card data. Next, companies need to understand not to introduce anything to those systems, Kindervag said. The easiest road to compliance: Don't store any credit card information, he said.

"PCI is a communicable disease," he said. "Anything you introduce can affect other things making them fall within the scope of PCI."

Banks and credit card carriers no longer require companies to save credit card data. Often companies save some of the data to handle returns, but there are now ways to handle a return without storing sensitive data, Kindervag said.

"PCI is not about securing sensitive data, it's about eliminating data altogether," he said.

Often companies get confused about Safe Harbor, an indemnification clause given to a company after it successfully complies with PCI-DSS. It provides merchants protection from fines and compliance exposure in the event of a data breach. The problem is that companies fail to keep complying with the standard after a QSA verifies that a company is compliant, Kindervag said.

"The only way to indemnify yourself from fines is to be compliant at all times," he said. "I know companies that were compliant at one time but fell out of compliance resulting in a breach."

### **Preparing for an assessment**

Companies shouldn't hire a QSA until they are absolutely sure they are in compliance with PCI, Kindervag said. Start by conducting a policy review. Make policies electronic by creating a Wiki, designed to making finding the

appropriate PCI requirements easier and give anyone who accesses it the ability to contribute and modify content, Kindervag said.

Next, conduct a gap analysis. Focus on wireless, Kindervag said. It's an area that is constantly changing and riddled with possible security holes. Also, implement layer 2 bridging on wireless networks so you don't have to re-architect the whole network, he said. Ensure that you're collecting log data, but understand that it's a requirement to aid the card brands.

"Logging is a backup requirement," Kindervag said. "It's a great place to consider outsourcing, but it's also a good place to start a threat management program."

Finally, prioritize the difficult projects, such as network segmentation and encryption deployments.

### **Hiring a QSA: An insider's perspective**

QSA's come in two flavors, Kindervag said, a hacker and an assessor. Find a QSA that you are comfortable with, he said.

Every QSA is unique and has their own way of doing things. Understand that QSAs have no power, the acquiring banks ultimately accept the final report. Although QSA's are hired by the merchant, they are independent and in many circumstances, they're required to make an ethical judgment, Kindervag said.

Conducting an audit is a tedious and time consuming process.

"If you find a QSA that likes the auditing process, you probably want to get a different one," he said.

Most QSAs start by conducting a policy review, followed by a log report review. The QSA also conducts sample testing of company systems for cardholder data. Once that is complete, the QSA completes the report on compliance (ROC).

"If you are not compliant, everything stops and you have to start all over again," he said.

## Compliance recycling: Combining compliance efforts to manage PCI DSS

By Diana Kelley, Contributor  
SearchSecurity.com

Going “green” is becoming a way of life for many of us. The “reduce, reuse and recycle” approach can help save materials and decrease impact on the environment.

In compliance work, the concepts of reducing work and “reusing” existing controls can also be applied. Many organizations have invested time and effort to implement ISO 27002 controls and certify against 27001 Information Security Management System (ISMS) processes. Others have adopted the IT management techniques from the UK Office of Government Commerce (OGC), known as ITIL. And many organizations have made significant investments to create a standardized compliance framework for use across business units and divisions.

Although compliance with the Payment Card Industry Data Security Standard (PCI DSS) cannot be accomplished by using another framework or methodology exclusively, organizations have found that they can leverage valuable mappings between existing frameworks. Additionally, some of the policies and tools implemented for PCI DSS may provide unexpected compliance benefits for other initiatives.

David Howell, senior manager of compliance solutions at RSA, the security division of EMC Corp., said he’s observed a desire for compliance normalization. Companies are looking for a “common framework that can be used to eviscerate the walls between disparate compliance programs,” Howell said, “defining commonalities so that pieces can be leveraged.”

Reuse can work bidirectionally. Controls implemented for PCI DSS can be used for other initiatives in the organization, and controls implemented before or independently of PCI DSS may be reusable as part of PCI DSS validation work.

Examples of PCI DSS controls that can be reused are policies and procedures related to protection of sensitive data. PCI mandates that sensitive authentication data cannot be stored after the authorization phase, but primary account numbers (PANs) can. Requirement 3.4 of the PCI DSS provides specific details on how PANs must be stored in order to achieve compliance. Implementing these specifics can be a challenge, involving the use of native encryption on databases, or a cryptographic gateway or library to encrypt the data before passing it to the data-base for storage. Such encryption requires key management, and PCI DSS also details rules regarding proper key storage, aging and control. With sophisticated storage protection in place, a number of companies have found that the techniques in Requirement 3.4 can be applied to other sensitive data in the organization.

Michelle Stewart, manager of data security for AirTran Airways, discovered some unexpected benefits from using PCI DSS controls. Monitoring systems that were put in place for PCI DSS became valuable tools for the operations and audit teams. Information from network and host scans were used to identify “devices that weren’t in compliance with company policy,” Stewart said. The increased visibility provided by the tools helped AirTran enforce policy management for non-PCI DSS-related initiatives like ensuring that no unwanted applications, such as streaming

radio, were running on the corporate network. Stewart said savvy companies can leverage IT spending intended for PCI DSS compliance for work beyond PCI DSS and card data protection.

The relationship between ISO 27001/27002 and PCI DSS is a little more complex, but worth investigating, especially for organizations that are ISO 27001 certified. ISO 27001 is a methodology for managing a security program using the Plan-Do-Check-Act (PDCA) quality control cycle. Organizations that build security programs can use ISO 27001 to certify their ISMS approach to the standard. ISO 27002, on the other hand, is a list of controls. The PCI DSS is something of a mix of the two; it encompasses both technical controls and defines management techniques and approaches. While a company could be fully ISO 27001 certified, that is no assurance that it is also PCI DSS compliant. Since controls in ISO 27001 are adopted based on an organization's risk assessment determination, the final decision regarding which controls to implement rests with the organization itself. PCI DSS is not that flexible; controls listed in the standard are mandatory for compliance.

However, if a company is ISO 27001 certified, it is likely that the organization has already implemented many of the controls that PCI DSS requires. Though the two aren't aligned, an organization could perform a gap assessment of existing controls, such as those implemented from ISO 27002, to the mandatory PCI DSS controls. Sections A.10, A.11 and A.12 of the ISO standard focus on more technical controls, and this is where the majority of the overlaps occur. The end result would be a delta highlighting additional controls required for PCI, potentially streamlining compliance and assessment work. Another benefit for ISO 27001 certified organizations is that extensive documentation is required. Insufficient documentation is a core reason that companies fail PCI DSS compliance, so having it in place for ISO will make the PCI compliance work easier.

Finally, the Unified Compliance Framework (UCF) is an interesting approach to compliance. Developed by Dorian Cougias and Marcelo Halpern, UCF attempts to help companies streamline compliance work by mapping normalized controls and management approaches. In February 2008, the group behind UCF published a "harmonization" that integrates the PCI DSS Self-Assessment Questionnaire (SAQ) v1.1 and PCI DSS requirements into the UCF. Companies using the UCF as a meta-compliance framework may find the integration document helpful for normalization and mapping between the two. The document is available to all PCI Qualified Security Assessors (QSAs) as well as UCF subscribers.

Compliance is a cornerstone to a healthy IT environment. Consider "going green" when it comes to compliance. In other words, rather than throwing out previous compliance work when new regulations come along, look for areas where controls and policies can be mapped and "recycled" for applicability to the new mandates.

**About the author:** *Diana Kelley is a partner with Amherst, N.H.-based consulting firm SecurityCurve. She formerly served as vice president and service director with research firm Burton Group. She has extensive experience creating secure network architectures and business solutions for large corporations and delivering strategic, competitive knowledge to security software vendors.*

## The 'security standards dilemma': Network segmentation and PCI Compliance

Stephen Cobb, Contributor  
SearchSecurity.com

While the exact details of the Hannaford Bros. data security breach may always be called into question, we do know that criminal hackers accessed as many as 4.2 million credit and debit card numbers by installing malware on the servers of more than 270 of the company's stores. The tactics used by the attackers raise serious questions for retailers and have equally serious implications for information assurance practices.

One of the questions that security professionals must ask is: "Could better network segmentation have prevented or limited the scope of the breach?" Some have also wondered whether the Payment Card Industry Data Security Standard (PCI DSS), with which Hannaford had been deemed compliant, adequately addresses the importance of that type of separation.

This tip will examine the practice of network segmentation; that is, building larger networks out of multiple and separate small networks or sub-networks, communications between which is strictly controlled.

### Passing PCI

So, how *did* a breach of this scale occur at a company that was compliant with PCI DSS? Apparently, malware installed on company servers intercepted card data as it was transmitted from cash registers to credit card processors. The malware then stored the purloined data on store computers before forwarding it to servers located offshore; from there it could be collected and used for fraudulent purposes (some 1,800 cases of such fraud were reported).

Some security-savvy consumers were quick to ask why the card data was not encrypted. The PCI standard, after all, generally requires card data to be encrypted when at rest or in transit over public networks. However, the guidelines do not specifically require encryption at the time of capture. Not surprisingly, since the incident came to light, Hannaford has started encrypting card numbers from the moment they are swiped at checkout counters. Many retailers already perform these actions as a best practice, although it is likely that many more currently do not.

Encryption on this scale can be expensive, both in terms of installation and of key management and maintenance, and even some security experts would agree that such a measure is overkill if certain other security measures are in place. The PCI DSS took this assumption into account. Contrary to some interpretations of the standard, PCI does not mandate encryption of card data at all times. In fact, the standard spells out how a company could avoid the use of encryption and still remain compliant through the use of "compensating controls" to protect data at rest. This approach is allowed "for companies unable to render cardholder data unreadable (for example, by encryption) due to technical constraints or business limitations."

The basis for such compensatory controls is spelled out in Appendix B of PCI DSS version 1.1, which makes it clear that "Only companies that have undertaken a risk analysis and have legitimate technological or documented

business constraints can consider the use of compensating controls to achieve compliance.” The standard goes on to make it clear that compensating controls consist of either a device or combination of devices, applications and controls that meet four very specific conditions:

1. Provide additional segmentation/abstraction (for example, at the network-layer)
2. Provide ability to restrict access to cardholder data or databases based on the following criteria:
  - IP address/Mac address
  - Application/service
  - User accounts/groups
  - Data type (packet filtering)
3. Restrict logical access to the database
  - Control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP)
4. Prevent/detect common application or database attacks (for example, SQL injection).

## **PCI on network segmentation**

So here we have PCI DSS 1.1 addressing network segmentation, and this is not the only place that mentions the practice. In discussing the scope of the standard, the PCI DSS preface notes that “Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment.” In other words, if you segment your network and keep cardholder data within its own segment, you will not only make it safer, you may also reduce the burden of PCI compliance, which was never intended to apply to all networked devices within an organization, only those that store, process, or transmit cardholder data. The standard suggests, but does not mandate, that companies keep cardholder data on a separate network segment behind a firewall with proper user authentication and a properly configured ACL (access control list). In this scenario, the task of compliance is potentially contained to that network segment.

Of course, implementing a network architecture that enables this type of segmentation may not be easy for some organizations given the way that their systems have evolved over time. However, one has to wonder why network segmentation was not part of the original architecture; after all, it is hardly a new concept. For more than a decade, well-designed systems built with data protection in mind have split internal networks into sub-networks. Not only are performance benefits to be gained, but such segmentation can also limit the scope of a compromise, whether it is an internal or external attack, a malicious breach or even a non-malicious misconfiguration. The separation-of-duties requirement in financial systems often drives network segmentation.

Network segmentation means that each network exists within a “boundary of trust.” Anything that crosses the boundary needs to be checked to make sure it can be trusted, whether they are devices, packets, protocols, applications or users. And the checks must be applied to both incoming and outbound traffic. We don’t yet know how malware got onto all those Hannaford servers, but it seems likely that they were all part of the same network; there is nothing in PCI DSS to say that’s not acceptable. But both PCI DSS and traditional network security thinking caution against putting all of those machines in the same network, particularly when, as in the Hannaford case,

---

they were known to transmit targeted data in the clear. It seems that whatever trust boundary existed did not prevent card data from being sent out of the network to offshore servers.

## **Segmentation and the 'security standards dilemma'**

What should the standard say about segmentation? This is the point at which we run into the "security standards dilemma." Make a security standard too broad and you risk making statements that boil down to something ridiculous like: "Protect all sensitive data at all times so that no attackers can possibly access it, ever." Get too detailed in prescribing specific technologies and you risk people saying things like: "Compliance does not require us to encrypt over non-public networks, so we don't" or "Network segmentation is not mandatory, so we don't use it."

The goal of any security standard is better security, but simply working to a standard cannot by itself create security. That result comes from smart system design, implementation and management, which weighs all of the risks, even as those risks evolve. If nothing else, the Hannaford breach teaches retailers that they need to up their game. Attackers are now well-funded and profit-driven. Simply getting certified as PCI-compliant will not protect against them (although it will protect against some finger-pointing and most of the fraudulent charges that result from attacks). It's important to note, too, that network segmentation is not a cure-all. A trusted user can always take advantage of that trust. However, by properly setting trust boundaries, you can limit that abuse.

**About the author:** *Stephen Cobb has nearly three decades of experience in computer audit, security, and data privacy. He authored a comprehensive manual of personal computer security in 1992 and has been a CISSP since 1996. One of the first analysts to predict that privacy concerns would become a leading driver of enterprise security, Stephen published a privacy handbook for businesses in 2002. A co-founder of two successful security startups, he helped develop ground-breaking network security technology acquired by Symantec in 2004. When he is not busy advising clients or conducting seminars, Stephen is an adjunct professor of Information Assurance at Norwich University, Vermont, where he helped create the curriculum for the award-winning Master of Science in Information Assurance degree.*

## PCI compliance and Web applications: Code review or firewalls?

Michael Cobb, Contributor  
SearchSecurity.com

When the Payment Card Industry (PCI) Security Standards Council released version 1.1 of the PCI Data Security Standard in September 2006, it clarified existing mandates and added, in Requirement 6.6, some new ones pertaining to the custom application code that handles protected payment card data.

Basically, the council offered enterprises a choice: have an application security organization review custom application code for common vulnerabilities, or install a Web application firewall in front of Web-facing applications.

In keeping with the council's measured approach to improving the security of payment card data, what was put forward as a "best practice" in 2006 became a full-blown requirement on June 30, 2008. Many companies are already bemoaning the burdensome nature of PCI compliance and will no doubt chafe at paying for either more outside consultants or more security hardware and software.

On the other hand, there are plenty of security professionals who will say that what the PCI DSS requires is nothing more than the same application development and deployment approach that many companies have used for years. I can think of several financial and telecom companies that adopted a similar strategy when working with internally imposed PCI-comparable standards in 1999. Since then, there has been an increase both in the number of people qualified to conduct code reviews and in the availability of commercially supported application-layer firewalls.

Amid today's threat climate, where there is no shortage of people prepared to use whatever attacks they can to gather and exploit payment card data, a strong case can be made for both putting an application-layer firewall in front of Web-facing applications and having application code independently reviewed. However, in the real world, where cost constraints have never been tighter, some enterprises must choose one or the other.

### The case for application firewalls

The main reason for an application firewall is that it will, if properly supported, actively protect against emerging threats, something a one-time code review will not. Sure, a code review might be able to list classes of attack against which the code is deemed secure, and a reviewer may be able to discount some emerging threats by referring to that list. A code review, however, does not provide a way to tweak application proxies in response to attacks.

One common argument against the application firewall is that it may be tricky to fit into an existing architecture. Another objection is that it may work out to be more expensive than a code review. Pricing varies between brands but you could easily be looking at a purchase cost of around \$5,000 for something that will handle around 900 MB of throughput, rising to around \$8,000 for 2 gigabites per second (Gbps). Total cost will depend upon the level of application traffic, ongoing licensing fees and personnel costs to manage and maintain your Web application firewall capability. However, if you have staff on hand with the skills to tune and manage an application firewall, like the folks who are already running your enterprise firewall, the additional cost may only be incremental.

## The case for code review

A code review is not cheap. For whomever performs it, you are probably looking at tens of thousands of dollars in cost, although the exact figure will obviously depend upon application complexity. Bear in mind, though, that a code review doesn't require the same level of ongoing care and maintenance as a firewall (although future code revisions will need review).

However, enterprises should already be budgeting for code review as part of the software development process. Unfortunately, some earlier PCI guidelines gave the impression that internal code reviews would not be acceptable. Thankfully, we now know it's possible to use an internal staff for the review if it is a) trained and specialized in application-code assessments and b) not the same people who developed the application, this according to the February 2008 "Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified" document.

This clarification document approves, with the above caveat, the "proper use of automated application source code analyzer (scanning) tools" and the "proper use of automated web application security vulnerability assessment (scanning) tools."

## Making the choice

So now it looks like there may be three avenues available, and in each case the choice may simply come down to people. Does the enterprise have staff who can:

- a. Configure and maintain an application-layer firewall?
- b. Perform a code review?
- c. Use a third-party vulnerability detection tool and fix any problems the review uncovers?

Of course, the decision could also depend upon architecture considerations and how well an application-layer firewall would work with existing systems and devices.

Another factor to consider, particularly for those leaning toward a third-party code review, is how comfortable the organization may be with the status of its code. It is not unusual for payment card applications to develop over time and include some legacy code of unknown origin and unclear purpose. A security staff may not want to remove legacy code and run the risk of breaking a mission-critical application. Without suggesting that anyone should sweep potential bugs under the carpet, placing a firewall in front of an application might be less costly, or less disruptive, than re-writing it in light of a code review.

Finally, it has to be said that PCI DSS, admirable as its goals may be, has been far from perfect in practical terms. Not knowing exactly where the PCI Security Standards Council has drawn the line with Requirement 6.6 can be frustrating for those who are otherwise keen to toe that line. To a security professional who would normally urge the use of both code reviews and firewalls, it is another example of the compliance dilemma. If you promulgate a standard intended to increase security, you must be prepared to answer the question: "What must I do to comply with the standard?" The problem is, the question often becomes "What is the minimum I can do to be in

compliance?” Just a few weeks ago, the PCI Council also released a clarification stating that companies can either perform the code review or install the application firewall, but that they would ideally like to see enterprises do both.

I recommend taking the time to understand PCI’s Web application requirements, including the clarification documents, and consider how the approved options mesh with your architecture and resources. It is now clear that enterprises have multiple paths to compliance and, if executed properly, any of the options will not only help achieve compliance, but also improve Web application security.

**About the author:** *Michael Cobb, CISSP-ISSAP is the founder and managing director of Cobweb Applications Ltd., a consultancy that offers IT training and support in data security and analysis. He co-authored the book IIS Security and has written numerous technical articles for leading IT publications. Mike is the guest instructor for several SearchSecurity.com Security Schools and, as a SearchSecurity.com site expert, answers user questions on application security and platform security.*

## Midmarket CIOs turning to log management for compliance

By Shamus McGillicuddy, News Writer  
SearchCIO.com

Midmarket firms are looking for affordable log management technology to help them deal with growing scrutiny from regulations such as the Payment Card Industry Data Security Standard and the Health Insurance Portability and Accountability Act (HIPAA).

"The midmarket tends not to have security staff, or the need for a security console," said Eric Ogren of The Ogren Group, a Stow, Mass.-based consultancy. "They just need to collect event log data that they can produce on demand. The midmarket is not trying to boil the security management ocean. They just need to retain event log data for PCI compliance."

Log management tools collect the logs that devices produce for every transaction, store them centrally and offer varying levels of analysis that allow administrators to detect unsanctioned activity and hardware and software failures.

"There's an alphabet soup of regulations, but what's really been driving the need for log management is PCI," said Nick Selby, senior analyst and director of the enterprise security practice at New York-based The 451 Group. "These standards really have bite. The vision of a CEO in an orange jumpsuit has been replaced with the image of not being able to process credit cards."

With that in mind, vendors of log management technology are trying to offer products midmarket companies can afford. For instance, Houston-based Alert Logic Inc. offers Alert Logic Log Manager, a product delivered through the Software as a Service model. Instead of paying up to \$75,000 up front for a log management appliance, Alert Logic customers can pay \$1,500 a month.

Other log management vendors are offering more affordable appliances. ArcSight Inc., a Cupertino, Calif.-based vendor of security and compliance technologies, offers ArcSight Log Management Suite, a log collection, archival and analysis appliance line with a starting price of \$20,000.

"Most of the log management vendors have a low-end product like that, but ArcSight is not known for its low prices," Selby said. "It's good to see they're really taking a fairly bottom-to-top look at the log management market. But this product is by no means as mature as its competitors in that space, such as LogLogic and even LogRhythm. But we have seen ArcSight devoting a fair amount of resources to this. We believe the midmarket will continue to be an expanding opportunity for the log management market."

Ogren said ArcSight's product has three features that will appeal to the midmarket. He said it has focused functionality on log data management that makes it easier for midmarket administrators to use. He said the remote connectivity makes it easier for midmarket companies to include branch offices. And he said the appliances are easy to just plug into the network. They autodiscover each other, so there is minimal upfront work to get the product going.

## Tool helps hospital exec 'bubble up' info

Arsen Kousnoutdinov, manager of networks, security and telecommunications at Boston Medical Center, said he has used ArcSight's log management technology for three months. Compliance and security are part of Kousnoutdinov's business case for the technology, but his initial motivation was to improve the performance and availability of the network at the \$909 million hospital.

"I wanted to have the ability to bubble up the most important information every day," Kousnoutdinov said. "I wanted to know when hardware failures happen, when a power supply fails, when something gets disconnected. When it happens, it might not be catastrophic [because of redundancies] but if something else happens there's a problem."

Kousnoutdinov said he's also preparing for future HIPAA audits and other regulatory requirements by adopting ArcSight.

"I know that those occurrences of audits are not unheard of," he said. "I'm positioning myself for future regulatory action. Part of what I have to deal with also is security matters at Boston Medical Center. We sometimes get involved with legal and human resources on incidents outside the work norm. If someone is utilizing the Internet not according to policy or sometimes with criminal intent. I deal with legal quite a bit, the state police and local authorities. Log management may be utilized at some time for some of that."

Prior to adopting ArcSight, Kousnoutdinov managed logs with a combination of the syslog monitoring tools in CiscoWorks and a homegrown syslogger the hospital built on Linux.

"CiscoWorks did not help at all," Kousnoutdinov said. "It was quite a heavy solution to implement and use, and every time a Java update came around it rendered the logs useless because of incompatibility."

Kousnoutdinov said his homegrown syslogger sniffed logs, but his administrators had to manually search through the stored logs.

"The homegrown solution was to make sure we captured the logs, but it was like looking for a needle in a haystack to find a specific log," he said.

With ArcSight, Kousnoutdinov said he can see what's happening with his most critical logs over a day, a month or a year and respond quickly. He said ArcSight's user interface is also more user friendly than other log management products.

"I had to have a point-and-click interface," he said. "I had to get away from a dependence on Linux or Unix knowledge and have my lower-experienced staff be able to use this application. It enables me to free up the utilization of our most senior staff, which needs to be spending time doing something other than logging."

With 1,000 wireless access points, 400 network switches, 100 routers and about 8,000 workstations, Kousnoutdinov estimates that his total investment with ArcSight's log management technology will be about \$85,000. He said that's cheaper than he would have spent with some of the company's competitors. He said he also uses some of ArcSight's other products, so going with its log management product made more sense.

---

## **Version 1.2 of Payment Card Industry (PCI) Data Security Standard answers questions, raises others**

By Diana Kelley, Contributor  
SearchSecurity.com

On Aug. 18, 2008, the PCI Security Standards Council, stewards of the PCI Data Security Standard, released a four-page summary document detailing changes in the upcoming 1.2 version of the PCI DSS.

The clarifications to the standard are great news, but what most retailers, merchants, and processors want to know is: "What will v1.2 mean to my organization?" Will the new version require additional PCI work, such as more processes, procedures, and technical product purchases? This analysis of the expected changes will seek to answer those questions.

### **PCI 1.1: Open to interpretation?**

Here's the good news: PCI DSS version 1.2 is not a sweeping rewrite of version 1.1. Most of the changes listed in the summary document are clarifications of wording and terminology. Bob Russo, general manager of the PCI Security Standards Council, said of the group's goal was "eliminating as many questions as possible."

Many will likely welcome the changes, since some terms were poorly defined in the last iteration, making them confusing and difficult to interpret. For example, Requirement 6.6 of version 1.1 called for an "application-layer firewall." Retailers and PCI assessors (QSAs) alike wondered whether an application-layer-aware firewall, like the Cisco Systems Inc. PIX or ASA firewall, would suffice, or if it called for a Web application firewall like Barracuda Networks Inc.'s Web Site. Although the summary changes continue to reference "application-layer firewall," the Council issued specific guidance on the terminology regarding product type intended. Troy Leach, technical director of the PCI Security Standards Council, said that the testing procedures for Requirement 6.6 in version 1.2 make it clear that the Council is referring to Web application firewalls.

Other terms that received clarification and usage consistency makeovers are primary account numbers (PANs) and "strong cryptography." In version 1.1, "strong cryptography" is not defined, however, the audit/assessment procedures used by QSAs did list "Triple-DES 128-bit and AES 256-bit" as examples. Still, questions remained about AES 128-bit; was it acceptable? The clarifications in version 1.2 should answer these questions.

Another tricky one: does the PCI DSS apply to electronic media exclusively or is paper included? According to version 1.2, it applies to both electronic and paper media that contains cardholder data. This will create additional work for those organizations that had misinterpreted version 1.1 and kept paper media out of scope during DSS compliance work.

## Compensating controls

When enterprises are not able to meet the exact letter of the standard, they look to controls that will provide the same level of protection. Perhaps the most well-known example of this is PCI Requirement 3.4, which requires that *if* PANs are stored, they must be either rendered unreadable (by one-way hashing or truncation) or encrypted (using strong cryptography). When many organizations found neither of these options was feasible, Appendix B of PCI DSS version 1.1 provided a list of acceptable compensating controls that could be used in place of those listed in the requirement.

Version 1.2 provides additional information about compensating controls and flexibility options for other requirements. In the updated standard, Requirement 1 eases the timeline for reviewing firewall rules from quarterly to every six months. And the 30-day patch cycle, from the often-dreaded Requirement 6, now has *"added flexibility... by specifying that a risk-based approach may be used to prioritize patch installation."* Under version 1.1, many retailers scrambled to install patches within 30 days, often short-circuiting their standard patch life cycle testing in an effort to meet the strict timeline. A thorough approach to patching, however, requires testing, prioritization, and a robust pre-production process, which can take longer than 30 days. The change allows for risk-based approaches that may require more time.

Another welcome change concerns physical security. PCI DSS Requirement 9 called for cameras to monitor *"sensitive areas,"* but was an area like a restaurant dining room—where credit cards are handed to staff—considered sensitive enough to require a camera? How about a point-of-sale (PoS) cash register at a food court kiosk? Under version 1.2, organizations now have more flexibility to select other access control mechanisms when appropriate.

And though it's not in the summary document, the Council has stated there will be additional clarifications regarding definition of scope. According to Leach, the next version of the standard will include a section on scoping and sampling to explain what's within the PCI assessment and what is not.

## More requirements?

While the clarification and compensating control changes are welcome, there appear to be some additional requirements in version 1.2. For example: *"Wireless must now be implemented according to industry best practices (e.g., IEEE 802.11x) using strong encryption for authentication and transmission."* For those of you who thought perhaps the Council meant 802.1X, you're not alone; I thought that at first, too, because 802.11x is a placeholder for upcoming standards and not an IEEE standard.

Leach said 802.11x was used to indicate that upcoming versions of the DSS may include recommendations for using emerging 802.11 standards, such as 802.11i. So for more specifics, we'll all have to stay tuned. On the plus side, version 1.2 will continue to allow SSL/TLS and IPsec for protection of data transmissions over both wired and wireless networks.

Some potential heartburn may come from this change regarding wireless network encryption: *"New implementations of WEP are not allowed after March 31, 2009... Current implementations must discontinue use of WEP after June 30, 2010."* Wired Equivalent Privacy (WEP) has been broken for many years, so it makes sense for the Council to call for an end to its use in cardholder data environments, but many "out of the box" point-of-sale packages still commonly rely on WEP for proper operation. The two-year timeline for complete replacement of these systems may be too aggressive for retailers. If so, the Council will need to amend the timeline.

Finally, the antimalware requirement has been updated to include "all operating system types." Antimalware for Mac platforms and Unix/Linux are available, but options are limited. As for mainframes (like System z), there just aren't options. Look to the actual wording in version 1.2 for clarification beyond what is listed in the summary. It is unlikely that mainframes will be included in the final list. Also, for platforms like mainframe and some flavors of UNIX, organizations can consider layering anti-malware protection by using gateways or other compensating controls.

**About the author:** *Diana Kelley is a partner with Amherst, N.H.-based consulting firm SecurityCurve. She formerly served as vice president and service director with research firm Burton Group. She has extensive experience creating secure network architectures and business solutions for large corporations and delivering strategic, competitive knowledge to security software vendors.*