



WHITE PAPER

Lessons Learned: Top Reasons for PCI Audit Failure and How To Avoid Them

VeriSign® Global Security Consulting Services





CONTENTS

+ Top Reasons Customers Fail PCI Audits	3
+ Compromise Trends	4
+ Correlating Audit Failures and Compromise Trends	5
+ Practical Tips: What You Can Do Better	6
+ Store Less Data	7
+ Understand the Flow of Data	7
+ Encrypt Data	8
+ Address Application and Network Vulnerabilities	9
+ Improve Security Awareness and Training	11
+ Monitor Systems for Intrusions and Anomalies	12
+ Segment Credit Card Networks and Control Access to Them	13
+ Future Considerations	14
+ Glossary	15
+ For More Information	16



Lessons Learned: Top Reasons for PCI Audit Failure and How To Avoid Them

Since Visa mandated the Cardholder Information Security Program (CISP) in June 2001 and MasterCard® introduced the new Site Data Protection (SDP) program in June 2004, many merchants, processors, and acquiring banks have been working diligently to meet their specific requirements. Today's Payment Card Industry Data Security Standard (PCI DSS), which combines requirements of the Visa and MasterCard programs, prevails as one of the most preeminent achievements in the information security industry. However, many merchants and service providers are struggling with the increased complexity associated with the PCI Data Security Standard. Although the drive to protect credit card data is vital, many companies have yet to implement the technology and processes needed to address the standard's specific requirements. Even companies that have welcomed the standards are discovering holes in their PCI compliance strategy.

As a leading provider of PCI assessments and supporting security services, the VeriSign® Global Security Consulting team has performed several hundred PCI assessments since the program's inception. The requirement failures and actual compromises that we have observed during these assessments exhibit common themes. This paper identifies proven tactics that help companies achieve PCI compliance and, more importantly, avoid compromise.

+ Top Reasons Customers Fail PCI Audits

VeriSign was one of the first assessors to conduct an onsite audit and scanning service under the Visa Cardholder Information Security Program (CISP) and MasterCard Site Data Protection (SDP) program. Since the beginning of these programs, we have performed more than 100 assessments annually. Over the past four years, PCI customers have included merchants and service providers of all sizes, but mainly in the Level I category. The following chart, based on a sampling of actual PCI engagements, lists the ten most commonly failed PCI requirements. The Percentage column indicates the percentage of assessments that were non-compliant with the particular requirement.

Backup Tapes, PCs, and Laptops: Do You Know Where Your Data Is?

Loss and theft of backup tapes, PCs, and other physical assets that hold credit card data is taking a higher profile as financial institutions, universities, government agencies, and other sectors report significant losses. With almost half the states having security breach reporting laws, the risk of reputation damage for compromised companies is significant. A review of data breaches reported to the Privacy Rights Clearinghouse reveals sobering information. The analysis spans the period from February 15, 2005 to January 25, 2006. Of 114 reported data breaches*, representing 52.5 million compromised records, 38 percent were due to lost or stolen hardware or backup tapes. Although the breaches accounted for only 14 percent (7.7 million) of the records compromised, the high toll underscores the need to understand the flow of data in your organization and to better protect data and the repositories it is stored in.

*Privacy Rights Clearinghouse, *A Chronology of Security Breaches Since the ChoicePoint Incident*, originally posted April 20, 2005; updated January 27, 2006 <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

PCI Requirement	Percentage of Assessments Failing
Requirement 3: Protect stored data.	79%
Requirement 11: Regularly test security systems and processes.	74%
Requirement 8: Assign a unique ID to each person with computer access.	71%
Requirement 10: Track and monitor all access to network resources and cardholder data.	71%
Requirement 1: Install and maintain a firewall configuration to protect data.	66%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.	62%
Requirement 12: Maintain a policy that addresses information security.	60%
Requirement 9: Restrict physical access to cardholder data.	59%
Requirement 6: Develop and maintain secure systems and applications.	56%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.	45%

Source: VeriSign sample of 112 assessments, where 30 ultimately passed and 82 did not

Although many customers that came to VeriSign for these assessments had robust security programs in place, less than 25 percent passed the assessment on their first attempt. Those that did pass were Level II or smaller Level I service providers. This can be attributed to the smaller, less complex nature of their environments. Companies were most frequently non-compliant with Requirement 3 of the PCI Data Security Standard: 79 percent of the failed assessments did not meet the requirement to protect stored data (that is, they did not encrypt data). In most cases, a company failed multiple requirements. The top five most commonly failed requirements were failed by at least two-thirds of companies.

+ Compromise Trends

In addition to PCI non-compliance data, a key data point for understanding security challenges in credit-card processing environments is the actual compromises that occur in the field. Besides conducting PCI assessments, VeriSign is also an approved provider of forensic and investigative services for compromised entities. Our consultants have responded to numerous incidents over the past four years, many of them high profile. Through these investigations, we have discovered a number of security issues that contribute to these compromises.

VeriSign consultants frequently encounter the following weaknesses when responding to compromises:

- **Unsecured physical assets.** Unencrypted data may be stored on backup tapes and other mediums that are prone to loss or theft (see sidebar, *Backup Tapes, PCs, and Laptops: Do You Know Where Your Data Is?*).
- **Point of sale (POS) application vulnerabilities.** Applications may be creating logs that store card track data. PCI requirements prohibit the storage of track data under any circumstance. Nefarious individuals who are interested in obtaining track data know which applications store this data and where the information is typically stored.

- **Unencrypted spreadsheet data.** Users may be storing card data in spreadsheets, flat files, or other formats that are difficult to control as they are transferred to laptops, desktops, and wireless devices. A key source of PCI audit failure is storing unencrypted data in Excel® spreadsheets.
- **Poor identity management.** Users and administrators may not be handling authentication properly. Although password-based authentication is one of the easiest authentication methods to implement, it is also the most prone to compromise, because passwords can be easily shared, stolen, or guessed.
- **Network architecture flaws; flat networks.** Many businesses did not develop their IT infrastructure with security in mind. They often fail PCI assessment because they have very flat (non-partitioned) networks in which card databases are not segmented from the rest of the network. The lack of a secure network enclave is a serious issue regardless of PCI implications, and can be very difficult to remediate.
- **Lack of log monitoring and intrusion detection system (IDS) data; poor logging tools.** Without log information, it is difficult to determine whether processes and security systems are working as expected. In addition, insufficient data makes it more difficult to investigate compromises that do occur. For example, if there were no record of the timeframe of a compromise, it would be difficult to determine the number of credit cards exposed during the compromise.
- **Card numbers in the DMZ.** POS terminals may be storing credit card numbers in the externally facing perimeter network. In some companies, the POS terminal acts as a card-present terminal that sits on the Internet. Because there is no firewall between the system accepting the card-present transaction and the Internet, this arrangement does not comply with PCI requirements (and hackers can easily find credit card data). Frequently, these systems are also storing track data.

+ Correlating Audit Failures and Compromise Trends

The following chart maps PCI audit failures to compromise trends and recommended tactics (discussed below). It's important to note that compromise trends do not always map directly to audit trends. In some cases, an organization may pass a PCI requirement and still be vulnerable to compromise. For example, Requirement 6 of the PCI Data Security Standard states that companies must develop and maintain secure systems and applications. The VeriSign consulting team often encounters companies that can pass this requirement, even though their applications are compromised. Of course, if the company tests the application, as required by Requirement 11 of the PCI Data Security Standard, it will be more likely to detect any vulnerability, and thus the application will less likely be compromised when exposed to the Internet. This example illustrates the interdependence of the PCI requirements and highlights the importance of a defense-in-depth approach to credit card security. A company can have strong policies and state-of-the-art technology, but it must also regularly test its network, firewalls, and applications to ensure that these security measures are working properly and data is secure.

<i>Top Five Failed Requirements</i>	<i>Relevant Compromise</i>	<i>Recommended Tactics</i>
Requirement 3: Protect stored data.	Unencrypted spreadsheet data; unsecured physical assets	Store less data; understand the flow of data; encrypt data
Requirement 11: Regularly test security systems and processes.	POS/shopping cart application vulnerabilities; most data compromises can be attributed to a Web application vulnerability	Rigorously test applications; scan quarterly
Requirement 8: Assign a unique ID to each person with computer access.	Weak or easily guessed administrative account passwords	Improve security awareness
Requirement 10: Track and monitor all access to network resources and cardholder data.	Lack of log monitoring and IDS data; poor logging tools	Install intrusion detection or prevention devices; improve log monitoring and retention
Requirement 1: Install and maintain a firewall configuration to protect data.	Card numbers in the DMZ; segmentation flaws	Segment credit card networks and control access to them

+ Practical Tips: What You Can Do Better

In conducting PCI assessments and helping companies meet compliance requirements, VeriSign consultants have identified a number of tactics that address the core reasons that companies fail PCI audits. These tactics—when applied collectively, consistently, and across the entire enterprise—help create an environment that lends itself to compliance and minimizes the need for piecemeal, reactionary solutions. In addition, these tactics take into account the real-world environments and limitations that many companies face. In most cases, companies already have the needed infrastructure to create better security and improve compliance. It’s simply a matter of finding creative solutions.

The following sections will discuss these tactics:

- Store less data
- Understand the flow of data
- Encrypt data
- Address application and network vulnerabilities
- Improve security awareness and training
- Monitor systems for intrusions and anomalies
- Segment credit card networks and control access to them

Creative Solutions: How One Take-Out Chain Is Eliminating Credit Card Numbers from Its Environment

One of the nation's top take-out food chains, with more than \$4.6 billion in 2004 sales, worked with VeriSign® Global Security Consulting to implement a surprisingly simple, cost-effective alternative to encrypting credit card numbers: The innovative solution allows the company to accept credit card payment without storing or transmitting credit card numbers. The company uses a one-way hashing algorithm to transform card numbers into strings of code that uniquely identify each card account without revealing the account number itself. This allows the food chain to use a hash as a record key, much like it would use a credit card number. The company can still perform all necessary business processes—from conducting credit research and tracking sales data, to settling transactions and collecting payment. Even when a business process requires the card number itself, the number can be easily retrieved in a manner that transfers risk away from the company, and back to the acquiring bank or processor (i.e., the institution that processes credit card authorizations and payments for merchants). Alternatively, when storing the actual card number is essential, the company can store the number on a secure, smaller subset of its entire network. By eliminating card numbers from its environment, the food chain has greatly narrowed risk exposure and thereby reduced the impact of PCI requirements and assessments on its organization. In addition, creating and implementing the functionality was simpler and far more efficient and cost-effective than planning, implementing, and managing public key infrastructure or other strong encryption mechanisms.

+ Store Less Data

By storing less credit card data, you reduce not only risk but also the scope of what falls under PCI regulations and auditing. Many companies store card data simply because they have always done so or because they do not regularly purge their systems of information that is no longer needed. Others store card data because they believe—often mistakenly—that the information is required for auditing, business processing, regulatory, or legal purposes. Often, they confuse the need to store the card's transaction history with the need to store the number itself.

Increasingly, companies are discovering that they may not need to store card numbers at all; or that they can remove numbers from the general environment and store them in isolated segments of the network. One-way hashing, truncation, and other techniques allow companies to perform discovery, fraud analysis, audits, charge-backs, and other tasks without storing a card number. For more information on using relatively inexpensive one-way hashing to replace credit card numbers, see <http://www.verisign.com/static/036133.pdf>

What you can do better: Justify the storage of credit card data. Determine where credit card data exists in your organization, what it is used for, and whether it is needed there. In addition, be sure that legacy reports have been modified to remove data that is no longer needed.

One large, top-tier VeriSign financial customer went a step further: It completely cut off access to credit card data, and allowed exceptions only for departments that could prove they needed the data. Doing so forced constituents to develop creative alternatives to storing credit card data.

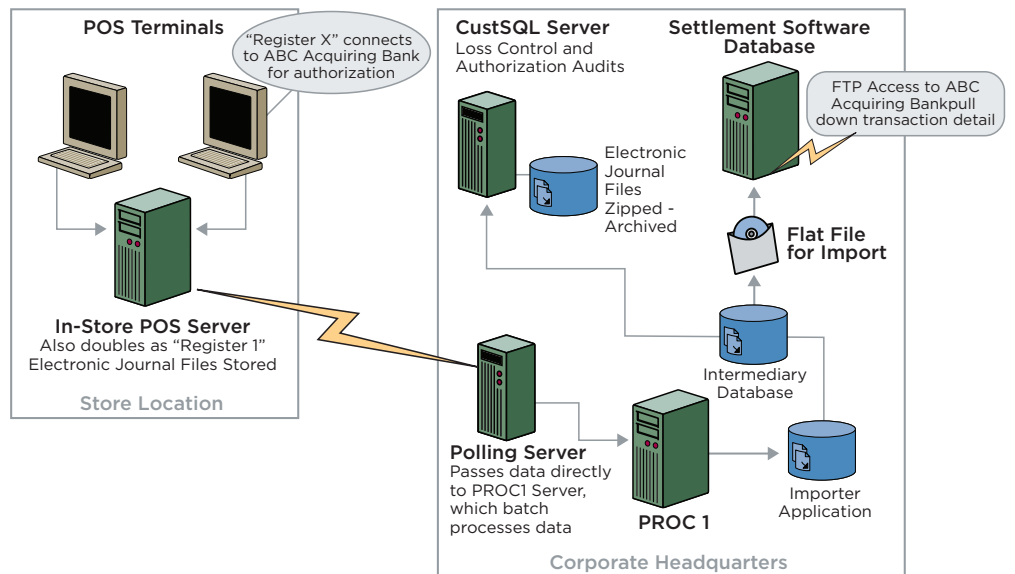
+ Understand the Flow of Data

Many companies have no diagrams or documentation showing how credit card data flows through their organization. Unless you have performed a system-wide audit of all data repositories and then continue to perform audits regularly, you have no way of determining where data lives and whether you're complying with PCI standards. Companies can curtail many of the compromises discussed earlier by tracking the flow of data and then correcting the associated problem.

In one PCI engagement, VeriSign tracked the flow of card data to 60 different locations in the company. By removing, scrubbing, or masking the card number, VeriSign consultants helped the company reduce the flow of card data to just three locations while maintaining full business process functionality for all users who needed transaction data.

What you can do better: Document the flow of credit card data throughout your organization. Understand where data goes—from the point where you acquire it (either from a customer or third party) to the point where the data is disposed of or leaves your network. The following illustration is an example of a flow diagram for credit card data.

Sample - Data Flow Diagram



+ Encrypt Data

Encryption is a key component of the “defense-in-depth” principle that the PCI attempts to enforce through its requirements. Even if other protection mechanisms fail and a hacker gains access to data, the data will be unreadable if it is encrypted. Unfortunately, many companies store credit card data on mainframes, databases, and other legacy systems that were never designed for encryption. For these companies, encrypting stored data (data at rest) is a key hurdle in PCI compliance.

Typically, companies choose one of the following options in order to remediate encryption problems:

- **Retrofit all applications.** With this approach, encryption is rolled into the coding of the payment application. Instead of writing the card number to a database, the payment application encrypts the number first. The database receives and stores the already-encrypted number. This approach is popular with companies that outsource their payment applications to other vendors, for example, small banks that provide online banking. In these cases, the vendor handles the encryption.
- **Use an encryption appliance.** A new class of appliance sits between the application and the database. It encrypts the card data on the way into the database and decrypts the number on the way out. Most companies use this approach because the trade-off between expense and business disruption versus time to deployment is very good.
- **Use an encrypting database.** An encrypting database offloads encryption to the storage mechanism itself, so companies don't have to significantly modify their applications or buy an appliance. This product, which is new from Oracle, also provides fairly good key management. However, it is very expensive. In addition, it does not operate on IBM® mainframes and AS400®, which financial institutions—especially card processing and fulfillment banks—tend to rely on.

- **Obfuscate without encryption.** Another way around encryption is to not use it. The PCI Data Security Standard calls for obfuscation—making the credit card unreadable—not encryption. One-way hashing, truncation, and other approaches are less costly to implement than encryption, and in many cases, companies can still perform all necessary business functions related to credit card numbers. For more information about one-way hashing in credit card environments, please see <http://www.verisign.com/static/036133.pdf>

What you can do better: Incorporate encryption at the development phase. Use an encryption framework during development instead of developing applications and then retrofitting them for encryption.

What you can do better: Have an overall encryption strategy. A typical company has multiple encryption requirements—for everything from VPN tunnels using IPSec, email secured by SMIME, and SSL certificates, to mainframe, database, and disk encryption (e.g., for users with laptops). To minimize costs and avoid problems associated with managing multiple keys, consider a strategy that encompasses not only PCI requirements but the entire range of encryption requirements within your organization. Then, consolidate key management to the fewest number of points possible.

+ Address Application and Network Vulnerabilities

Many application and network vulnerabilities can be remedied by updating POS applications, identifying poorly coded Web applications, and scanning quarterly. The best approach, however, is to develop applications with security in mind.

Update POS Applications

Some POS terminals, Web shopping carts, and other payment applications—especially older versions—automatically generate log files that store track (full magnetic stripe) data, CVV2 data, and other credit card information, even though PCI regulations prohibit doing so (even if the data is encrypted). Many merchants are unaware that this is occurring. To help address vulnerabilities at the application development level, Visa has developed Payment Application Best Practices guidelines for software vendors. Visa also publishes a list of CISP-Validated Payment Applications. Using products from these vendors will help you avoid this problem and other application vulnerabilities. (For more information about the Visa guidelines or vendor list, see URLs at the end of this paper.)

What you can do better: Update your software with patches as they are released. Ask your POS application vendors whether their current or older-version applications store track data. Validate their statements yourself by testing the application or looking for third-party validation of the output and data stores. Many application vendors are releasing new software versions that comply with Visa's Best Practices program.

Identify Poorly Coded Web Applications

Many data compromises occur because of improper coding, especially in Web applications. In fact, Web application vulnerabilities account for the largest percentage of compromise cases that VeriSign sees. Poor coding can result in weak password control or applications that are vulnerable to SQL Injection and other attack vectors. The Open Web Application Security Program (OWASP), referenced in the PCI Data Security Standards, provides information on these attack vectors. SQL Injection attacks are especially threatening because hackers can penetrate the network simply by using an Internet browser to execute code at the database layer of an application. This code can cause the database to hand over private information to hackers, redirect users to a bogus site without their knowledge, or compromise data in some other way.

What you can do better: Have a third party conduct an application test and code review to ensure that your custom Web applications are securely coded. Improve internal software development lifecycle practices by integrating security into these cycles.

Scan Quarterly for Application and System Vulnerabilities

The PCI standard requires companies to perform quarterly scans, both externally and internally, and whenever changes are made to a system. Scanning should also include wireless systems and devices. In addition, the standard specifically requires scanning for Open Web Application Security Program (OWASP) vulnerabilities. OWASP attacks try to subvert application security by injecting commands directly into databases without the company's knowledge. Currently, there is no good way to scan automatically for these vulnerabilities. The process requires assistance from an analyst, which can be prohibitively expensive when conducted in house. For this reason, some companies outsource this task to a qualified third party that can perform additional manual tests and analyze results for the company.

In our experience, most companies scan their external perimeters, but many do not scan internally. They mistakenly believe that data is secure if their perimeter is well guarded. Frequently they believe that insider threats are not an issue. In fact, insider threats may present a higher risk in terms of damage or data loss. Employees in accounting or software development, for example, can often do greater damage than an outside hacker because they know your system; they know what controls are in place and they know how to beat them. In addition, they often have the authorization to legitimately access secured data.

What you can do better: Do it.

Implement Strict SDLC Processes

A proper system development lifecycle (SDLC) process is part of a well-defined security program and involves well-defined phases: risk analysis; prototype design and building; testing; deployment; maintenance; and retirement. Ideally, security is applied at the analysis phase, and then built in and tested throughout the application's life. Many companies do not have the resources required to implement the rigid processes and detailed documentation that the PCI Data Security Standard calls for. Some companies try to cobble together enough documentation to pass PCI, but their efforts are rarely systematic or adequate.

What you can do better: Avoid ad hoc development, implement replicable processes, and document everything. If you do not have an onsite expert, at least delegate a representative to be part of the SDLC process. Then document the relevant processes to verify that the application development team performed risk analysis, set security requirements, performed requirements testing, and so on. Alternatively, outsource the task to a qualified design review service that oversees the development lifecycle to ensure that security requirements have been met. This approach not only supports compliance with PCI, but also helps you catch security defects early in the process, when corrections are less costly.

+ Improve Security Awareness and Training

It is often surprising to see how many compromises and PCI audit failures could be avoided by improving security awareness. Security awareness is specifically covered in Requirement 12 of the PCI Data Security Standard but impacts other areas within the standards as well. This is especially true for mistakes related to poor password control, improper data storage, and overly permissive use policies. “Security” is defined by three distinct control points: people, process, and technology. People are easily the weakest link and can subvert controls put into place by process and technology.

Many users and administrators don't take password control seriously. They share passwords with other users, leave them in easy-to-find places, or create passwords that can be easily guessed. Part of the problem is that many people simply do not believe that a threat exists. Stronger identity management includes ongoing security awareness programs as well as policies that ensure enforcement.

Ongoing training and security awareness programs can also help minimize the following data storage issues:

- Non-compliant storage of CVV2 data or other card data
- POS terminals that generate track data
- Potential abuse of the last four digits of a credit card number (hackers can access information online—name, address, and so on—that combined with these digits, would be enough to make a purchase)

Finally, users sometimes forget that visitors, cleaning crews, and others may be able to view data that is not intended for them. In one VeriSign engagement, the consultant went to the reception desk to introduce herself. Credit card numbers were displayed on the receptionist's computer screen, in full view of anybody who walked up to the desk. Clearly, data control decreases as the number of people with access increases. Managers must learn to restrict credit card data to those who truly need the information for legitimate business purposes.

What you can do better: Continually educate and train internal staff; develop processes that ensure adherence to security procedures and policies.

+ Monitor Systems for Intrusions and Anomalies

It's hard to make informed security management decisions if you don't have visibility into the network. Effective monitoring entails more than simply looking for known attack signatures. It also involves looking for data anomalies and variations in your normal host and network logs that could indicate a new type of attack or threat.

When performed consistently and properly, the following measures help maintain security over time and through changes:

- Intrusion detection and prevention
- Log monitoring and retention

Allow IDS Devices to Accumulate Sufficient Intelligence

Intrusion detection and prevention devices are placed next to key entrances to the network and act as a last-chance virtual safety net. They monitor network traffic, and when other safety measures (such as firewalls, anti-virus software, and access control) fail to stop suspicious traffic, they notify the organization of potential break-ins, malicious activity, or non-compliant traffic.

Companies usually use two types of IDS device in tandem. One device is signature based and works like an anti-virus solution. That is, if it doesn't know about a particular threat, that threat can potentially get through. The second type of IDS solution is anomaly based. The system learns about traffic and patterns and creates rules to understand how traffic typically looks. If something out of the ordinary occurs, it creates alerts based on its accumulated knowledge.

Many companies expect these devices to work well from the outset. This is not the case, and can lead companies to assume that all is well on the network. It takes six to twelve months for either type of solution to accumulate enough intelligence to provide useful, accurate information. In addition, an IDS provides visibility only at the network layer. You'll need other mechanisms (such as application log monitoring) to monitor potential threats at the application layer. Finally, although an intrusion detection system requires a substantial investment, it can be leveraged not only for security but also to understand traffic flow and optimize resources.

What you can do better: Place IDS devices near the assets you want to protect. Doing so helps ensure that they will detect the types of activity you are most concerned with.

What you can do better: Establish a centralized server for reviewing, correlating, and managing IDS logs.

Improve Log Monitoring and Retention

The PCI Data Security Standard requires companies to track all access to card data and maintain a record of that access. (In fact, this particular aspect of security is so important that Requirement 10 of the PCI Data Security Standard is dedicated entirely to logging.) Tracking and logging access is difficult because it involves looking at massive databases that have live card numbers in them. For each access, logs must record who accessed the data and from where, the authentication mechanism used, the date, the time, and so on. Some solutions help companies set up this process, but they can be costly. Depending on how the logs are generated and whether they're meaningful, though, companies can gain significant visibility into a particular machine.

Many companies fail PCI audits because of improper log monitoring and retention. From a logging perspective, the following issues are particularly daunting:

- **Scattered log collection.** Many companies do not point all their logs to a central location for collection and analysis. This results in piecemeal log analysis and almost always creates voids.
- **Complexity of application logging.** Operating system logs are difficult enough to collect and analyze; application logs are even more so. Many applications do not store the quality of information needed for PCI compliance or for investigating an incident. In addition, application logs are almost always in plain text; this is a problem, because they frequently store card data, leaving it vulnerable to compromise.
- **Poor monitoring and review capabilities.** Some companies collect logs, but they do not review them—often, because it is too difficult to do so. If logs are collected, normalized, and aggregated at a single point, analysis becomes easier and review occurs more frequently. Besides reviewing the logs, companies must be able to track the fact that reviews are being done and how often. Although one option is to sign off manually on a form, log solutions should allow users to mark in the log itself what has (or has not) been reviewed.

What you can do better: Centralize logs and use active correlation. Attacks often involve multiple assets. If you watch only one asset in isolation, a specific activity may not seem threatening. But if you can observe that activity directed toward more than one asset within a certain period of time, you may be able to detect an attack. Log aggregators, security information management technology, and outsourced (online) solutions all provide this capability. Centralized solutions also allow you to monitor who has access to credit card data and track the workflow of your activities.

What you can do better: Hold people accountable for monitoring logs. Log monitoring can be tedious, but someone has to do it. You can outsource some of the log collection, normalization, and correlation, but at some point, someone from the company must review the reports to determine whether there are any risks to credit card data.

What you can do better: Watch the applications. Many problems occur in application logs. Make sure that you can get to the logs easily and that they are tracking necessary access data. In addition, be sure that they do not store credit card data in clear text. These application-level controls are core requirements of the PCI Payment Applications Best Practice (PABP) framework. By either purchasing PABP-certified applications or having your applications certified, you can further ensure proper logging.

+ Segment Credit Card Networks and Control Access to Them

Experience has shown us that companies with the least segmented networks suffer the most when compromises occur. Although network segmentation is a complex, time-intensive task, companies should design and build their network so that credit card data is protected, even if another part of the network is compromised. Start by isolating credit card data in its own segment, where connections are separate from the rest of the corporate network, especially the development and testing network.

Creative Solutions: How an Internet Content Company Met Firewall Requirements Without Having a Firewall

In some cases PCI requirements can be met by addressing the spirit, rather than the letter, of a requirement. Such was the case for a leading Internet content company that engaged the VeriSign® Global Security Consulting team to analyze its system and help prove that it met PCI firewall requirements. Although the PCI Standard requires companies to install and maintain a firewall configuration, the VeriSign customer's system did not meet the classic definition of a firewall. Instead, it had multiple routers with stringent access control lists (ACLs), an intrusion detection system with proprietary software that cuts off intruders before they can do damage, a reverse proxy, 24/7 external scanning, and many other mechanisms that, in reality, protected the perimeter better than a firewall would. VeriSign worked with the customer to understand its configuration and then make the case to Visa that its systems met, and even exceeded, the underlying requirement for a secure perimeter. Visa accepted VeriSign's assessment. The company has passed PCI audits for two years using the configuration.

Note: If you intend to prove that compensating controls will meet requirements, keep in mind that interpretation is an art. Hire an expert who is deeply familiar with PCI regulations, has proven expertise in security technologies and processes, and has the experience to determine whether the compensating control mitigates the risk to a level that is equivalent to what would be obtained by meeting the PCI requirement. It should also be noted that compensating controls must be "above and beyond" what is already required by the PCI standards. Meeting other PCI requirements cannot be considered a compensating control.

Conversely, from a network availability perspective, out-of-band management and continuity capabilities should be provided for credit card systems. This set-up helps ensure business continuity should Internet-facing systems undergo a denial of service (DoS) attack. DoS attacks can be very damaging, and although companies cannot do a lot to prevent them, there are certainly ways to lessen their impact. Good router configuration management and additional bandwidth capacity are a good start. You may also want to consider secure backup servers and other technology to keep your systems available during an outage or attack.

Finally, companies should use a multi-level network authentication strategy to control access to the credit card network. First, disable network ports that could potentially connect to credit card systems in non-secure areas such as conference rooms or even employee cubicles. Second, limit the number of people who can access the credit card systems. Third, use MAC address filtering, reverse proxies, network access controls (e.g., 802.1x), and even strong authentication to allow IP connectivity to your systems. The PCI standard requires two-factor authentication for remote access. You can leverage this capability inside the network to maximize your strong authentication investment and further protect access to critical credit card data.

+ Future Considerations

The PCI standards are a living document that will continue to evolve as network and application threats become more sophisticated and new credit-card technologies emerge. As an example, current compromise trends have resulted in new PCI requirements related to application security and wireless device security. Mobile commerce security is an area that has yet to be addressed in the PCI standards.

Application Security

As discussed earlier, application vulnerabilities are already a significant issue and will only increase in focus as new applications are developed. Requirement 6.5 of the PCI Data Security Standard may herald a new battery of application-related topics. This relatively new requirement specifically addresses Web applications and has ten sub-requirements. As companies deploy new applications, the ideal course is to use only CISP-Validated Payment Applications (see URLs at the end of this paper). When developing custom applications in house, use a strict system development lifecycle (SDLC) process.

Mobile Commerce Security

Wireless devices used as payment instruments present even thornier security and compliance issues. Even so, some leading-edge companies are already experimenting with embedding credit card numbers, virtual cash, and other personal data into wireless devices. The basic idea is to embed one or more payment methods into a mobile device and use the device itself like a "virtual wallet." Instead of swiping a credit card through a POS terminal, for example, consumers could simply wave their wireless device across the terminal. Radio-frequency technology would transmit the transaction data to the terminal, which would then tender the charge and respond with an appropriate confirmation to the device. Commercial deployment of mobile payment capabilities can already be seen in Japan, South Korea, Singapore, and several European countries, such as Austria, Norway, and Spain, with trials evolving rapidly in the US market.

These early deployments have their limitations. In 2004, Japan's NTT DoCoMo launched its first wallet phone, which can store up to \$450 in virtual cash. If the phone is lost or stolen, the phone can be locked, preventing further use. However, the virtual cash cannot be replaced*. Protection from such loss, as well as security and identity management, are of paramount concern for consumers as this technology quickly matures. As recently as September 2005, Kiyoyuki Tsujimura, NTT executive vice president of Products and Services, cited security as a key stumbling block for consumer adoption**.

So far, mobile payment technology is so new that the PCI has not instituted requirements to govern it. However, it's logical to assume that any new technology will have to adhere to existing standards. At the same time, new standards will likely evolve to support the new technology. For now, the best course is to adhere to existing standards. In addition, if you're interested in deploying mobile technology, get involved in industry associations such as the Mobile Payment Forum, Mobey Forum, Near Field Communication (NFC) Forum, or Open Mobile Alliance. Doing so will give you more insight into future trends. It will also allow you to participate in and possibly influence early-stage discussions of these technologies so that you can potentially benefit from the end results.

*CBS.com, *Cell Phones & Cash*, July 22, 2004 www.cbsnews.com/stories/2004/07/22/tech/main631231.shtml

**The Sydney Morning Herald, *Big cash is being tucked into wallet phones*, September 15, 2005 <http://www.smh.com.au/news/technology/big-cash-is-being-tucked-into-wallet-phones/2005/09/14/1126377378315.html>

VeriSign is positioned in the Leaders Quadrant of the August 2007 "Magic Quadrant for MSSPs, North America, 1H07" Gartner report.

+ Glossary

Card Verification Value (CVV) – This is the information stored in the magnetic strip on the back of a credit card. If stolen, this data can be used to print new credit cards. Also called track data.

Card Verification Value 2 (CVV2) / Card Validation Code (CVC2) – This three-digit number is printed on the signature panel of a credit card and helps card-not-present merchants (mail order, online, or other merchants that transact business without seeing the physical card) verify that a customer is using a legitimate credit card. On American Express cards, this number is four digits long and appears on the front of the card. PCI prohibits the storage of this number. Called CVV2 under Visa's program, CVC2 under MasterCard's program, and Card Identification (CID), under American Express's program.

Data at rest – Data that is stored in a database or other repository as opposed to being in transit.

Track data – The data that is stored in the magnetic strip on the back of a credit card. If stolen, this data can be used to make a new card. Also called Card Verification Value (CVV).

For additional terms, please see Visa's Glossary at http://usa.visa.com/business/accepting_visa/support_center/glossary.html

or

http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_GlossaryofTerms.pdf[http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_tools_faq.html](http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_GlossaryofTerms.pdf?it=il/business/accepting_visa/ops_risk_management/cisp_tools_faq.html)|Glossary%20of%20Terms



+ For More Information

VeriSign® Security Services

For more information about VeriSign® PCI Compliance Solutions, please call 650-426-5310 or email enterprise_security@verisign.com

For more information about the VeriSign® Security Certification Program, please see <http://www.verisign.com/products-services/security-services/security-consulting/services/security-certification-program/index.html>

PCI Data Security Standard and Related Information

For more information for merchants, including the current transaction volumes/categories for each level, please see

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_merchants.html?it=il/business/accepting_visa/ops_risk_management/cisp.html|Merchants

For more information for service providers, including the current transaction volumes/categories for each level, please see

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_service_providers.html?it=il/business/accepting_visa/ops_risk_management/cisp.html|Service%20Providers

For the full text of the Data Security Standard, please download the PDF document at http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_merchants.html

To review the standards for the PCI Payment Applications Best Practices program or to view a list of CISP-Validated Payment Applications, please see

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_payment_applications.html

To review the standards for Qualified Data Security Companies, please download the PDF document at

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_payment_applications.html

Visit us at www.Verisign.com for more information.

©2007 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, the checkmark circle, and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. MasterCard is a registered trademark of MasterCard International Inc. Excel is a registered trademark of Microsoft Corporation. IBM and AS400 are registered trademarks of the IBM Corporation. All other trademarks are the properties of their respective owners. The Magic Quadrant is copyrighted August 2007 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

02-19-06