Retail

PCI compliance: First step to secure transactions

ebook

An SC Magazine publication

Sponsored by

PCI: A foundation for smart business

The PCI standard is a good security baseline for retailers, but merchants need to do security every day, reports Stephen Lawton.

Conventional wisdom states that if an IT department complies with security standards, its systems should be secure. Yet for the Payment Card Industry Data Security Standard (PCI DSS), this truism fails. Rather, compliance is more of a first step to security instead of ensuring security itself. This is not only the opinion of naysayers who question the validity of the standard, it is the opinion of the PCI Security Standards Council and security experts who enforce the standard.

In fact, professionals in the field agree that while compliance with the standard certainly is necessary, companies that do payment card transactions need good overall security policies, procedures and people in place to create a secure environment. Security does not come from compliance to a standard. Rather, compliance to various security standards comes from having a company where security is an integral part of every action the company takes, says Deven Bhatt, CISO for Wright Express Financial Services Corp., a Salt Lake City-based provider of payment processing and information management services to the U.S. commercial and government vehicle fleet industry.

When reviewing the causes of major security breaches over the past several years, virtually every case involved a company that was out of compliance in some way with the PCI DSS standard when the breach occurred, says Bob Russo, general manager of the PCI Security Standards Council (PCI SSC), the standards body for the payment card industry. In some cases, the breached company might have thought it was in compliance with the standard, but a network modification, new software or other change to the network environment that should have been tested and fixed was not, creating the opportunity for the breach.

For some companies – primarily smaller firms with a limited number of card transactions – compliance is something that they do because the five major card brands that created the standard require it. Compliance becomes a scheduled checklist task, not part of the company's overall operations policies.

What is compliance?

The PCI Security Standards Council defines the standard this way: "The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data."

Essentially, it is a set of rules that ensures the security of user data, such as credit card numbers and user-identifiable information, as well as describing the process and policies on how companies store and transfer such data. The standard itself is very prescriptive, setting down specifics on how a company that accepts payment cards must manage its networks and perform security maintenance.

The standard was developed in conjunction with five payment card brands – American Express, Visa, MasterCard, Discover Financial Services and JBC International – which founded the council. The council, which manages the standard, is not a policing organization. Each card brand maintains its own compliance program and definitions of validation levels and reserves the right to place fees on its merchants or fine those out of compliance with the standard. As a result, only merchants that accept these five card brands are required to meet the standard per the terms of the brands themselves.

"The standard is a good security baseline, but [merchants] need to do security everyday," says Russo. Instead, he says, merchants

$204

was the average data breach cost per record in 2009

– Ponemon Institute

"have to live [security]. It has to be part of their DNA."

Russo acknowledges that simply meeting the basic standard itself does not address a company's full security needs. Being complaint simply means that on a given day at a given time when the compliance examination occurred, the merchant was compliant. However, even small changes, such as replacing a router or reconfiguring a network with additional systems, can put that network out of compliance.

"That's why we're more focused on security than on compliance," he notes. If a merchant employs a set of comprehensive security protocols on a daily basis, compliance will occur as a byproduct.

Speaking at recent SC eConference and Expo in March, produced by *SC Magazine*, Bruce Rutherford, the 2010 chair of the PCI SSC and MasterCard group head, fraud management solutions, cautions that compliance itself is only a point-in-time assessment. "Compliance is only an illusion of security."

Underscoring the Council's position that compliance itself is not security, Rutherford says that security should be designed ahead for the next threat, the next attack vector, the next piece of information that a company might be exposing to a possible breach.

Source: PCI Security Standards Council

Specifically, the standard addresses 12 requirements needed for compliance. The challenge for the payment card brands is to ensure that merchants use these prescriptive requirements as part of an overall security program and not as a checklist.

But, security experts agree that simply using a checklist approach to PCI security likely will not result in a secure environment. While larger companies generally have IT staff and security experts who can install and maintain highly secure networks, many small- and mid-sized companies could be vulnerable. These firms often do not have IT or security staffs. In many small companies, the owner might be responsible for everything from sales to administration and IT to finance. In such cases, data security is often given a lower priority than making the daily sales numbers.

A term that is commonly used to describe the PCI specification is "prescriptive." Bhatt notes that the standard is very specific about what companies need to do and how to do it.

Russo agrees that the standard strives for clarity and consistency so that when companies certify their networks, they are using common terms and procedures.

For example, requirement one of the standard states: "Install and maintain a firewall configuration to protect cardholder data."

PCI Data Security Standard: High level overview

BUILD AND MAINTAIN A SECURE NETWORK
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PROTECT CARDHOLDER DATA
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

IMPLEMENT STRONG ACCESS CONTROL MEASURES
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

REGULARLY MONITOR AND TEST NETWORKS
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

MAINTAIN AN INFORMATION SECURITY POLICY
Requirement 12: Maintain a policy that addresses information security

$6.7m

was the average data breach cost in 2009

– Ponemon Institute

While such a requirement might seem straightforward and obvious, the standard goes into more than three pages of testing procedures to ensure that the requirement is met. However, the standard also makes allowances for different size companies to meet the standards in different ways. In order to be fully compliant, each of those subsections must be configured and tested. But not everyone goes through the full standard.

Virtually every router sold today, including those for consumer use, has a firewall capability built in. Buying and installing a router with a firewall is a first step, but it does not necessarily mean the requirement is met. If the unit is installed, but the default login and password are not changed, the network is hardly secure. While the specification states that defaults must be changed, someone who simply goes down the checklist and sees "Install and maintain a firewall…" might think they are secure and compliant, Bhatt says. According to the PCI DSS, that configuration is not compliant.

So what are the consequences of being out of compliance, perhaps even for just a short time? The consequence is a potential data breach. According to the Verizon Business RISK team, it's more than just an IT or security officer understanding what is on a company's network and the security status of each component. It also is necessary to know what the IT manager doesn't know about the network. For instance, are there computing assets on the network – such as a seldom-used server or storage device – that might have been left off the list the last time a network map was created? Is it possible that an unaccounted-for or rogue wireless router is connected? Are there any former employees who still have access privileges on the network? These unaccounted-for assets and components are referred to as unknown unknowns.

In the past five years, Verizon Business has investigated some 600 breaches, according to its "2009 Data Breach Investigations Report" – the most recent report available. These breaches represented more than 285 million records breached through a variety of attack scenarios. The retail sector took the brunt of the attacks, accounting for 31 percent. Financial services followed closely behind at 30 percent. No other industry sector saw more than 14 percent.

Of the 90 breaches Verizon Business investigated in 2008, approximately one half were classified as coming from an unknown source. While that percentage seems high, Verizon says that is a considerable improvement over the previous four years and 500 breaches, where some 90 percent of the breaches had at least one unknown component.

Sharing breach information

One significant challenge security experts face is the dearth of shared information about breaches. In some cases, publicly held companies don't want to discuss security breaches because the impact of the discussion could affect stock prices. In other cases, companies have corporate policies not to discuss ongoing investigations. In one recent example, the CISO of the state of Pennsylvania lost his job because he spoke publicly about a data breach without the proper authorization from state officials.

The challenge for IT and security officials is that without information on current hacking attempts, companies that have yet to be hacked might be at risk if they do not have current information on new malware or attack strategies. While some companies prefer not to release information about data security due to the possible release of privileged corporate information, other companies potentially become at risk because they won't know about additional security barriers that they might be able to put in place against these new attacks.

Wright Express's Bhatt sees cooperation and open discussion of breaches as critical to disseminating actionable information to protect against breaches. "Sharing information responsibly is always good," he says. "If you find a security problem, tell the vendor. Today's hackers are getting smarter," he says.

69%

of data breaches were discovered by third parties

– Verizon Business 2009 Data Breach Investigations Report

However, Bhatt is bothered that information about data breaches is not made public until, perhaps, the criminal's trial, if indeed a trial even occurs. International cooperation is required for laws that go after cybercriminals, and companies should be more proactive in indentifying data breaches, he stresses.

Legal requirements

While larger companies with internal IT staffs and security personnel are well educated on the PCI standard and other related security issues, many smaller companies simply are not informed about what their responsibilities are when it comes to payment cards, notes Phil Cox, principal consultant and a qualified security assessor (QSA) with SystemExperts Corp., a Sudbury, Mass.-based IT security and compliance consultancy.

Although the PCI standard was developed by a private industry organization, its requirements are starting to make their way into state laws, he says. In Nevada, for example, Senate Bill 227, which went into effect Jan. 1, states: "If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization." The law, which goes into detail about protecting personally identifiable information (PII), is the first in the nation to specify the PCI DSS, but it is not the only law about payment card security.

Other states also have laws addressing PCI data, although not identifying the PCI DSS specifically. North Carolina law states that if a company throws out even one piece of paper with PII data, it can be open to a $10,000 fine. Minnesota passed the *Plastic Card Security Act* in 2007 that says that any Level 1-3 company that is breached and is found to have been storing "prohibited" PCI data is required to reimburse banks and other organizations for costs associated with blocking and reissuing cards. This law makes violating companies vulnerable to private lawsuits. Massachusetts also has a new law implementing some of the PCI DSS regulations.

Although many states, as well as the federal government, have laws against releasing PII, the introduction of concepts derived from the PCI DSS standard is relatively new. However, companies that violate the PCI DSS, while not necessarily subject to legal consequences, can be fined by the brands they represent, Cox notes. From a risk management perspective, the fines are relatively small and could be considered part of the cost of doing business. "If [PCI security] matters that much, the fines should be higher," Cox says.

Education

Smaller companies want to do the right thing, but they need guidance, Cox says. The conundrum is that many of these companies don't know what they don't know about security or payment card information laws. Although there is a lot of information available on the web about security and PCI compliance for companies of all sizes, owners of small firms often don't know the right questions to ask and therefore do not find the information they need.

Rich Baich, a principal with Deloitte & Touche, concurs that smaller firms generally do not have the same level of education in PCI requirements as larger companies with dedicated staffs. While some administrators at small- and mid-sized businesses (SMBs) understand the concept of risk management in basic business operations, they often do not understand the principle as it impacts the cyber environment, he says.

While the level of understanding about technology issues for small companies that accept credit cards doesn't match that of Level 1 companies – those that do six million transactions a year – the compliance requirement is the same. Only the reporting requirement is different.

81%

of data breach victims were not PCI compliant

– Verizon Business 2009 Data Breach Investigations Report

Level 1 firms have strict reporting regulations, including an annual report on compliance by a QSA and a quarterly network scan by an approved scan vendor (ASV). Levels 2 and 3 merchants need only an annual self-assessment questionnaire (SAW) and the quarterly network scans. Level 4 merchants, which include the millions of small companies that do fewer than 20,000 e-commerce transactions annually or up to one million transactions annually, need the SAQ but, in some cases, might not require the annual network scan.

The responsibility for educating the smaller merchants about PCI requirements is unclear. Although all merchants that accept payment cards from the five co-founders of the PCI Council are required to meet the same requirements, training at the low end can be spotty, says Jen Mack, director of Verizon Consulting Services. Some small companies believe that if they outsource their PCI card transactions to third parties, such as PayPal, they are no longer responsible for the security of the personal information. That is not the case.

"Just because you outsource the transactions, doesn't mean you outsource the risk [or liability]," she says. "You just outsource the process."

Mack recommends that every company that outsources its payment card transactions ask their service provider to give them a copy of their PCI compliance documents on an annual basis. "You need to do your due diligence," she says.

Based on the level of credit card activity, it is possible for a merchant to be at one level with, for example, MasterCard or Visa, but at a different level for American Express. As a result, the merchant might have different reporting responsibilities to the different brands, according to American Express, which requires merchants that reach a higher level with its card meet the higher level of reporting, regardless of its level of activity with other card brands.

Visa merchant levels and validation requirements: The break down

Level / tier [1]	Merchant criteria	Validation requirements
1	Merchants processing over six million Visa transactions annually (all channels) or global merchants identified as Level 1 by any Visa region [2]	• Annual report on compliance ("ROC") by qualified security assessor ("QSA") • Quarterly network scan by approved scan vendor ("ASV") • Attestation of Compliance Form
2	Merchants processing one million to six million Visa transactions annually (all channels)	• Annual self-assessment questionnaire ("SAQ") • Quarterly network scan by ASV • Attestation of compliance form
3	Merchants processing 20,000 to one million Visa e-commerce transactions annually	• Annual SAQ • Quarterly network scan by ASV • Attestation of compliance form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to one million Visa transactions annually	• Annual SAQ recommended • Quarterly network scan by ASV if applicable • Compliance validation requirements set by acquirer

[1] Compromised entities may be escalated at regional discretion

[2] Merchant meeting Level 1 criteria in any Visa country/region that operates in more than one country/region is considered a global Level 1 merchant. Exception may apply to global merchants if no common infrastructure and if Visa data is not aggregated across borders; in such cases merchant validates according to regional levels.

91%

of all compromised records were linked to organized criminal groups

– Verizon Business 2009 Data Breach Investigations Report

While the credit card brands are ultimately responsible for enforcing compliance, they tend to migrate that day-to-day responsibility down to the acquiring banks, Mack says. The challenge banks face is that many Level 3 and 4 companies do not necessarily understand the full impact of data security. "You can't talk to a Level 4 merchant the same way you talk to a Level 1," she says.

While noting that there are considerable resources on the PCI Council's website for smaller companies, Mack acknowledges that not all companies are aware of the resources at their disposal.

Deloitte's Baich agrees, saying that education is one of the most important services his firm provides to companies that are preparing for audits.

As part of its analysis of past security breaches, Wade Baker, director of Verizon Risk Intelligence and co-author of the breach report, notes that commonalities in security weaknesses are cropping up that should be part of every company's internal testing. He and Mack cited three areas in particular where merchants can do a better job of protecting themselves from data breaches: spending more time analyzing network and server log files, protecting themselves against malware attacks in general and SQL injections in particular, and protection against attacks from cloud computing applications.

In virtually every case investigated by Verizon, indications that a breach occurred were found in log files, Baker notes. While companies collect log files from a variety of devices, corporate security personnel do not tend to read the files on a daily basis. Log files get even lower priority in small companies without IT departments or personnel, where the company owner might not understand what is in the log file or even how to access the files.

While log files alone will not protect a company from an attack – log files represent what has already happened rather than showing what might happen in the future – analyzing log files on a daily basis will sharply reduce the amount of time an attack is active and indicate potential attacks that have been prevented. According to Verizon's 2009 data breach report, the time span from compromise to discovery was measured in months in nearly half of all breaches and weeks in one quarter of the attacks. By contrast, more than three-quarter of the breaches, measuring from the point of entry to data being compromised, was measured in days. That means the attackers had multiple weeks to months to conduct their activities before the breaches were identified and shut down.

From a malware perspective, two issues caught the eye of Verizon forensics investigators: In some 82 percent of all of the breached records, or roughly 234 million records, the most effective type of malware was the "capture and store variety." Additionally, some 85 percent of the records were harvested by custom-created malware.

Baker says that some malware creators are starting to develop customized malware designed to defeat a specific company's infrastructure. Because anti-virus and anti-malware software is becoming very good at recognizing specific malware patterns, he notes, new versions of the attack software is being developed so that the patterns are not identified. Each time the malware creator finds a potentially lucrative target, the software is modified again so that it won't get caught by regular anti-virus or anti-malware scans.

When successfully planted, these modified malware programs tend to be more effective than traditional malware programs because they are harder to identify and therefore have the potential to last longer in a corporate system.

Stopping malware

Another important method of stopping malware requires companies to spend more time building security into home-grown and commercial applications, particularly those susceptible to SQL injections, Mack says. Many web-based applications are designed

22%

of breaches involved privilege misuse

– Verizon Business 2009 Data Breach Investigations Report

first and foremost with usability as the top priority rather than security, she says. Additionally, the goal of many companies is to get new applications out to users quickly rather than putting them through rigorous security tests first. As a result, she notes, many applications, both custom-built and commercial, have security holes that are not evident until they are compromised.

A better approach would involve more intense testing of home-grown applications, especially web-facing applications that require customers or partners to enter data into a corporate SQL database, Mack says.

For commercial applications, patches should be applied as soon as they become available, Baker adds. Although only a handful of breaches in 2008 were due to unpatched applications, all of the patches had been available for more than six months, and most for more than a year. All of those breaches could have been stopped, he says.

In addition to SQL injections, many networks are vulnerable to other software holes, says Sheldon Malm, senior director of security strategies at Boston-based Rapid7, a vendor of vulnerability management products. AJAX, JavaScript and Flash also pose security risks and are often the initial point of entry for a multistage network attack, he says.

As cloud computing becomes a standard in corporate and, by extension, PCI networks, companies are at greater risk to web-based breaches, he notes. Applications written in C or Java have a lower threshold of security breaches than those that use web applications, like Flash, he notes.

"The real business driver for web applications is to be responsive to the market," Malm says. "However, there is a real disconnect for companies to trade security for today's business base."

Segregating the networks

The best way to protect a payment card network is to isolate it completely from the corporate network, says Bradley Schaufenbuel, senior vice president and chief information security and privacy officer at Midwest Banc Holdings, based in Melrose Park, Ill. By segregating the PCI network from the corporate network, the IT manager can employ appropriate security protocols to each network and reduce overall network security expenses.

If PCI data goes over a corporate network, then all PCI compliance-testing measures must be done on the corporate network, a process that could increase network management costs significantly, particularly for a global company.

However, by segregating the networks, the company can ensure that PCI data is kept out of the hands of employees who have no reason to access that data, he notes. By isolating the payment card infrastructure from the corporate network, the IT manager can keep network compliance testing to a minimum and reduce the complexity of the network infrastructure. Each time a PCI network is modified, be it by adding a new server or desktop system or by installing new networking devices, the entire process must be done based on a defined change-control process.

One method of segregating PCI data for a small company is to use a dedicated payment card device that is linked via phone lines to the processing center. By taking all PCI data off the corporate network, Schaufenbuel says, companies can keep employees without need-to-know access from any cardholder data. Currently, many companies do not understand who requires need-to-know access, so many firms make that data available to too many employees.

Schaufenbuel also cautions merchants to ensure that their wireless networks are locked down. While securing wireless networks is already part of the specification, he says some companies that do not currently use wireless as part of their infrastructure might not realize they have accessible networks. Among the ways companies that have wired networks might accidentally open up their networks to rogue wireless connections is through an un-

38%

of breaches used malware to attack

– Verizon Business 2009 Data Breach Investigations Report

authorized router that is added to the network by an employee who wants wireless access for a laptop, wireless routers with open transmitters being used on wired networks, a wireless router that is surreptitiously connected to a wired network, or a laptop connected to a network via an Ethernet cable that also has a wireless network interface card installed and powered up.

In many instances, Schaufenbuel says, the wireless device creates an unintentional vulnerability. "It's not necessarily a case of someone trying to steal data."

Baker notes that Verizon identified a "definite trend" to fewer wireless breaches in recent years. He attributes the trend to better compliance across the board by merchants and better testing by QSAs.

Five years ago, Mack says, many unknown wireless devices were found on corporate networks, along with fake point-of-sale systems. It is the responsibility of the QSAs to find these devices during the course of their certification inspection of the merchant.

"PCI DSS is driving a lot of good changes," Mack says. "There are no fanfares for the successes."

As noted, education is the key to building a secure and compliant network, and there are considerable resources that address PCI DSS compliance on the web – assuming that merchants know the right questions to ask and where to find the answers.

The PCI Council has an extensive library of white papers, questionnaires and FAQs designed to assist companies with questions about PCI compliance. Hardware and software vendors also have reams of documents touting best practices for PCI compliance, with titles ranging from "PCI Wireless Compliance Demystified: Best Practices for Retail" from Motorola to "Best Practices in Starting Your PCI Data Security Standard Compliance Initiatives" from LogLogic.

Some vendors offer free software downloads of applications, such as one designed to test a network for potential security holes. The major card brands also offer libraries of data for merchants of all sizes that discuss ways to make networks secure and ensure compliance.

Again, the question comes back to education. Deloitte's Baich says merchants need to address security from a risk-based position. "You have to understand the criteria for security," he says, emphasizing that checkbox compliance does not result in a secure environment.

"Approach PCI compliance from a risk-based standpoint," he says. "Be prepared to do additional actions to reduce the risk of doing business over the internet. Finally, remember that PCI is focused on industries that are also subject to state legislations for protecting personally identifiable information."

Baich recommends that smaller merchants not only go to the traditional sources of information, such as the PCI Council and vendors, but also sit down with their bankers, go to Chamber of Commerce meetings, and talk to the Small Business Administration and other business-oriented organization to obtain information that might assist them in being compliant. ■

Stephen Lawton is a freelance writer and consultant with more than 30 years of experience covering technology issues. He currently is president of AFAB Media Services and is the former editor-in-chief of MicroTimes, Digital News & Review, SunWorld *and* NetscapeWorld. *He can be reached at sl@afab.com.*

64%

of breaches resulted from hacking

– Verizon Business 2009 Data Breach Investigations Report

Sponsor

LogRhythm

LogRhythm provides enterprise-class log management and SIEM 2.0 solutions that empower organizations to comply with regulations, secure their networks and optimize IT operations. LogRhythm's rapidly growing customer base includes Fortune 500 corporations and mid-sized enterprises spanning a variety of industries, including retail, financial services, utilities, health care and higher education, as well as military and civilian government agencies and MSSPs.
For more information, visit www.logrhythm.com.

ArcSight

ArcSight is a leading global provider of security and compliance management solutions that protect businesses and government agencies. ArcSight identifies, assesses and mitigates both internal and external cyberthreats and risks across the organization for activities associated with critical assets and processes. With the market-leading ArcSight SIEM platform, organizations can proactively safeguard their assets, comply with corporate and regulatory policy, and control the risks associated with cybertheft, cyberfraud, cyberwarfare and cyberespionage.
For more information, visit www.arcsight.com.

Tripwire

Tripwire is the leading global provider of IT security and compliance automation solutions that help businesses and government agencies take control of their entire IT infrastructure. Over 7,000 customers in more than 86 countries rely on Tripwire's integrated solutions. Tripwire VIA™, the comprehensive suite of industry-leading file integrity, policy compliance and log and event management solutions, is the way organizations proactively prove continuous compliance, mitigate risk and achieve operational control through Visibility, Intelligence and Automation. Learn more at tripwire.com.
For more information, visit www.tripwire.com.

Masthead

EDITORIAL
EDITOR-IN-CHIEF Illena Armstrong
illena.armstrong@haymarketmedia.com
DEPUTY EDITOR Dan Kaplan
dan.kaplan@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com
DESIGN AND PRODUCTION
ART DIRECTOR Brian Jackson
brian.jackson@haymarketmedia.com
SENIOR PRODUCTION/DIGITAL CONTROLLER
Krassi Varbanov
krassi.varbanov@haymarketmedia.com

U.S. SALES
ASSOCIATE PUBLISHER, VP OF SALES Gill Torren
(646) 638-6008 *gill.torren@haymarketmedia.com*
EASTERN REGION SALES MANAGER Mike Shemesh
(646) 638-6016 *mike.shemesh@haymarketmedia.com*
WESTERN REGION SALES MANAGER Matthew Allington
(415) 346-6460 *matthew.allington@haymarketmedia.com*
NATIONAL INSIDE SALES EXECUTIVE Brittany Thompson
(646) 638-6152 *brittany.thompson@haymarketmedia.com*

Achieving PCI Compliance: What You Need to Know

The collection, management, and analysis of log data are integral to meeting the Payment Card Industry (PCI) Data Security Standard (DSS). LogRhythm enables organizations to meet over 15 specific PCI-DSS requirements throughout Sections 1, 5, 10 & 11 of PCI DSS and automates many of the tasks associated with meeting compliance.

Requirements Include:

- Review logs for all system components at least daily
- Protect stored cardholder data
- Track and monitor all access to network resources and cardholder data
- Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis

LogRhythm Delivers:

- Automated collection, review and secure archiving of all log data
- Extensive data visualization with meaningful, easy-to-use analytics tools
- Real-time alerting and detailed reporting on suspicious user behavior
- Compliance automation for PCI DSS

"Powerful product with plenty of easy-to-use features, this one is our Best Buy."

SC MAGAZINE BEST BUY

READER TRUST AWARD
"Best SIEM"
INNOVATOR OF THE YEAR

OVERALL RATING

LogRhythm®
COMPLY. SECURE. OPTIMIZE.

www.logrhythm.com

Learn more about achieving PCI Compliance and how LogRhythm can help!

Find the cybercriminal.

(Never mind. ArcSight Logger already did.)

Stop cybercriminals, enforce compliance and protect your company's data with ArcSight Logger.

ArcSight™

Learn more at www.arcsight.com/logger.

THINK SECURITY. AUTOMATE COMPLIANCE. TAKE CONTROL.

tripwire™
TAKE CONTROL.

Every organization needs to comply with certain standards, whether they're internal policies, industry requirements or legal regulations. In the quest for proving compliance and achieving audit goals, organizations can easily get bogged down in details and lose sight of the ultimate goal of compliance—to protect sensitive data and secure their critical infrastructure.

Common Challenges

- Compliant organizations are still experiencing breaches
- Constant reactive stance to audit demands
- Multiple regulations to comply with (e.g. PCI, SOX, HIPAA, NERC, etc.)
- Achieving compliance is a burden on resources

Meeting compliance to satisfy audit demands creates operational inefficiencies, reduces productivity and takes away resources needed to perform planned work and strategic initiatives.

What's more, sensitive data is still being compromised because compliance is not viewed as a strategic component to improving the overall security posture.

tripwire ENTERPRISE

tripwire LOG CENTER

How the Tripwire VIA Suite Can Help

- Simplify compliance
- Reduce audit burden
- Achieve proactive, continuous compliance
- Consolidate multiple compliance controls
- Reduce costs and inefficiencies
- Ensure a more secure environment

Tripwire® VIA™ solutions enable you to achieve continuous compliance while ensuring a more secure environment. Unlike tools that simply collect massive amounts of change or event data without any context, Tripwire VIA solutions transform data into knowledge to help you proactively act on the changes and events that move your organization out of compliance. Tripwire alerts you when changes and events might put your IT environment at risk of compromise, and provides the controls necessary to reduce costs and secure your environment.