



Business case for establishing a security management program for merchants affected by PCI

A solution note on the benefits of QRadar when used to deliver PCI-driven security control objectives

Is “good enough” acceptable in the face of looming PCI deadlines?

Credit card merchants are scrambling to meet the requirements of the Payment Card Industry’s (PCI) Data Security Standard (DSS) prior to upcoming hard deadlines imposed by Visa. PCI-DSS is a set of data and networking security standards for merchants that process credit card transactions for the purpose of protecting sensitive credit card holder information.

Deadlines set by Visa dictate a successful audit, verifying compliance of PCI-DSS, by September 30 for tier 1 merchants (more than 6 million transactions annually) and by December 31 for tier 2 merchants (1-6 million transactions annually). Other credit card companies, including Mastercard, American Express and Discover, recognize PCI-DSS as the de-facto information security standard for merchant companies and, although they have not set hard deadlines for compliance, expect their merchants to implement a PCI-enabled security program. Similarly, smaller merchants are expected to show compliance with PCI-DSS through a self assessment report and can also be held accountable for non-compliance. As organizations work diligently to shore up their IT security program to meet the looming deadline or meet the PCI control objectives, it is important to make sure that the investments made to comply provide long term value and are not just “good enough” to pass a short term audit. One area where strategic planning is tantamount and where many organizations are not sufficiently prepared is the section of PCI titled “Regularly Monitor and Test Networks”.

There is no single bullet to meeting all of the PCI requirements. The standard is a composite of six relatively broad control objectives for network security that includes detailed guidelines around how an organization should deliver network security across technology, people, and process. The best defense for PCI is a good offense – a well thought out and repeatable security process. It is beyond the scope of this discussion to cover all areas of concern for meeting PCI compliance. However, we will focus on presenting a business case for implementing a security program and important considerations when selecting a centralized security management solution to meet specific monitoring, auditing and reporting requirements of the standard.

Making a business case for an information security program

There are many compelling reasons for credit card merchants to institute a comprehensive information security program including minimizing risk of penalties for non-compliance, an improved ability to detect and mitigate data theft which will result in decreased litigation, decreased expense and an improved corporate image.

For Merchants under the scrutiny of the standard there is a risk of real penalties for failing to meet the PCI security objectives. In addition, some merchants can incur a significant increase in transaction fees from credit card companies when the organization is non-compliant. Specific penalties for non-compliance include:

Fines

Organizations that do not successfully comply with PCI-DSS can face significant fines that vary based on the merchant's level and the depth of non-compliance. Visa acknowledged \$4.6M in fines in 2006 which shows that penalties are being levied for non-compliance by the credit card companies. Fines are not just limited to just those imposed by credit card companies. For example ChoicePoint was fined over \$10M by the FTC for a major breach.

Increased transaction fees

It is this penalty area that can be quite costly for merchants. Suppose a tier 2 merchant performs 2 million transactions per year with an average transaction of \$500 (\$1B collected annually). If the credit card company's transaction fee per \$100 is \$.25 for PCI-compliant merchants and \$.30 for non-compliant merchants, the difference in transaction fees would be \$2.5M versus \$3M (\$.5M more expensive for non-compliant merchants).

Risk of being barred from performing transactions

Any organizations that fail to comply could inevitably be dropped from the roster of merchants certified to process credit card transactions. This would have untold consequences to the merchant.

In addition, merchants that have a breach of customer information will incur significant expense recovering from the breach including:

Post breach clean up

Many companies have a business practice to notify customers after any breach of confidential information, and in some states, including California, it is mandated by law. In addition, some merchant companies will provide additional services to victims whose confidential information was compromised including credit monitoring services. As an example, a merchant faced with notifying 50,000 customers of a breach could potentially incur a post-breach clean up expense of \$15M if we assume a \$300/customer expense (\$100 processing and mailing notification + \$200 fee for services).

Litigation

It is difficult to measure the potential expense of litigation, but it can be considerable.

Diminished reputation

It is difficult to measure what long term harm is caused by the diminished reputation of a merchant when a breach occurs. Many companies have been able to make it through a breach without a significant impact to the business. This is most likely due to the fact that many of these breaches impacted only a small percentage of all confidential information managed by the company. A company's ability to weather the storm of a breach is greatly improved when consumers can be shown that a security program is in place and that, although some weakness existed that resulted in a breach, the company can document the breach and ensure consumers that the majority of consumer information is protected. There is a big risk for all merchants to suffer irreparable damage to their reputation and business in general if a significant breach occurs that touches all customers of the business.

Other solutions miss the mark for meeting PCI information security

Many organizations under the scrutiny of PCI have looked to log management and security information and event management (SIEM) solutions to provide PCI mandated network and security visibility. Although these solutions are an important facet of a repeatable security process, it is important to consider if they can hold up under some of the more complex monitoring requirements specified by PCI or to other security processes that are just common sense. In contrast to other less prescriptive security standards, PCI-DSS dictates specific physical safeguards in the areas of:

- Control of trusted and risky protocols (Requirement 1.1.6/1.1.7)
- Control of traffic from “un-trusted” or “public” networks (Requirement 1.2/1.3/1.4)
- Use of default vendor passwords (Requirement 2.2.1)
- Use of encryption technologies (Requirement section 4)
- Use of vulnerability and anti-virus solutions (Requirement section 5)
- Use of unique user IDs and passwords (Requirement section 8)

A bare-bones approach to meeting PCI will include implementation of various physical safeguards including firewalls, network encryption, vulnerability scanners, and authentication systems. A long term strategic consideration must be how does an organization detect if these systems are mis-configured or ineffective? Although a traditional log management and SIEM solution might be capable of answering this question some of the time, there are many circumstances where they will fall short because of a lack of visibility into what applications are traversing the network and how they are being used.

Many log management and SIEM solutions are only capable of correlating network and security events. Although completely relevant to the security process, a more comprehensive network security management approach will integrate additional information that takes a deeper look at application and protocol use. This information is provided in many networking devices in the form of “flow data” which provides a summary of protocol and port usage on the network. This class of information is necessary to meet some of the more detailed requirements of PCI to monitor and report on network and application activity on servers that maintains credit card holder information. Incremental value can also be gained by incorporating valuable identity information provided by directory systems like LDAP or active directory.

A strategic network security management solution will leverage all of the aforementioned information sources to build a network, application and user identity context so that current user activity can be gauged against past behavior. This results in much better visibility into the security posture of the network.

QRadar benefits for meeting PCI security control objectives

QRadar network security management platform, from Q1 Labs, takes an innovative approach to meeting specific PCI security control objectives. Recognizing that discrete analysis of security events is not enough to properly meet all of the requirements of PCI; QRadar was developed to provide an integrated approach for network security that combines the use of traditionally silo'd information to assist meeting complex security management tasks specified by the PCI standard. Specific information silos that have been combined in QRadar include:

Network events:

Includes events generated from networked resources including switches, routers, servers and desktops.

Security events:

Includes events generated from security devices like firewalls, VPNs, intrusion detection/prevention, anti-virus, identity management, and vulnerability scanners

Host and application logs:

Includes log data from industry leading host operating systems (Microsoft Windows, UNIX, and Linux) and from critical business applications (authentication, database, mail and web)

Network and application flow data:

Includes flow data generated by networking devices from vendors including Cisco, Juniper, Foundry, HP, and Extreme. Information provides the ability to build a context of network and protocol activity.

User and asset identity information:

Includes information from commonly used directories including Active Directory and LDAP.

Many traditional SIEM solutions will only incorporate a subset of this information and typically lack the ability to leverage the valuable point of perspective that is provided by flow data, user and asset identity information. We cover many examples below where a combination of all of the aforementioned data

sources is required to detect threats that will be missed by other solutions because they lack an integrated awareness of network, security, application, and user identity.

QRadar's more advanced integrated network security management capability adds strategic value to a PCI initiative including:

- Increased protocol and application visibility providing detection of inappropriate use of trusted and risky protocols
- Increased awareness of the what systems are accessing sensitive information enabling detection of rogue use from "untrusted" or public networks
- Deep inspection of protocols to detect use of default administrative passwords and unencrypted data protocols
- Improved correlation across the network, systems, and applications to detect more complex integrated threats
- Improved use of existing user and system naming conventions enabling tighter controls

A more detailed list of areas of the PCI standard that will benefit from a QRadar deployment can be found in appendix A of this document.

Summary

As credit card merchants struggle to implement controls required by PCI-DSS it is important to consider solutions that have long term value and not just provide a quick fix for an upcoming audit. There are many good reasons to implement an information security program; meeting PCI security control objectives is just one of many. We've discussed multiple PCI-specific regulations that may have a temporary fix that is "good enough" to pass an upcoming audit. However, these solutions may not provide an effective solution for existing and future requirements of PCI. It is important, and in many cases required by PCI, to implement a security management solution that can provide log management, monitoring, reporting, correlation, and auditing capabilities to verify the effectiveness of the physical safeguards in place. An important consideration in selecting a network security management solution, as part of an over PCI strategy, is to make sure that it provides this visibility across the network, application and identity layers to meet the more stringent PCI requirements of controlling access to sensitive credit card information.

Appendix A – Specific areas of PCI supported by QRadar

PCI Area	#	Requirements	QRadar Enables
Build and Maintain a Secure Network	1.	Install and maintain a firewall configuration to protect data	1.1.6 & 1.1.7 <u>Justify/document all protocols & risky protocols</u> Monitor and report on all protocols Alerting & reporting of protocol offenses Discover mis-configured firewalls allowing inappropriate traffic
			1.2 <u>Deny traffic from “untrusted” networks</u> Detailed reporting of firewall logs Discover mis-configured firewall rules allowing unauthorized traffic
			1.3 & 1.4 <u>Restrict public access to/from systems storing cardholder data</u> Definable groups to isolate inappropriate system communications Easy to use rules engine to define specific system use policies Detect outbound internet traffic from internal systems Validate DMZ firewall rules
			2.2.1 <u>Implement only one primary function per server</u> Detect inappropriate services on specific servers
		Do not use vendor-supplied defaults for system passwords and other security parameters	2.3 <u>Encrypt all non-console administrative access</u> Detect non-encrypted user names and passwords
Protect Cardholder Data	3.	Protect stored cardholder data	3.x <u>Protect Stored Data</u> Alert and notify of any suspicious attempts to sensitive data
			4.x <u>Encrypt sensitive data during transmission</u> Detect unencrypted data through the use of flow data Detect unencrypted transfer protocols like ftp, instant message, Peer-to-peer, & mail Report on logs from encryption technologies such as SNMP V3

Maintain a Vulnerability Management Program	5.	Use and regularly update anti-virus software	5.x	<u>Use and regular update anti-virus software</u>
				Automatic correlation of AV data with other logs and network information Reporting and real-time analysis of anti-virus logs
	6.	Develop and maintain secure systems and applications	6.x	<u>Develop and maintain security systems and applications</u>
				Log Management, SIEM and behavior analysis critical to any comprehensive security management program Real-time passive profiling augments AV data which is typically not kept up to date. Leveraging asset profiles and behavior analysis detect threats not covered by AV signatures
Implement Strong Access Control Measures	7.	Restrict access to data by business need-to-know	7.x	<u>Restrict access to cardholder data</u>
				Complete auditing and alerting on access, configuration change and data change on systems containing credit card data Detection of all successful and failed login attempts Default PCI policies for alerting on abnormal login behavior
	8.	Assign a unique ID to each person with computer access	8.x	<u>Assign a user ID to each person with computer access</u>
				Integration of log and flow data with existing user identity information provides detailed audits of user activity Point-in-time snapshot of user profiles provide unique ability to accurately report the user of reported activity
	9.	Restrict physical access to cardholder data	9.x	Not Applicable
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data	10.x	<u>Monitor access to network resources and cardholder data</u>
				Effective and secure (Q4) log management Out-of-the-box as well as customizable PCI specific monitoring and alerting rules Deep L7 forensic inspection of monitoring and auditing data
	11.	Regularly test security systems and processes	11.x	<u>Regularly test security systems and processes</u> QRadar provides un-paralleled 24x7 monitoring and alerting capabilities
Maintain an Information	12.	Maintain a policy that addresses	12.x	<u>Maintain a policy that address information security</u> Combined Log Management, SIEM, and behavior

Security Policy		information security		analysis is critical to any information security program
------------------------	--	----------------------	--	--