Clear Skies SECURITY
Intelligence. Secured.

RISKWATCH®

A New Approach to Managing PCI Compliance

Leveraging the Power of Assessments and other Efficiencies to Reduce Costs

By:
Rick Belisle, COO Clear Skies Security, LLC
Howard Glavin, VP Professional Services, RiskWatch

January 2009

Summary

In the past, security controls were typically one of the first areas a business would consider cutting back when budgets were tight. In today's business environment, regulatory demands such as Payment Card Industry (PCI) compliance, as well as other regulations calling for protection of privacy related information makes investment in security an on-going budget requirement.

This whitepaper will discuss a new process for achieving PCI compliance. This process provides companies the opportunity to leverage the results from the technical and risk management assessments, to better and more efficiently manage the compliance effort and to achieve maximum Return on Investment (ROI).

Summary Issues

Understanding Risk

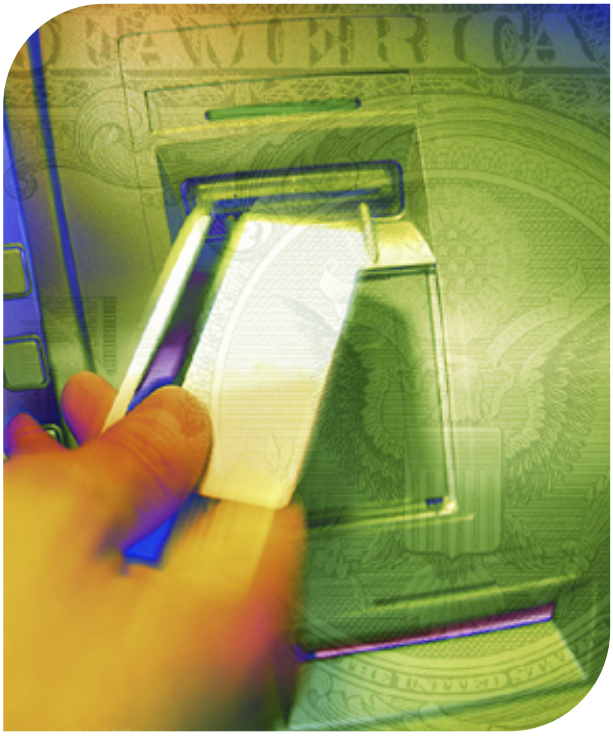
Many companies view the technical testing during these compliance assessments as another "check box" that needs to be marked off. In reality, these assessments are vital to understanding the overall risks that might impact the business. This "check box" mentality generally leads to increased costs for compliance and will not achieve the results required to protect the data; and could possibly expose the business to unreasonable risk. The technical testing should be viewed as additional insight into your business security risks, and not just as a necessary evil for compliance. Failing to use the assessment results for anything but a compliance check-box significantly reduces its value to the organization.

Reduce Scope

Compliance assessments are challenging enough to achieve without having to revamp the operations of the entire company. By fully understanding how PCI data is used throughout the business, the compliance scope can be reduced to minimize the impact to overall business operations. This scope reduction can only be achieved by thoroughly understanding how the data is used and where it is needed. Understanding and controlling data flow will allow you to isolate the PCI data to a very small portion of the environment. This results in a reduction in both time and cost to meet the compliance requirements.

Remove Complexity

The more complexity that can be removed from daily processes, the simpler the solution is to meet regulatory controls, and the sooner compliance can be achieved. From a financial perspective, these simple process improvements will allow compliance to be achieved at a fraction of the cost.



Background

When budgets are tight, everyone looks for ways to reduce operating costs. Typically these cost reductions are ranked first by those items that generate profit, and then those items that are nice to have but may not contribute directly to the bottom line. Depending on the organization's perspective, compliance can be placed in either of these buckets. These cost reduction decisions, however, need to be analyzed from both an immediate financial perspective as well as from an overall compliance perspective.

The PCI Security Standards Council (SSC) has stressed that 90% or more of losses today occur from within a company either through application weaknesses or through the actions of trusted third parties that have permission to access the data as part of their service. Most companies assume incorrectly that the losses occur to external sources hacking into the systems and stealing data. To prevent both internal and external losses, a company must have a balanced approach leveraging internal and external technical assessments to ensure the exposures are identified early on, along with a process to safeguard critical data to protect against those who have approved access.

The goal of this whitepaper is to summarize some key issues that will help any organization achieve or maintain PCI compliance in the most direct fashion possible to minimize overall operating costs, reduce compliance cost, and most importantly, reduce risk to the business.

Understanding the Issues

PCI compliance can be a daunting task with requirements frequently filled with many grey areas left to the interpretation of the company, the assessors, and the regulators. The best way to achieve compliance without expending unnecessary effort and cost is to ensure you understand the underlying intent of the compliance criteria. Armed with this knowledge you can make informed decisions on how your company can best achieve the compliance requirements. Most organizations try to start by reviewing the compliance requirements and determine how their current processes meet these requirements. To further add complexity to this approach they look at each requirement as a standalone activity and work toward meeting each implicitly. Our recommendation, however, is to start with a full understanding of where the compliance data is stored, and how it is used by all areas of the business. Understanding the compliance standards along with the knowledge of where the data is, or where data could be, will greatly simplify the process.

Understanding Data Flows

Most organizations automatically assume they "know" where their compliance data is stored and how it is processed. To do this properly though, a full logical and physical data flow analysis must be conducted. This is not a network diagram nor is it an application flow chart. A physical and logical data flow depicts exactly how the business uses the network, applications, databases, and any output of these systems in normal operations. It also shows how a single piece of data traverses through these components and where it finally resides, along with where it could reside due to errors or flaws in the applications, databases, and networks in that path. This data flow covers data in all forms and formats including but not limited to:

- Magnetic media
- Paper media
- Logs
- Reports
- Error recordings and data dumps

A physical and logical data flow depicts exactly how a single piece of data traverses through the networks, applications, and databases to show where it finally resides, along with where it could reside due to errors or flaws in the process.

To achieve this data flow, it is recommended that you conduct a facilitated meeting by an unbiased third party that is familiar with this activity. The meeting facilitator will help ensure that all potential areas for data processing use and storage are covered in appropriate detail and the business units make no incorrect assumptions. This meeting is recommended to have at least the following stakeholders attend:

- Each vertical business unit
- Compliance
- Physical Security
- Network/Infrastructure
- Operations
- Third Party Service Providers (managing data processing systems or networks)
- Application development and maintenance
- Databases development and maintenance
- Legal
- Finance
- IT Security

The goal of this meeting is to document all the areas where regulated data could be located as part of normal business operations. This information should then be depicted as a logical data flow diagram, which can be used as a reference for the remainder of the decisions surrounding compliance.

Understanding the Assessment Process

Armed with the data flow diagram, the next step is a gap-assessment, or Initial Report on Compliance (IRoC) for PCI. As part of the overall assessment process, technical testing also needs to be conducted and will minimally include: 1) annual internal and external Penetration Testing; 2) Application Assessments of Internet facing or public facing applications; and 3) scanning of the Internet facing IP addresses and internal network where the data is known to reside or could reside.

When conducting these assessments it is imperative to ensure that all of the technical testing activity has a constant feedback loop into the entire compliance process. All too often we see the assessment work conducted in an isolated fashion by the technical security teams and the only information the business side wants to know is that the test is done and issues were remediated. This view towards the assessment process does not take advantage of the value that technical testing results may have to business managers and needs to be reconsidered if successful compliance is to be achieved in the most cost efficient manner. The data derived from these assessments will be critical to understanding risk and reducing the scope of the compliance effort.

A New Approach to Compliance

By taking a slightly different approach to your compliance process, it is possible to achieve compliance and generate a return on the investment made in becoming compliant. The following three steps will help any business achieve compliance in the most cost effective way:

1. Understand your business risks - leveraging the power of assessments
2. Reduce the scope for compliance activities wherever possible
3. Remove complexity from your business processes

Understanding Your Risk

Understanding risk and risk management is not a difficult concept to grasp, but it is difficult to achieve if it is only driven by individual business units. Risk covers all areas of the business and therefore needs to be owned by the business, not the technology or compliance departments. When organizations try to assign ownership of risk to these departments it typically falters because they inevitably end up creating a series of invalid assumptions because they are not the true owners of the underlying business processes. Rather, each step of risk measurement must have a firm base in the business and must be applied consistently across the company. This is going to require input from senior management, middle management, line managers, finance, and the general worker population to develop an initial risk profile.

Historically, risk has been defined as “Threat x Vulnerability = Risk”. This is partially correct but it is not sufficiently detailed to allow for the correct

measurement of risk. To fully define risk you need to consider and measure (at a minimum):

1. Vulnerabilities
2. Frequency of exploit
3. Ease of exploit
4. Types of threats
5. Value of the asset(s)
6. Full valuation of the business
7. Complexity of the assets
8. Complexity of the business process
9. Mitigation process
10. Acceptable Risk
11. Impact of meeting compliance
12. Potential issues for non compliance

From the non-technical perspective, unless you are an expert in risk calculation and risk management, this process is best left to the use of a tool like RiskWatch PCI for the calculation of risk. Use of automated tools like this allow you to concentrate on the solutions to reduce risk that will move you towards meeting your compliance goal, and generate increased profitability of the business as a result. This compliance activity can and will lead to a ROI if this process is done properly.

One of the many ways to reduce the cost of the compliance effort is to try to leverage existing enterprise security assessments to meet your compliance needs.

Leveraging the Power of Assessments

From purely a technical perspective, the top three (3) aspects above should be derived from good security assessments. The main goal of these assessments is to identify vulnerabilities that are present throughout the environment, which could be used to gain access to PCI related systems or data. The scope of these assessments is therefore not limited to just PCI systems, and the resulting findings need to be utilized as critical data points in the remainder of this process.

One of the many ways to reduce the cost of the compliance effort is to try to leverage existing enterprise security assessments to meet your compliance needs. As mentioned above, these assessments are not limited to PCI systems, and there is no reason to complete security assessments just for compliance purposes. Rather these assessments should be performed against the larger enterprise systems as part of a regular risk assessment process. This will help reduce risks on a regular basis, and more importantly ensure all of the systems are already compliant when the necessary annual compliance testing is required. One of the biggest issues we see when customers tie their assessments to the PCI testing process is that most of them will have systems that fail the technical assessment the first time through. This creates a situation where other business processes are put on hold to have the systems remediated so they can be re-tested. This process increases the cost of the entire compliance process, and reduces the efficiencies that a regular assessment process would provide the organization.

In addition to identifying the vulnerabilities, a good assessor should also help identify the ease of exploitation of each vulnerability identified. This risk factor will examine the likelihood of a successful attack based on availability of exploit code, criticality of data exposed, as well as other compensating controls on the network. Given that the rest of this process relies heavily on the data gathered from these assessments, it is critical to work with security assessment companies that do not rely solely on automated tools, but are also capable of providing the details necessary to assist

you with measuring your true risk. Again, this should not be viewed as a technical exercise to "check the box", but rather as an essential control point that is vital to getting the data necessary to make informed business decisions that will drive your compliance goals. If done properly, the data collected during the assessment process will provide you with the data points needed to reduce scope and complexity of the compliance process.

Reduce Scope for Compliance

To reduce scope you must first understand what needs to be protected and what protection mechanisms are currently lacking, which can now be derived from the risk measurements you conducted in the previous step. For compliance areas like PCI, controlling scope is the key to rapid success, which also results in a reduction in cost and hence a higher ROI.

Using the data flow and risk analysis information, you can now reduce some of your scope by determining which pieces of protected data can be converted to a generic reference identifier. A generic reference identifier is simply a unique mapping of one piece of data to another, essentially obfuscating the original protected data. By using this generic reference identifier in place of the protected data, you can continue many of the normal business operations you may be using without having to conduct extensive compliance testing as long as the process of how to map the identifier back to the protected data is protected at the same level as the original data. For example, if one area of finance needs to run reports that aggregate credit card numbers, rather than using the actual credit cards numbers, the reports can be run using the reference identifier in its place. If the actual credit card numbers were used then the PCI assessment scope would include all of those finance systems that utilize that report, but if just the reference identifier is used then those systems can be removed from the scope of the PCI assessment. This process is detailed fully in the PCI DSS standard, which states that credit card data can be protected by masking that data (see section 3 and in particular requirement 3.3).

The next step to further reduce the compliance scope is to confine critical data processing to a small area of the organization, separated from the rest of normal operations. If any other areas of the business need access to the critical data, then the generic reference as stated above can be used in its place without disclosing the protected credit card data. In areas like PCI this will reduce or eliminate the need for application rewriting and database redevelopment. For example, if an online retailer can both physically and logically isolate where the credit card information is stored and is processed from the rest of the company's assets, the PCI scope can be limited to just the systems that processes and store the credit card information. Without that separation and compartmentalization, all of the assets will be included in the compliance scope thus greatly increasing the amount of testing time required, the potential remediation effort, and the cost required to get those systems in compliance.

Remove Complexity

Reducing the scope is one way to help remove complexity, but complexity comes in many forms and makes your ability to meet the requirements more difficult. Removing further complexity from business operations is key to achieving your compliance goals. The first step is to leverage the created data flow diagram to question the business rationale at each step of the analysis process. Some typical areas to examine closely are:

- Daisy chained applications that perform numerous calculations where you only need one calculation
- Retaining extra database data instead of eliminating everything except for only the data you truly need
- Using applications that are no longer supported by the vendor
- Continuing to use old business processes that no longer have business justification
- Adding process for the sake of process that does not enhance or simplify the business

The best approach to reducing complexity is to ask "WHY?" to each business process, application, and database entry. If the answer does not show significant benefit to the business then the process needs to be reviewed to see how it can be removed or at the least further simplified. Given that 90% of the PCI DSS requirements are based on having well documented and enforced processes in place, removing the complexity from normal business operations reduces the level of effort required to assess all of these processes. And, more importantly, assures that compliance is sought only for those processes that really require it.

Conclusions

Compliance is a business issue and must be managed by the business with the technical teams acting as service provider to the business units. By focusing on these simple concepts, companies will have a higher success rate in achieving their compliance goals without unnecessary costs. The business, however, must learn to leverage the true value the technical side brings through the assessment process. Not only do the issues need to be remediated, but the value of the information gleaned from these tests, if used properly, will help identify areas of risk to the business and potential areas of compliance scope concerns.

Once this process is completed and the concepts and decisions are made to achieve compliance with PCI, it is very easy to replicate out to any other regulatory requirement to include HIPAA and other privacy regulations surrounding Personally Identifiable Information (PII).

12460 Crabapple Road
Suite 202-253
Alpharetta, GA 30004
(516) 612-2060

sales@clearskies.net
www.clearskies.net

About Clear Skies Security, LLC

Clear Skies is a security consulting organization specializing in real world threat analysis through comprehensive security assessment services, specifically Penetration Testing and Application Assessments. Clear Skies focuses solely on services allowing our consultants to remain concentrated on providing the best vendor neutral advice to remediate the risks identified during the assessment process. Our primary goal is to become the Trusted Security Advisor for our clients. This allows us to work cooperatively to ensure the highest level of protection for the business and to provide some assurance in knowing that the true risks are being identified.

Clear Skies was founded by a team of elite security professionals, each bringing 10+ years of experience in the security industry, all with a specialty in security assessments. Our mission is to be a trusted name in the security industry, known for our technical knowledge, integrity, and business ethics. We do this by focusing on customer service and ensuring quality in everything we do.

In the end, our goal is to ensure that **our Intelligence Secures your Intelligence.**

2553 Housley Road
Suite 100
Annapolis, MD 21401
(888) 448-3002

www.riskwatch.com

About RiskWatch

The RiskWatch tools credibly guide the users through a process to qualify its security situation concerning threats, assets, potential loss, vulnerabilities, and safeguards per Gartner. The company has designed over a dozen specialized risk assessment software programs that are used by thousands of clients all over the world - in virtually every type of security assessment, gap analysis, and compliance assessment. RiskWatch clients include financial institutions, hospitals and healthcare organizations, insurance companies, infrastructure elements such as electrical producers, and both federal and state agencies. From multi-national corporations, to small banks, RiskWatch software is the most widely used security risk assessment software in the world. RiskWatch software was developed with Federal guidelines and a variety of US federal agencies, such as Veteran Affairs, the Department of Justice, the US Department of Defense, and the National Security Agency. All of these organizations have used RiskWatch applications for information security risk assessment and physical security assessments. RiskWatch is used by State governments in all 50 states, and internationally in Belgium, Canada, Dubai, England, Italy, Malta, Sweden, Saudi Arabia, Turkey, Romania, South Africa, Japan, Thailand and Switzerland.