ecora

WHITE PAPER

Securing Cardholder Data So You Don't Make Headlines

Using the PCI Data Security Standard as a Catalyst for Improving Information Security

PCI SECURITY VENDOR ALLIANCE MEMBER

Breaches in network security—particularly those that threaten customer credit card data—have impacted organizations of all sizes and types, from some of the world's most recognized brands to small, regional businesses, and these security breaches have made national, and international, headlines.

An escalation in the number of security breaches did not come about because the companies affected didn't have solid network security controls in place; most of them did. The fact is that security, and what needs to be secured, is more complex than ever before. It is no longer effective to secure just the enterprise perimeter. Today's organizations must secure the entire infrastructure, and they must control the people and processes that interact with the infrastructure as well. Neglecting security efforts in any one of these areas can leave an organization vulnerable to a security breach.

In fact, in today's business environment, focusing on IT security alone isn't enough. Organizations must broaden their thinking to encompass overall information risk. Information risk management is a business function and encompasses regulatory compliance as well as issues of intellectual property protection, insider abuse, and privacy. With a focus on information risk management, an organization will ensure a successful security program and a successful compliance program.

Security and Compliance through PCI-DSS

The Payment Card Industry Data Security Standard or PCI-DSS ensures that cardholder data is protected in the event of a security breach by requiring merchants and service providers that store, process, or transmit cardholder data to meet specific security requirements. When organizations work toward and achieve PCI compliance, they will have also implemented a number of key initiatives that improve overall information security.

According to Forrester Research, an audit for compliance with the PCI standard focuses on three primary areas reflecting the "processes," "technology infrastructure," and "people" that are critical to both compliance and security.

1. **Identification of sensitive data within your environment** such as electronic protected health information, social security numbers, cardholder data, and other confidential data.
2. **Identification of areas where data may be transmitted or stored**, including routers, switches, firewalls, IDS/IPS, and wireless; servers, PCs, mainframes, and PDAs; hard disks, printouts, backup tapes, audio recordings, vendors and third parties and their sub-servicers; load balancer(s), click tracker, middleware, SSL accelerators, TOE cards, web servers, application servers, and database servers; IVRs and call center "OB" capture systems; and temp files, C:\drives, flash drives, and file server with "everyone" access.
3. **Identification of all consumers of sensitive data**, including local staff, remote staff, consultants, business partners, and regulators.

Developing an Automated PCI Compliance Process

The most common challenges to PCI compliance center on protecting and managing data, controlling change, and auditing and enforcing policies. These challenges also link directly to the most commonly cited PCI violations. According to Forrester, the five most common PCI DSS violations include:

- Storage of prohibited data (e.g., full track, CVV2, PIN)
- Systems on which patches are not kept up to date
- Use of vendor default settings and passwords, such as with unsecured wireless
- SQL injection from poorly coded web-facing applications
- Unnecessary and vulnerable services on servers

The most effective way to address these challenges and to avoid any type of violation is through automation. In fact, the effective use of automation, combined with ongoing employee education and the adoption of effective policies, can help ensure compliance and security.

Continued on page 4.

The PCI "Digital Dozen"

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

Requirement 3: Protect stored data.

Requirement 4: Encrypt transmission of cardholder data and sensitive information across 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 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.

Johnny's Selected Seeds: Surviving a Breach

Founded in 1973, Johnny's Selected Seeds is a mail-order seed producer and merchant headquartered in Albion and Winslow, Maine. The company sells more than 1,500 varieties of vegetable, flower, and herb seeds to specialty commercial growers and home gardeners worldwide. The company also designs and manufactures garden hand tools and has an active plant breeding program.

Like many companies of this type, Johnny's Selected Seeds operated multiple servers dedicated to specific applications and housed behind a firewall. To further ensure security, the company looked to anti-virus and anti-spyware software to protect its infrastructure. According to Bill Gallagher, the company's director of operations, chief financial officer, and now chief security officer, the company felt confident that security access settings on its firewall were tight, allowing only minimal traffic, and that their general security was good overall.

On February 16, 2007, everything changed, however, when the company learned from a series of calls that some Johnny's customers had found fraudulent activity on their credit cards. "Red flags went up when a customer notified us that fraudulent charges had been placed on a credit card that had only been used on our website," Gallagher explained. "Audit logs confirmed that an intruder had accessed and likely downloaded 426 files containing cardholder data. To make matters worse, the files were in plain text and contained CVV data—and we had no idea that these files even existed. We estimated that approximately 11,500 records were compromised."

The company's internal investigation revealed that the security breach was not a result of "hacking" into the Johnny's Selected Seeds website; rather, the investigation indicated that the intruder had used a valid username and password to access the website's administration page. Clearly the work of a "professional," once the intruder had gained access, the strike was "surgical." The intruder went directly to the order file and then spent the next hour and 46 minutes downloading files. The hijacked IP address used by the intruder had never been used to access the site before the breach and has not been used to access the site since.

The internal investigation also showed that spyware programs, which had gone undetected by the company's anti-spyware software, were detected on 11 company workstations.

Johnny's Selected Seeds reported the breach and sent information on the compromised credit cards to their acquiring bank. In addition, hard drives were sent to forensic auditors and the FBI as evidence. "We also immediately notified all customers whose information had been compromised," Gallagher said. "I know this is not always the case, but we felt that we had an obligation to our customers. We also believe strongly that we—and our customers—were the victims of a crime."

At the same time, the team at Johnny's began a comprehensive review of infrastructure security using the PCI-DSS 1.1 standards as their guide. The company also hired a forensic auditor to analyze the breach.

> *"Automation has become essential to our preparedness and will play an important role in our ultimate success.*
>
> *—Bill Gallagher,*
> *Director of Operations*
> *Chief Financial Officer*
> *Chief Security Officer*

Since the breach, Johnny's Selected Seeds has tightened internal controls and procedures to align more closely with PCI requirements and industry best practices. The company no longer stores CVV data, for example, and retains credit card data only as long as there is a business reason to do so. In addition, the company has modified programs, changed encryptions, and updated access controls so that access to full, clear-text credit card information is extremely limited.

"To adopt industry best practices, we've worked with industry leaders such as Ecora to implement software solutions for audit logging, network monitoring, two-factor authentication to replace conventional username and password login, vulnerability scanning, intrusion detection, and centralized administration control of our patches, updates, and access," Gallagher said. "Automation has become essential to our preparedness and will play an important role in our ultimate success.

"We have committed financial resources to ensure PCI compliance by the end of 2007," Gallagher added. "We owe it to ourselves and to our customers. While our first full PCI compliance audit will likely pinpoint deficiencies, we are confident that we will be able to use the audit process to ensure compliance and more comprehensive security overall."

What has Johnny's Selected Seeds learned from the security breach and their ongoing efforts to ensure PCI compliance?

1. Do everything to limit the cardholder environment.
2. Do not store cardholder data beyond what is necessary for legitimate business purposes.
3. Encrypt, encrypt, encrypt; make it extremely difficult for anyone—whether internal or external—to access clear text cardholder data.
4. Centralize control to ensure that all security software is up to date.
5. Never assume that third-party vendors take security as seriously as you do.
6. Remember that the cost of PCI compliance is a lot less than the cost of a breach.
7. Adopt the mantra that ensuring network security is a journey, and sustain compliance by continuously looking for vulnerabilities in systems and processes.
8. Leverage software solutions, especially when it comes to audit logging and network monitoring. After a data compromise, it is more important to show what didn't happen, then to know what did happen. In the case of Johnny's Selected Seeds, the company can identify that 426 files were compromised, but because of the logging software they were using at the time, they can't show definitively whether the intruders accessed other information.
9. Listen to your IT people when it comes to security-related issues; see the world through their eyes. Johnny's had put off deploying some of their IT department's recommendations because it appeared that everything was fine. The problems came from what they couldn't see.

With the sheer volume of information processed, transmitted, and/or stored on virtually any infrastructure, collecting data manually is time consuming, expensive, and often not repeatable. In addition, because manual collection efforts may be conducted by different teams and at different intervals, auditors may not view the information as reliable, auditable evidence. Automated, systemic data collection is preferred to substantiate IT controls.

Adding to the problems with manual data collection is the increasing gap most organizations face between IT budgets and workload. Automation of processes is the only way to close this gap. See Figure 1. Automation can facilitate existing processes and can introduce cost and process efficiencies that can't be realized through manual efforts. Policy enforcement, monitoring, auditing, and reporting can all be streamlined through automation. Given the increasing demands placed on IT, in spite stagnant budgets and headcount, the only realistic way to sustain compliance is to automate the processes and controls within the organization.

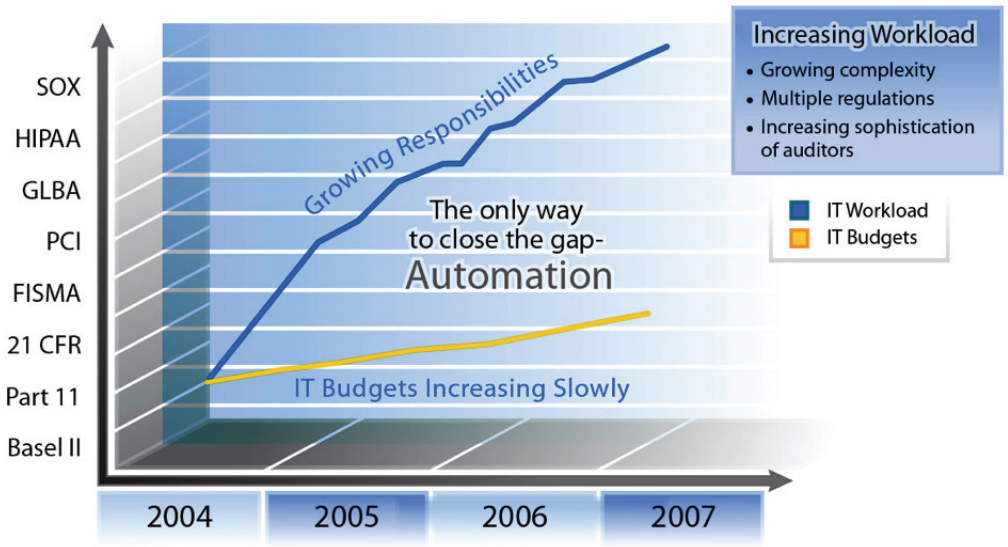

Figure 1. Increasing Gap between IT Budgets and Workload.

Most companies spend between one and ten percent of their IT budgets on compliance, but this figure depends on a number of factors, including maturity, industry, existing controls, timeframe to compliance, and executive buy-in. A recent InformationWeek study indicated that organizations with the fewest compliance problems spent nine percent more to automate audit functions and 11 percent less on contractors and outside services.

"It is on an order of magnitude more difficult to become PCI compliant than most of the audits that most of us have ever had to experience, because it goes so much deeper."

—Tony Rosanova, CTO, Zoot Enterprises, Inc.

Forrester's Seven Steps to Developing an Effective Compliance Process

1. Document the policy and control environment
2. Assign appropriate oversight of compliance management
3. Require personnel screening and access control
4. Ensure compliance through training and communication
5. Implement regular control monitoring and auditing
6. Consistently enforce the control environment
7. Prevent and respond to incidents and gaps in controls

FORRESTER®

The Evolution of IT Compliance and Best Practices

In the face of increasing requirements and expectation for continuous compliance, it is essential that compliance initiatives are strategic, integrated business processes and not one-time "projects." It is no longer acceptable to be in compliance for "audits only," and it is important to evaluate the effectiveness of IT controls and compliance initiatives regularly to ensure that goals are being met.

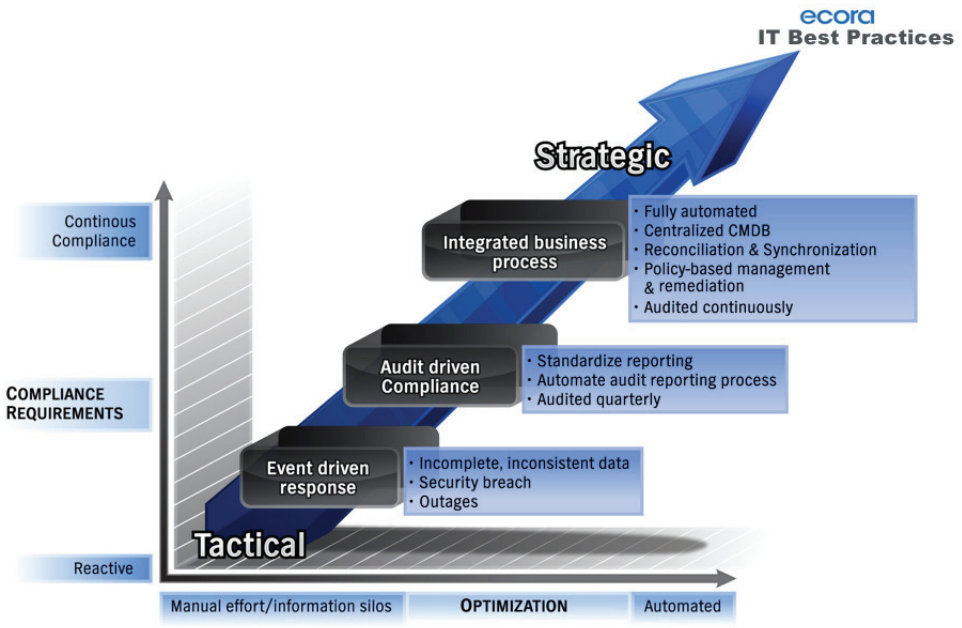

Figure 2. The Evolution of IT Compliance and Best Practices.

When compliance initiatives are treated as strategic, integrated processes, maintaining continuous compliance simply becomes a part of the way an organization does business. A centralized CMDB provides a single repository for data connection, configuration and change management becomes more effective, and policies are consistently enforced. In addition, because testing and reporting can be streamlined across the entire infrastructure, the workload and expense of manual identification can be eliminated, and organizations can reallocate scarce IT resources to focus on key, revenue-generating initiatives.

Building a Sustainable, Automated IT Compliance Program

Ecora provides software and services that allow organizations to implement sustainable, automated IT compliance programs. Organizations can realize both compliance and security, as well as greater operational efficiency. They will also benefit from the ability to validate compliance over time with a systematic approach to ensuring compliance throughout the IT infrastructure.

The Value of an Ecora PCI Gap Analysis

Ecora Professional Services offers merchants and service providers the opportunity to quickly analyze the existing control and process gaps associated with 9 of the 12 requirements that form the PCI Data Security Standard. Our value-added service offerings are based on the collective knowledge gained in working with our 3,600 world-wide customers.

An Ecora PCI Gap Analysis will:

- Assess the vulnerability and risk in your current IT operation
- Provide a gap analysis report that can be used to correct identified vulnerabilities
- Identify an automated process for reporting on PCI DSS audit requirements

"PCI has truly supported the concept that data classification is critically important so that you spend your money and your energy securing areas that need to be secured. Having visibility and making sure that you classify all your systems consistent with your data classification policy and the security requirements that exist are real challenges. "

—Tony Rosanova,
CTO, Zoot Enterprises, Inc.

The Ecora Approach

At Ecora, we don't believe in jumping directly from the problem to the solution without first asking questions, validating assumptions and gathering quantitative data. We employ a proven project framework to rapidly assess and document your specific IT challenges, not just PCI compliance. Recognizing that maximizing your time is critical, the assessment framework is typically conducted through a series of scheduled work sessions. Ecora professionals will organize, analyze, and develop all deliverables, then present our findings in a final meeting.

Gap analysis sessions are scheduled to identify system components that process, transmit, or store cardholder data and collect the configuration information necessary to provide a detailed assessment of the current information technology security processes. The stages of this service are:

- Introductory session with PCI Security Management team to review service requirements and deliverables,
- Identify PCI-significant systems that Ecora Auditor Professional will collect and analyze,
- Determine any existing security processes. If no policy or process exists, this will be noted in the final Gap Analysis report,
- Document security gaps within the customer's information systems environment that stores cardholder information,
- Preparation of a comprehensive gap analysis report

Tangible Results

With an Ecora PCI Gap Analysis, you will receive:

- Two-day engagement.*
- Documentation of the Business drivers and current process used to execute a PCI DSS audit. Use cases to describe the business driver's needs in detail.
- Documentation of the current physical inventory that are within the scope of a PCI DSS audit.
- Report documenting existing control gaps associated with the customer's computing environment that negatively impact the security of cardholder data and jeopardize compliance with PCI DSS.
- Executive Presentation of findings.

** Depending on size and complexity of the PCI-related computing environment, the Gap Analysis service may be extended beyond the current timeline at an additional fee.*

Find Out More

To learn how Ecora's PCI Gap Analysis Service or other Ecora software and services can help you automate detailed reporting for regulatory compliance audits and enabling IT best practices, call 877.923.2672 or +1 603.436.1616, email sales@ecora.com, or visit us on the web at www.ecora.com.

PCI SECURITY VENDOR ALLIANCE MEMBER

PCI Security Standards Council

As part of its commitment to ensure the ongoing security of cardholder data, Ecora Software is a participating organization with the PCI Security Standards Council, the independent body formed to develop, enhance, disseminate and assist with implementation of security standards for payment account security. Ecora is also a part of the PCI Security Vendors Alliance, whose mission is to provide products and services for the affected members of the payment card industry including retailers, E-commerce companies financial institutions, payment processors, POS vendors and any other organizations that must achieve compliance with the PCI Data Security Standards.

About Ecora Software

Ecora Software provides Enterprise Configuration Visibility™ to customers worldwide, ensuring their IT infrastructures are secure, compliant and effective. Ecora is the market-proven leader in transforming enterprise-wide configuration data into easy-to-understand reports for regulatory compliance and enabling IT best practices. The Company's flagship solution, Auditor Professional,™ provides the only patented architecture proven to automate the collection and reporting of configuration information from the entire infrastructure, without agents. Ecora Software takes the cost and complexity out of compliance audits and adopting IT best practices for more than 3,600 customers, including many of the Fortune 100. For more information, please visit Ecora at www.ecora.com.

ecora

2 International Drive, Suite 150 | Portsmouth, NH 03801 | p:877.92.ECORA 603.436.1616 | f:603.436.4344