2014 State of the Industry & PCI DSS

As we enter 2014, it is no secret that retail merchants remain one of the favorite targets of organized cyber thieves focused on stealing valuable personal data. In a statement in 2012, FBI Director Robert Mueller, summarized the state of the industry when he said: "...it is no longer a question of "if," but "when" and "how often."

"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[1]

Today we find Mr. Mueller's statements to have been prescient. In spite of increasingly rigorous security implementations and mandates, merchants continue to be victimized at alarming rates. Simply protecting sensitive personal data is challenging enough in today's environment, with increasingly rigorous and demanding regulatory mandates further increasing the challenges of doing business.

Achieving and maintaining compliance with PCI DSS v2.1 is difficult for many organizations. For large retailers, the burden of complying with the PCI DSS is often daunting, if not nearly impossible, at times. The complex, distributed environments of large retailers present unique challenges that are not seen within smaller or less complex merchants. One example can be found in Requirement 6.2 which mandates the implementation of "critical security patches" within "one month of release". In large, distributed environments with hundreds or even tens of thousands of systems, it becomes nearly impossible to comply with this seemingly simple requirement.

In November, 2013 the PCI SSC released PCI DSS V3.0. Although the Council has taken many recommendations to heart and made significant improvements, there are a number of changes that will increase the demands upon retail merchants required to comply with the PCI DSS. For example, the newly added Requirement 9.9 is expected to create additional effort and work to comply. Requirement 9.9 states that organizations must: "Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution." This single addition will require organizations to maintain an updated inventory of all devices including serial number and location, and establish a process to periodically inspect all devices to detect tampering or substitution. While the impact on a small retailer with 5 POS devices is minimal, the impact to a large retailer with 40,000 devices is extreme.

Why Care about PCI DSS?

Payment card operating regulations mandate that all merchants who accept branded payment cards comply with the PCI DSS at all times. There are additional requirements to validate compliance on an annual basis. The method of validation is based upon the merchant's transaction volume and other factors. For merchants that do not comply with the PCI DSS there are stiff penalties that can be passed on from the card brands to the acquiring banks, or in some instances, directly to the merchants. These penalties can range from $5,000 to $500,000, and can be assessed by both the banks and credit card institutions. Banks may also assess fees to recover the costs of the forensic research they must perform to remediate noncompliance.

In addition to these possible penalties, breaches of cardholder data can result in the following losses for a merchant:

- Suspension of credit card acceptance by a merchant's credit card account provider
- Loss of reputation with customers, suppliers, and partners
- Possible civil litigation from customers whose data was compromised
- Loss of customer trust, affecting future sales

Why AT&T for PCI Services?

In some situations, it is acceptable to use a vendor without worrying much about their expertise. Choosing the wrong lawn care service to mow the company's grass will not result in harmful effects lasting more than several weeks. However, choosing a tattoo artist, mechanic, or doctor who lacks the requisite expertise can create more significant and lasting problems. The same holds true in selecting a Qualified Security Assessor (QSA).

Although all QSAs must meet a basic set of requirements, they vary in skill, experience, and approach. These factors may impact the thoroughness and accuracy of the assessment you receive, as well as the QSA's ability to evaluate and improve your overall compliance and security posture. Before selecting a QSA, and during the engagement, keep in mind the following considerations: staffing, auditing vs. assessment, project scoping, onsite verification, feasibility of control recommendations, compensating controls, and recommendations and references. Your QSA should have the breadth and depth of security and compliance expertise to function not merely as an auditor but as a partner who can provide an in-depth assessment, recommend achievable controls, and help you develop a practical strategy for maintaining ongoing compliance and sound security.

In addition to being a level 1 merchant, AT&T is also a global provider that serves merchants and their vendors as a Level 1 Service Provider. In fact, AT&T has 20 distinct services which are validated annually for PCI DSS compliance. As such AT&T understands firsthand the complexities of achieving and maintaining compliance with the PCI DSS. The AT&T PCI Practice employs QSAs with industry leading experience and expertise. Some of our unique qualifications include specializing in large, complex retail merchants. AT&T Consulting is a Payment Card Industry (PCI) Qualified Security Assessor (QSA), a Payment Application Qualified Security Assessor (PA-QSA) and a Qualified Incident Response Assessor (QIRA).

AT&T Consulting has over 50 CISSPs, over 30 QSAs, and numerous team members holding other certifications such as CISSP, CISM, CISA, CFE, QSA, ITIL, and technology-specific certifications from Microsoft, Cisco, Checkpoint and other leading vendors. AT&T Consulting takes pride in its ability to staff a project with consultants possessing significant experience as practitioners and consultants in this field. Many of our consultants are risk management practitioners and security professionals from Fortune 1,000 companies. Consultants in AT&T average nearly ten years of experience. AT&T consultants hold elected officers and leadership positions within the Information Systems Security Association (ISSA) and the Information Systems Audit and Control Association (ISACA), are active participants in industry associations and consortiums, and are frequent presenters at conferences.

More than Simple QSAs

While many QSAs focus solely upon the annual assessment, AT&T focuses on helping companies achieve compliance in an efficient and cost effective manner. First and foremost, AT&T QSAs are information security professionals. This ensures that recommendations are not based only upon achieving compliance, but are also provided to help companies address and mitigate current market threats.

AT&T Consulting offers a range of comprehensive, customized PCI compliance solutions. The consulting team provides assessment certification, remediation, program development, penetration testing, code review and incident response services that help companies address specific areas of PCI compliance and best practice.

How to get started?

PCI DSS Version 3.0 becomes effective on January 1, 2014, and businesses will have one year to apply it. Some of the changes are future requirements that are classified as merely best practices until July 1, 2015.

Here is an action plan to help you get started with making security business as usual and getting a lead on PCI 3.0 Compliance:

- Adopt a data centric approach to security, risk and compliance
- Understand cardholder data, scoping and compensating controls
- Identify cardholder data locations and look for ways to "modify" data so it becomes 'non PCI' data. (Tokenization, truncation, etc.)
- Consolidate cardholder data and employ segmentation to reduce the PCI DSS 'footprint'
- Focus on policies, processes, and management of security
- Follow the PCI DSS from a logical and not sequential perspective
- Understand the intent of the requirements and when a specific requirement cannot be directly addressed, consider compensating controls.

As you consider the implications of PCI DSS Version 3.0 on your business, remember that AT&T Consulting is here to help you not only navigate the complex requirements of PCI compliance, but to do so with an eye towards improving your overall security posture.

Note

1. http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Share this with your peers

For more information contact an AT&T Representative or visit www.att.com/security-consulting.

Scan this code to learn more.

To learn more about AT&T Security Consulting, visit www.att.com/security-consulting or have us contact you.

12/27/13 AB-2859