Security solutions for retail

Retail businesses continue to face fundamental challenges to remain competitive with their peers. These challenges include reaching a broader customer base, improving customer satisfaction, managing inventory turns and controlling costs while also dealing with new technologies. This all brings pressure on the security needed to prevent fraud and maintain compliance in the retail industry.

Data breaches are very costly to the bottom line. The cost to mitigate a loss can range in the millions of dollars. In addition, corporate reputation is damaged and customer confidence is reduced due to data breaches.

Retail Data Protection Challenges

- Noncompliance can affect revenue and profit
- PCI is just one of several requirements issued by regulatory agencies liked the FCC or FDA
- Data can be lost anywhere from the point of sale to headquarters

PCI Compliance

Retail organizations of all sizes must protect their IT environments and the sensitive data they contain while maintaining compliance with mandates such as the Payment Card Industry Data Security Standard (PCI DSS). Because they often house sensitive data such as customer credit card numbers, social security numbers, PINs and other personally identifiable information (PII), retailers of all sizes are frequent targets for cyber-attacks.

Protecting Cardholder Data and Critical Systems

Protecting cardholder data, critical IT systems, web applications and e-commerce sites 24x7 is a complex and daunting task. Attack vectors range widely – POS systems, web applications, wireless networks, malware and more. Many retail environments are geographically distributed with numerous stores, distribution centers and branch locations. Because attacks can originate anywhere in the IT environment, it is important to secure and monitor these disparate systems.

Application Security

Weaknesses in application architectures have rapidly become the targets of choice for attackers. In fact, application security vulnerabilities have become one of the top information security issues facing organizations today. To stay ahead of the risks associated with the application layer, you must manage and maintain the security of every application deployed.

AT&T offers Application Security solutions that can help protect your most critical enterprise applications from both internal and external threats. Our consultants can dramatically improve your organization's ability to assess the security of existing applications as well as their ability to design, develop, test and maintain the security of applications in all phases of their development lifecycle.

Application security can be obtained and maintained only through a combination of activities – external testing of applications, application architecture reviews, source code reviews, database audits, continual training of development and security personnel, and implementation of security controls throughout the software development lifecycle (SDLC) processes.

AT&T provides information security services to help organizations of all sizes protect their IT assets, comply with industry requirements and government regulations, and reduce security costs. Other offerings include:

- **Managed Security** – Monitor and manage security devices 24x7 through our Security Operations Centers. Certified security specialists analyze network events and alert you to potential threats.
- **Security & Risk Consulting** – Evaluate vulnerabilities, manage compliance and help you improve the security of your network, communications and critical data.
- **Incident Response & Digital Forensics** – Investigate and resolve incidents ranging from single system compromises to enterprise-wide intrusions by advanced threats.

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

Share this with your peers

- **Threat Intelligence** — Identify emerging threats, develop countermeasures against new malware and exploits, and better protect customers by providing context around actual threats to their environment.
- **Security Risk Assessments** — Comprehensive analysis to identify the organizational security risks and compliance gaps.
- **Vulnerability and Penetration Testing** — Determine your system vulnerabilities and potentials for exploitation and help you close those gaps.
- **Policy and Procedure Development**—Ensure your policies and procedures are effective in communicating and delineating the proper protocol for security and compliance throughout the organization.
- **Employee Training** — Confirm employees know and follow correct policies and procedures and protocol for handling sensitive data.
- **Cloud and Mobile Security** — Ensure your cloud and mobile devices are effectively managed for security and data protection.
- **Business Associate and Vendor Management** — Assess and manage the privacy and security risks associated with business associates, sub-contractors and other third parties.

Count on Security Consulting from AT&T

AT&T has a long history of developing and managing security services that support a defense-in-depth architecture to help with your security policies. AT&T security consultants have experience handling large, complex infrastructure solution deployments. We follow industry best practices and a standardized methodology to help reduce risks and speed deployment of your end-to-end security solution.

Share this with your peers

For more information contact an AT&T Representative, call 877.542.8666 or visit www.att.com/security-consulting.

Scan this code to learn more.

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

06/16/14 AB-2948