WHITE PAPER

Protecting Credit Card Data: How to Achieve PCI Compliance

These days, anyone who owns a credit card is familiar with the problem of identity theft, in which technology-savvy thieves extract customer credit and debit card information from unsecured databases. It's a problem that affects everyone in the retail supply chain — the payment card companies, the banks, the retailers, and the individual customers whose identities are compromised. And while there are many ways to implement network protection, some retailers have delayed updating databases and networks with the latest authentication and encryption safeguards. Meanwhile, electronic thieves have been proactive in finding and attacking vulnerable networks. The problem has worsened over the years, especially with more and more retailers implementing wireless technology, which opens a new set of challenges. As technology proceeds in providing ease of use for consumers and stores alike, payment card security standards have been lax at best, especially in the United States, where credit card companies own the responsibility to protect the consumer data. Burdened by this liability, several credit card companies have joined forces to establish the Payment Card Industry (PCI) council, in order to create a common and accepted set of security guidelines. These guidelines are designed to keep retailers and their customers from falling victim to identity theft – to ensure that credit card data is protected.

History of the PCI Data Security Standard

Established in 2005 by a group of major credit card companies, the Payment Card Industry Data Security Standard (PCI-DSS) comprises a set of security guidelines that are designed to help retailers prevent credit card fraud and identity theft. In a nutshell, any company that processes, stores, or transmits credit card numbers must comply with the PCI DSS standard. Visa International, MasterCard Worldwide, Discover Financial Services, JSI, and American Express all require PCI compliance of the retail companies that run their customers' credit cards. And any company that fails to comply with the requirements may risk stiff penalties.

A governing body called the PCI Standards Council updated the standard in 2006. The current set of requirements is known as PCI v. 1.1, and retailers are required to comply with that version by September 2007. The Council anticipates that it will release technical updates to the standard once a year or even less than that, depending on emerging threats and industry trends. Notwithstanding such updates, the basic requirements of the PCI guidelines have remained pretty constant. The PCI DSS includes the following set of rules:

- **Build and maintain a secure network:** This includes firewall installation and a secure password policy.
- **Protect the cardholder's personal data:** This entails implementing data encryption across any public network.
- **Maintain a network vulnerability management program:** This includes regular updates to anti-virus software and other security software applications.
- **Implement strong access control measures:** This requires a unique ID assignment for each employee with network access.
- **Regularly monitor and test networks:** This means monitoring and keeping track of all access to cardholder data.
- **Maintain an Information Security policy:** Basically, this means adhering to all of the above, and documenting the policy as part of IT standard operating procedures.

The PCI Standards Council essentially considers wireless LANs to be public networks, and the standard includes several requirements that address WLANs specifically[1]. These requirements include:

- **Installing perimeter firewalls** between any wireless networks and the cardholder data environment, and configuring the firewalls to deny any traffic from the wireless environment — or from controlling any traffic, if such traffic is necessary for business purposes. This almost always requires installing a firewall between the retailer's company WLAN and the store's wired network.

- **Changing the default settings** for wired equivalent privacy (WEP) keys, SSIDs, passwords, and SNMP community strings; and disabling the automatic broadcast of SSIDs.

- **Encrypting any necessary wireless transmissions of cardholder data** by using Wi-Fi Protected Access (WPA and WPA2) technology, IPSEC virtual private networks, or secure socket layer/transport layer security (SSL/TLS). WEP is allowed, but if a retailer does use WEP, then WEP must be supplemented with an additional security mechanism.

- **Testing** security controls, limitations, network connections, and restrictions at least annually — and identifying all the wireless devices on the network at least quarterly.

- **Using a network intrusion detection system** to monitor all network traffic and send alerts about possible compromises. This applies to both wired and wireless network traffic.

Averting a security breach: the possibility is a reality

If you're thinking that the technology industry is so full of standards and specifications that it's nearly impossible to keep track of them all, you're right. If you're thinking that the PCI guidelines are among the specifications you can afford to ignore, you're wrong. The credit card industry created the PCI data security standard because the threat of identity theft is real, and it's growing.

According to a report by the consultancy Gartner Group, the U.S. saw more than a 50 percent increase in identity theft is between 2003 and 2006. Moreover, thieves were stealing more money, per capita, from the victims of identity theft; the average loss was $3,257 in 2006, up from $1,408 in 2005. Meanwhile, the percentage of funds that consumers were able to recover from thieves dropped from 87 percent in 2005 to 61 percent in 2006. Electronic theft of sensitive information continues to be a leading cause of credit card fraud, the report said, referring to card numbers as "low hanging fruit" for cyber criminals.

The cost of upgrading your network to comply with PCI DSS pales in comparison to the cost of compromising the credit card numbers of your customers. To wit, here are a few cautionary true crime stories:

- In the world's biggest known theft of credit-card numbers, cyber thieves launched an attack on a major national discount clothing retailer, a hack that began in July 2005 and continued throughout 2006. By the time the hack was discovered, the thieves had managed to steal at least 46 million credit and debit card numbers, along the with military identification and Social Security numbers of several hundred thousand customers. The hack served as a very public case for PCI compliance, as journalists from mainstream newspapers all over the world reported that the thieves had taken advantage of the retailer's poorly-protected wireless network. As it turned out, the retailer's WLAN had not yet implemented WPA or WPA2, relying instead on the outdated WEP standard. Moreover, auditors found that many of the computers that used the WLAN didn't have firewalls installed. The financial costs of the massive attack are still not clear, but it's safe to say the retailer is still looking at hundreds of millions of dollars in breach-related expenses — including several class-action lawsuits.

- In 2005, with similar methods, cyber thieves gained access to the customer databases of a national shoe retailer, and stole 1.4 million credit card numbers along with the names on those accounts. The theft affected 108 stores in 25 states.

1 - These items are culled from items 1.3.8, 2.1.1, 4.1.1, and 11.1 of the Payment Card Industry Data Security Standard. A complete copy of the PCI DSS can be found at https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

- Also in 2005, the *Jerusalem Post* ran the story of an Israeli bank that fell victim to a security breach when an enterprising criminal penetrated the building, installed a hidden wireless access point, rented an office space next door, and proceeded to break into the bank's network. This is a case in point that outlines why wireless intrusion prevention systems may be necessary for companies that don't even have a corporate WLAN.

- Back in 2000, a Russian hacker claimed to have gained access to some 350,000 user names and credit cards from an online music retailer, via the Internet, using nothing more than popular e-commerce transaction software.

Penalties for non-compliance

While the PCI data security standard provides a common set of security requirements for all the major electronic payment brands, each individual credit card company is in charge of enforcing that compliance. And every major credit card company is very serious about that enforcement. In fact, compliance audits are becoming more and more commonplace, as the industry works to prevent massive security breaches from happening in the future. Generally these audits comprise an on-site visit and a network scan by a PCI-authorized Qualified Security Assessor who can provide a Report of Compliance (ROC) certifying PCI compliance for any given site installation.

A retailer that is found to be non-PCI-compliant will face stiff penalties from the credit card company – regardless of whether the network has been compromised yet. Such penalties can include:

- **Hefty fines:** The fines for failing to comply with the PCI standards vary among the several card providers. Often fines are based on the size of the retailer, and according to whether a breach has occurred. But suffice it to say that the fees can be hefty. Some credit card companies have been rumored to charge up to $500,000 per incidence of non-compliance.

- **Sole Liability:** Historically, credit card companies have borne the brunt of the liability of electronic data theft. But today, if a retailer is the victim of a credit card security breach, the credit card provider is generally liable only if the retailer was PCI-compliant *at the time the security breach occurred*. Otherwise, the retailer will face a very expensive case of "we told you so." In addition to fines, non-compliant retailers face numerous damage control fees for compensating customers whose cards have been compromised. For example, most credit card companies charge a fee to reissue a new credit card or card number. That fee per customer is often nominal — around $25 per customer. But if a retailer is paying said fee for a million compromised customers, then that fee isn't a nominal penalty anymore.

- **Everyday fees:** Compliance has its privileges, and some credit card companies are making a point not only to penalize retailers who don't comply with the PCI standard, but to reward those who do comply. For instance, some credit card companies have said that they are considering raising the percentage-based fee per transaction that all retailers pay every time a customer uses a credit card, but that they will keep the percentage rate low for those customers who can prove PCI compliance.

- **The right to revoke a retailer's ability to accept credit cards:** If a retailer continues to flout PCI compliance, a credit card company may expel a retailer from its program, prohibiting that retailer from accepting its credit cards anymore.

For all of these reasons, it's important that retail operators have the tools for PCI enforcement, as well as the tools to prove compliance at any given time. The ability to enforce, prove and proactively report on compliance is especially important in case of a surprise audit by the credit card company — or an attempted security breach.

And while nobody can truthfully say that PCI enforcement is simple, retail IT administrators can keep headaches to a minimum by investing in a single-vendor solution that meets all the requirements of the standard. A Motorola Enterprise WLAN provides the tools IT administrators to adhere to the wireless networking rules of the PCI

standard, along with the reporting and forensics tools necessary to keep comprehensive records of network activity. *Motorola provides a one-stop shop for retailers who need to enforce PCI requirements. Comprising a complete suite of wireless networking products, a Motorola Enterprise WLAN is fully capable of compliance when implemented, maintained, and managed in accordance with recommended guidelines as part of a compliant system.*

Ensuring a PCI-capable solution with a Motorola Enterprise WLAN

All the mobile devices, access points, wireless switches, application servers, and management software in a Motorola Enterprise WLAN provide the support necessary for an IT administrator to build a PCI-capable wireless network:

- **Perimeter firewalls:** In accordance with the PCI guidelines, Motorola's RFS7000,WS2000 and WS5100 lines of wireless switches and the AP-51xx line of access points come with an integrated firewall that separates the WLAN from the wired network.

- **Comprehensive, up-to-date security support:** In accordance with the PCI guidelines, Motorola's wireless access points and switches offer support for both the WPA2 and WPA encryption standards, in addition to triple-DES IPSec encryption and a secure VPN client.

- **A seamless portfolio of PCI capable data capture products:** In maintaining a PCI-capable network, it is vital that the devices that access the network adhere to all security guidelines. Motorola offers a comprehensive line of data capture devices and mobile computers. By choosing to standardize on such client devices, you can ensure seamless interoperability between the devices and the WLAN. Moreover, you can be sure that every device on the network is PCI-capable.

- **Policy compliance:** One of the key concepts of PCI guidelines is that the IT administrator will create a set of fixed policies for the network and then ensure that all the sites and devices on the network adhere to these policies. The Motorola WIPS also helps IT administrators ensure that company employees and devices adhere to the rules and regulations of your PCI-capable network. In addition to keeping track of the devices, the WIPS keeps track of whether those devices adhere to any given network policies — including adherence to the PCI standard.

- **Intrusion detection and prevention:** To further enforce PCI rules, Motorola's comprehensive Wireless Intrusion Protection System (IPS) server software automatically takes necessary steps to mitigate malicious activity from rogue access points. In fact, WIPS detects the location of any device on the network, using an integrated location capability. This helps to ensure that everything on the corporate WLAN belongs there, further ensuring that rogue devices can be immediately thwarted. Thus, WIPS is a valuable tool even for retail environments that do not operate WLANs, but which do contain cardholder information on their wired networks.

Proving PCI compliance in the event of an attack or an audit

If a credit card company decides suddenly to audit your network for PCI compliance, it's likely because the credit company suspects that you may be shirking its compliance requirements; and it will be up to you, the retailer, to prove that you are, in fact, enforcing the rules. An audit is very stressful for any IT administrator, because failing an audit means facing the previously-mentioned penalties. An audit is even more stressful if you are dealing with a possible security breach at the time of the audit.

Motorola will help you pass a PCI compliance audit, not only by providing the tools to meet PCI requirements, but also by providing the tools you need to prove that compliance. That doesn't just mean proving that the network is compliant during

the audit. It means proving that your network has been compliant for as many months as the rules have been in place, and that you have kept up with any necessary updates. This is key: remember that the credit card provider is generally liable for damages incurred during a security breach only if the retailer was PCI-compliant *at the time the security breach occurred*. If a retailer was not PCI-compliant at the time the breach occurred, then that retailer will likely be solely responsible for the damages.

The Motorola WIPS is the tool that lets an IT administrator prove that the network is PCI-compliant. This added value of the Motorola WIPS comes from two of its most overlooked but most important features: reporting and forensics.

The Motorola WIPS server can generate various reports on the current or past several months of network status. Among these is a PCI-specific report that summarizes the security-related activity of the network, giving an immediate overview of how PCI-compliant the network was during any given time period. Thus, if a credit card company conducts a surprise audit, a retailer's IT administrator can be ready with a report that proves compliance. Without such a report, the retailer might be subject to a penalty.

Furthermore, the WIPS has an easily-searchable data store that lets IT administrators delve into several months of network events, to determine not only what happened to the network, but how it happened. In the event of a security breach, WIPS can show the IT administrators (and the auditors) how the breach was able to occur, even when the network adhered to the PCI guidelines. Not only does this feature help a retailer to pass the audit, but it also helps determine where best to implement safeguards to prevent future breaches. The forensic ability of the WIPS helps IT administrators to understand network compromises — and it also helps them to discount those events that are not network compromises.

Conclusion

Any retailer that accepts, processes, or stores credit card information must comply with the standards set by the Payment Card Industry Security Standards Council, or risk a hefty penalty. The best way to ensure standard compliance is to invest in technology that is PCI capable. A Motorola Enterprise Mobility solution — including data capture devices, mobile computers and Enterprise WLAN infrastructure -- can provide the tools necessary to build a complete end-to-end PCI-capable solution. A Motorola Enterprise WLAN will help to protect your customers' credit card data from identity thieves, who thrive on pulling your customers' information out of the air. At the end of the day, nothing is more important than protecting your customers.

The good news is that Motorola has over 30 years of experience in providing our customers security solutions and Enterprise Mobility products that work together to create a flexible PCI solution. We have the team and industry expertise to talk to retailers about PCI and are here to help you strategize to tackle these scenarios.

To inquire how a retail mobility assessment can help you better understand Enterprise Mobility solutions and provide guidance on PCI Standards, contact Ed Weiser of the Retail Industry Solutions Group at ed.weiser@motorola.com.

For more information about Motorola Enterprise WLAN products visit: URL here http://www.symbol.com/wireless-infrastructure/wireless-lan

For more information on PCI Security Standards Council, visit https://www.pcisecuritystandards.org/

MOTOROLA

motorola.com