PCI Compliance: Building a Secure Network

OVERVIEW

With credit card breaches unveiled in the news so frequently, it's become evident it's more important than ever that all merchants, no matter how big or small, take security seriously. Lack of education and awareness around payment security, as well as poor implementation and maintenance of the required standards leads to many of the breaches occurring today, as cardholder data continues to be a target for criminals.

In 2006, five founding global payment brands – American Express, Discover Finance Services, JCB International, MasterCard and Visa Inc. – joined forces to create the Payment Credit Industry Data Security Standard (PCI DSS), compiling rules and guidelines for businesses to follow in order to establish procedures that protect customer data and help prevent breaches.

Nearly a decade later, the PCI compliance standards have continued to become more stringent. One of the main, and most essential, PCI requirements focuses on preventing outsiders from gaining access in to companies' servers through firewalls. New standards and requirements within the third version of the PCI DSS are to be enforced on January 1, 2015.

The reality of meeting these PCI standards can be a daunting task, especially for a large company with multiple locations. However, even more daunting can be the huge losses from having to pay to replace customer's credit cards as well as having to refund the cost of the fraudulent purchases. For example, the data security breach at Home Depot in September 2014 cost nearly $60 million to reissue cards and cover fraudulent charges according to the Credit Union National Association.

DATUM
strategic | compliant | results

ABOUT DATUM

Datum is a full-service technology consulting partner and provides all-inclusive IT solutions to clients nationwide. Founded in 2003, Datum integrates best-of-breed technology solutions with specialties in the multi-unit restaurant market. Headquartered in Sarasota, Florida with satellite offices in Phoenix, Dallas, Los Angeles and Honolulu, Datum serves nearly 3,500 active locations. There are currently over 145,000 client employees supported by Datum's technology center 24 hours a day, 7 days a week, 365 days a year.

www.datumcorporation.com

PCI REQUIREMENTS & BEST PRACTICES

Although the size of the business will determine the specific compliance requirements that must be met, compliance with the PCI DSS is mandatory for any and all merchants who accept credit cards, online or offline. In order to comply with the new version of PCI DSS the core 12 security areas remain the same, but updates include several new sub-requirements that did not exist previously. According to the PCI Security Standards Council, the updates provide stronger focus on some of the greater risk areas in the threat environment, such as the firewall.

Payment security is an ongoing process that needs to be continuously monitored and assessed. Evaluating operations regularly and fixing any vulnerabilities discovered is crucial. Any costs associated with having to make changes to business operations are easily outweighed by the risk of costs from the aftermath of a credit card breach occurrence. According to the Ponemon Institute's *2014 Cost of Data Breach Study: Global Analysis*, sponsored by IBM, the average total cost to a company for a data breach increased 15% to $3.5 million in 2014.

Businesses can easily become overwhelmed by keeping up with PCI DSS' technical and operational requirements, especially with new updates being released in an attempt to stay ahead of the curve against hackers. With guidance from industry professionals and technology consultants such as Datum Corporation, merchants can gain expert advice and help to overcome any obstacles that are in their way of obtaining compliance and protecting their business.

BUILDING A SECURE NETWORK

Merchants can easily request a review of business operations and receive recommendations on security best practices as they relate to PCI compliance. As a national leading technology consulting company, Datum ensures proper procedures are in place by providing software solutions and helping to configure secure network layouts.

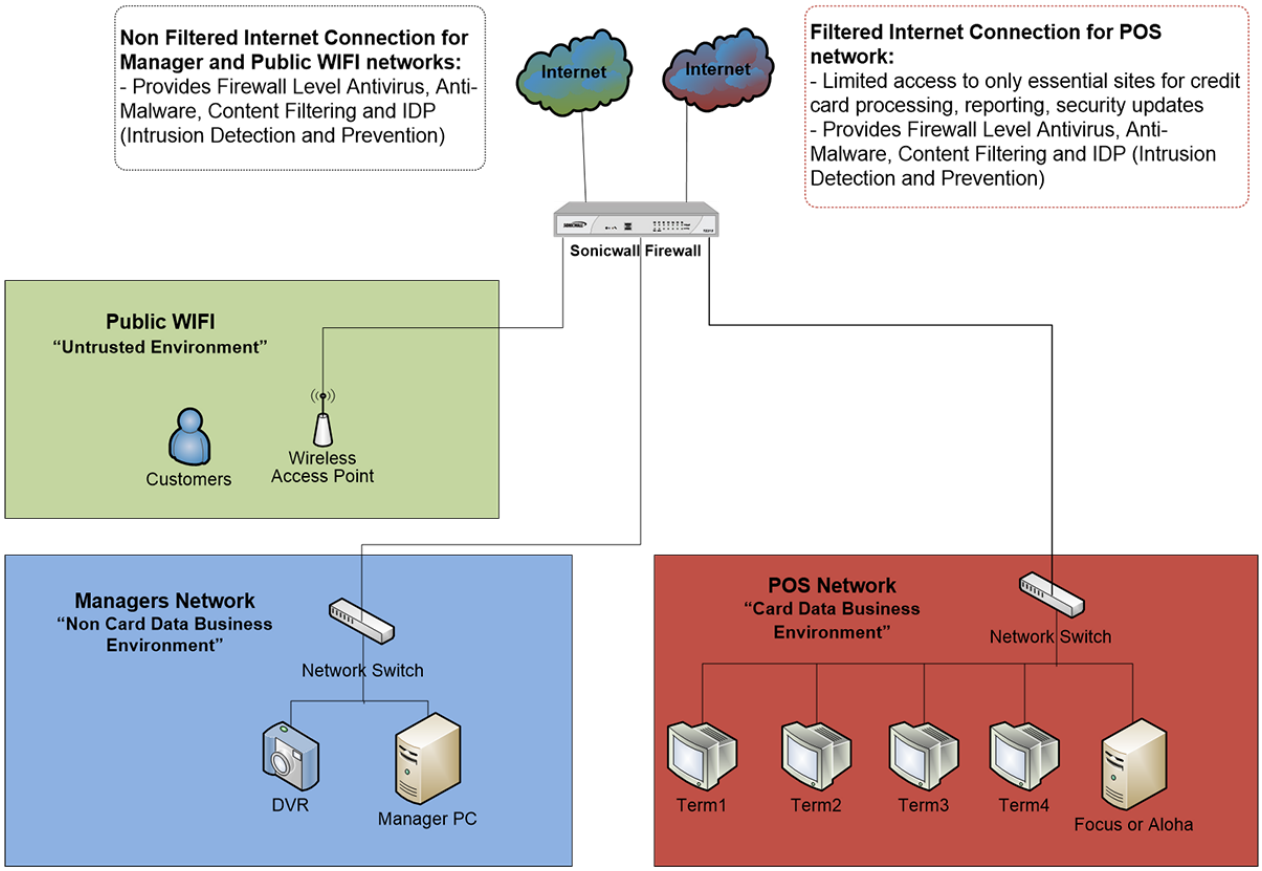
One of the best ways to attain protection and comply with several of the most important PCI rules and regulations is by installing a business class firewall. This will simultaneously protect customer's data by preventing hackers from gaining access to their information, and help protect businesses from large fines and loss of sales.

Installing a business class firewall allows for separation between trusted and untrusted networks. The trusted network is where the point-of-sale system and its customer data is stored, while a manager's network and public Wi-Fi access are a part of the separate untrusted network. As a PCI requirement, merchants must restrict inbound and outbound traffic so that cardholder data stays protected, and a business class firewall does just that. In fact, the business class firewall meets the very first of the PCI DSS requirements:

- Install and maintain a firewall configuration to protect cardholder data

DATUM
strategic | compliant | results

The following graphic illustrates an example of how to build a recommended secure network layout with a business class firewall.



This suggested network layout meets multiple PCI requirements, including but not limited to:

- Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks
- Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment
- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic
- Secure and synchronize router configuration files
- Prohibit direct public access between the Internet and any system component in the cardholder data environment
- Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network
- Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties

DATUM
strategic | compliant | results

ABOUT DATUM

Datum is a full-service technology consulting partner and provides all-inclusive IT solutions to clients nationwide. Founded in 2003, Datum integrates best-of-breed technology solutions with specialties in the multi-unit restaurant market. Headquartered in Sarasota, Florida with satellite offices in Phoenix, Dallas, Los Angeles and Honolulu, Datum serves nearly 3,500 active locations. There are currently over 145,000 client employees supported by Datum's technology center 24 hours a day, 7 days a week, 365 days a year.

www.datumcorporation.com

CONCLUSION

All merchants are expected to understand and comply with PCI standards and regulations. Securing cardholder data is a shared responsibility, and the newest PCI DSS place an emphasis on education, awareness and increased flexibility for businesses.

The ramifications of a data breach can be not only extremely costly financially, but can also cause irreversible damage through the loss of consumer trust. According to Retail Customer Experience, 87% of people surveyed are “not at all likely” or “not very likely” to do business with an organization that had suffered a data breach involving credit card details.

Many data breaches can be avoided in the future by following these best practices and adhering to the latest PCI standards. Now is the perfect time to review your security procedures and confirm PCI DSS compliance for your business. Although the technical nuances can be overwhelming for some business owners, there are many resources and vendors that provide solutions to make sure your business is not the next to make headlines in the news for a data breach.

For more information and details on PCI DSS compliance, visit https://www.pcisecuritystandards.org.

Sources

1. PCI Security Standards Council: https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf
2. Washington Business Journal: http://www.bizjournals.com/washington/blog/2014/11/how-much-did-the-home-depot-data-breach-cost-local.html?page=all
3. Ponemon Institute: http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis
4. Retail Customer Experience: http://www.retailcustomerexperience.com/blogs/5-lessons-learned-from-recent-retail-data-breaches-infographic/?rb=false
5. Payment Card Industry (PCI) Data Security Standard, v3.0, 2006-2013, PCI Security Standards Council, LLC

DATUM
strategic | compliant | results

ABOUT DATUM

Datum is a full-service technology consulting partner and provides all-inclusive IT solutions to clients nationwide. Founded in 2003, Datum integrates best-of-breed technology solutions with specialties in the multi-unit restaurant market. Headquartered in Sarasota, Florida with satellite offices in Phoenix, Dallas, Los Angeles and Honolulu, Datum serves nearly 3,500 active locations. There are currently over 145,000 client employees supported by Datum’s technology center 24 hours a day, 7 days a week, 365 days a year.

www.datumcorporation.com