



Lippis Report 176:
**PCI 2.0: Maintaining Compliance in a Mobile,
Cloud and Virtualized IT World**

By Nicholas John Lippis III
President, Lippis Consulting

July, 2011

It seems like every week or so there is news of a massive cyber attack where criminals get away with stealing credit card and other personal data on the order of tens of millions of individual records. Sony, Bank of America, Epsilon, Nintendo, the International Monetary Fund, the US Senate and CIA are but a few of the targets for high-profile cyber attacks that took place in 2011. According to a recent study by the Ponemon Institute, “cyber attacks have recently become more harsh and recurrent. At least 90% of the IT practitioners surveyed claimed that they had experienced one or more cyber breaches within the last year, and 89% of these respondents could not identify the source of these breaches.”

To mitigate and avoid these breaches and protect credit card information, the Payment Card Industry (PCI) Security Standards Council issued PCI Data Security Standard (DSS) 2.0 in late 2010. The emphasis of PCI DSS 2.0 is two-fold: 1) provide increased protections not addressed in the previous standard (i.e., wireless and virtualized infrastructure) and 2) maintain compliance. As all of the breached organizations above were in compliance at some time but failed to maintain it, this exposed their customers to hackers and ultimately being breached. In short PCI DSS 2.0 is about being vigilant about maintaining security.

In the data center, virtualized servers are now defined within PCI and guidance is given on how to secure them given that all hypervisors are deemed insecure. In addition, wireless detection methods were expanded to address the variety of retailer capabilities.

IT business leaders who support any organization that stores, processes or transmits credit card data are required to ensure PCI 2.0 compliance not only during an assessment but continually to avoid the fate of the above-mentioned organizations. The key to a successful PCI assessment is to simplify this major effort. Some tech firms are assisting this effort through validation and assessment of compliance prior to installation. In this Research Note, we review Cisco's PCI Solution 2.0 as it offers a unique network-based approach that is comprehensive, holistic and end-to-end. It has been tested in a simulated retail environment and assessed for compliance by a Qualified Security Assessor, QSA, and Verizon Business.

Cisco's PCI Solution 2.0

The Cisco PCI Solution 2.0 is built on network security best practices, proven Cisco products and partner technologies that meet Payment Card Industry security standards. Because PCI covers many parts of the network, no single product or technology meets all PCI technology requirements. Therefore Cisco's updated PCI Solution 2.0 is an architectural approach that maps to the updated PCI DSS 2.0 requirements. This comprehensive perspective allows retailers to see the bigger picture to prepare and design across the relevant parts of the enterprise. Cisco's PCI Solution 2.0 is a holistic approach as it spans an end-end architecture.

Cisco's approach provides templates and services that simplify PCI compliance. This simplification enables customers to maintain compliance year round, not just during assessments. Detailed information, including product configurations from validation efforts, is included in the Cisco PCI Solution 2.0 Design and Implementation Guide (DIG) to provide additional guidance and best practices.

Simplifying PCI Compliance

As a first step toward simplifying compliance, Cisco recommends segmenting the IT infrastructure and isolating cardholder data from the rest of the network. As with any complex problem, breaking a problem down into smaller solvable pieces reduces the complexity and simplifies the solution. Cisco's approach reduces the scope of audit via network segmentation. Without network segmentation, the entire IT infrastructure is in PCI scope, which drives cost and complexity significantly upward. While segmentation sounds easy, it's a bit more challenging in a virtualized data center infrastructure.

PCI Compliance in the Virtualized Data Center

Most IT business leaders are challenged with complex PCI audits within virtualized infrastructure as well as rogue wireless access detection. These two areas, virtualized infrastructure and rogue wireless access detection, tend to be the two largest pain points. Confusion around virtualization and security has existed for several years until the PCI standards body clarified that all hypervisors are considered insecure. With so many organizations having virtualized their data centers, this detail results in extra compliance considerations to protect cardholder data. Before virtualization, traditional infrastructure could be easily protected with a firewall appliance, as this device was placed directly in the path of traffic. In highly-virtualized environments, traffic is not as well-behaved, offering IT managers a challenge to restrict cardholder data.

Cisco's Virtual Security Gateway (VSG), along with its Nexus 1000k virtual switch, intercepts and steers traffic to either VSG or firewall appliances before it gains access to cardholder data, providing a means for segmentation and access restriction in virtualized data centers.

Therefore to be PCI DSS 2.0 compliant, both physical and virtualized infrastructure need to secure and restrict access to cardholder data. Cisco does this with both its own VSG solution as well as with technology partners such as EMC, VMware, VCE and HyTrust.

Rogue Wireless Access Detection

Rogue access point detection is a PCI requirement. Even if a merchant does not use wireless technology within its stores, it still must have a method for detecting unauthorized access points that may have been inadvertently or maliciously deployed. The PCI Council expanded the flexibility of the requirement to allow for several methods, including Wireless IDS and NAC/802.1x to detect rogue wireless access points.

Unified Wireless and Cisco's Identity Services Engine (ISE) technology offer technical solutions for these methods that have been validated by Verizon Business to successfully address these requirements. In addition, Cisco offers CleanAir technology, which monitors the entire frequency spectrum, surpassing the security requirements of PCI.

Risk Management

While a portion of PCI compliance is addressed through technology, it's also addressed with process and compliance audits. One of the largest challenges is to maintain compliance between audits. Many retailers seek the lowest cost solution to achieve PCI compliance during the audit, but this may very well be penny wise and pound foolish. For example, some retailers conduct a visual inspection of Ethernet switches quarterly to ensure that unauthorized wireless access points are not connected into the corporate network, thereby opening a door to rogue access. The difficulty of this approach is that quarterly physical scans only work during inspection day. The day after the quarterly scan someone can

plug in a wireless access point, putting the site and cardholder data at risk until the next quarterly inspection. A more continuous and secure approach is the implementation of wireless IDS, IPS, CleanAir and ISE, where every single wave is monitored and wireless devices plugged into the corporate network are detected assuring continual PCI compliance.

How to Approach PCI Compliance?

PCI can be an overwhelming topic. How do IT and small business leaders approach PCI compliance? To simplify PCI, Cisco offers three recommendations.

Recommendation One: Reduce PCI Scope. Scope means all systems and people that are touching cardholder data (i.e., firewalls and IT administrators). Are there people accessing cardholder data who shouldn't be? If they are, then remove their access by restricting access to the systems that contain cardholder data. Are there systems or applications or networks that are touching cardholder data that don't need to? Segment and narrow the scope of the Cardholder Data Environment (CDE) with network addressing and filters to decrement the risk as much as possible. If the CDE is smaller, the cost of the audit will be smaller as will be the complexity of maintenance. Standardizing network and system architectures across branches can also decrease cost and complexity as it allows auditors to sample same store/branch footprints and data center designs.

Recommendation Two: Secure the Perimeter. With a new smaller PCI scope implemented, the perimeter of that scope needs to be secure. Firewalls configured to only allow business-justified access to the cardholder data environment and IDS need to be installed. In addition, administrative access to this environment needs to be locked down to the bare minimum with complete logging for audit trails.

Recommendation Three: Maintain and Simplify. It's not good enough just to segment and reduce the scope of cardholder data and then protect the perimeter. IT business leaders need to maintain and simplify their PCI recommended implementation. Cisco's solution utilizes RSA technology to provide real-time alerts, tuned logs and compliance management dashboards that assist in maintaining compliance. The firms mentioned in the opening paragraph were all in compliance at some point in time, but they were not when they were breached. So take these requirements seriously.

Implementing a PCI Solution 2.0

The above three recommendations will go a long way toward reducing cost and keeping an organization's systems PCI compliant. Cisco has made a huge commitment in its thoughtful approach to PCI DSS 2.0 compliance where it offers an end-end architecture that has been assessed and documented. A critical element of the Cisco PCI Solution for Retail 2.0 is Cisco network architecture and validated network designs. Cisco network architectures have been designed for stores, enterprise data centers and the Internet edge to support e-commerce operations, store employees, customers and teleworkers. Cisco's PCI solution also supports wireless 3G technology deployments and multiple store formats, including pop-up stores, and convenience stores, in addition to typical small, medium and large stores.

Cisco's PCI Solution 2.0 offers thought leadership for those seeking to simplify their PCI deployments; Cisco's new PCI DIG is an in-depth, roadmap for organizations looking to achieve PCI compliance. It addresses technologies such as virtualization, wireless and mobile payments. As the number of high profile and alarming plus brazen cyber attacks occur, IT business leaders would be well-served to review Cisco's PCI Solution 2.0 and Design and Implementation Guide.

About Nick Lippis



Nicholas J. Lippis III is a world-renowned authority on advanced IP networks, communications and their benefits to business objectives. He is the publisher of the Lippis Report, a resource for network and IT business decision makers to which over 35,000 executive IT business leaders subscribe. Its Lippis Report podcasts have been downloaded over 160,000 times; i-Tunes reports that listeners also download the Wall Street Journal's Money Matters, Business Week's Climbing the Ladder, The Economist and The Harvard Business Review's IdeaCast. Mr. Lippis is currently working with clients to design their private and public virtualized data center cloud computing network architectures to reap maximum business value and outcome.

He has advised numerous Global 2000 firms on network architecture, design, implementation, vendor selection and budgeting, with clients including Barclays Bank, Eastman Kodak Company, Federal Deposit Insurance Corporation (FDIC), Hughes Aerospace, Liberty Mutual, Schering-Plough, Camp Dresser McKee, the state of Alaska, Microsoft, Kaiser Permanente, Sprint, Worldcom, Cigitel, Cisco Systems, Hewlett Packet, IBM, Avaya and many others. He works exclusively with CIOs and their direct reports. Mr. Lippis possesses a unique perspective of market forces and trends occurring within the computer networking industry derived from his experience with both supply and demand side clients.

Mr. Lippis received the prestigious Boston University College of Engineering Alumni award for advancing the profession. He has been named one of the top 40 most powerful and influential people in the networking industry by Network World. TechTarget an industry on-line publication has named him a network design guru while Network Computing Magazine has called him a star IT guru.

Mr. Lippis founded Strategic Networks Consulting, Inc., a well-respected and influential computer networking industry-consulting concern, which was purchased by Softbank/Ziff-Davis in 1996. He is a frequent keynote speaker at industry events and is widely quoted in the business and industry press. He serves on the Dean of Boston University's College of Engineering Board of Advisors as well as many start-up venture firm's advisory boards. He delivered the commencement speech to Boston University College of Engineering graduates in 2007. Mr. Lippis received his Bachelor of Science in Electrical Engineering and his Master of Science in Systems Engineering from Boston University. His Masters' thesis work included selected technical courses and advisors from Massachusetts Institute of Technology on optical communications and computing.