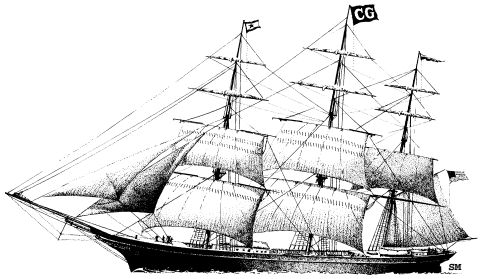
THE CLIPPER GROUP
Captain's Log™



Navigating Information Technology Horizons℠

Published Since 2001 Report #TCG2007093 October 31, 2007

The Brave New World of PCI DSS — Why You May Need to Think Differently about Your Systems Architecture(s)

Analyst: Mike Kahn

Management Summary

A day doesn't go by when I don't get several alarming emails proclaiming the pending difficulties that many businesses will face under the requirements of *PCI DSS*. Today, I got offers for nine white papers or webcasts, each addressing a piece of the problem. For those not familiar with this acronym, PCI DSS is *Payment Card Industry (PCI) Data Security Standard (DSS)*. The key word in this is *security* and is applied broadly to all things informational, especially those pieces dealing with private/personal information.

If your first thought is that requirements of PCI DSS only will apply to financial institutions and credit card companies, you would be wrong. This also applies to anyone handling credit cards (i.e., processing credit card transactions). All of a sudden, you begin to realize how wide the PCI DSS net will be cast and how vulnerable your business might be to embarrassment and litigation, if you fail to "get on board" quickly.

If you are reading this, it probably pertains to your enterprise or organization. Now that you understand that you need to do something, it is important that you understand the breadth of the requirements. This is, by itself, a significant undertaking, as the requirements are spelled out in 16-page specification, which can be downloaded from https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf. It consists of 12 requirements grouped into seven areas, which are outlined below.

- **Build and Maintain a Secure Network**
  - *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
  - *Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
  - *Requirement 3:* Protect stored cardholder data
  - *Requirement 4:* Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
  - *Requirement 5:* Use and regularly update anti-virus software
  - *Requirement 6:* Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
  - *Requirement 7:* Restrict access to cardholder data by business need-to-know
  - *Requirement 8:* Assign a unique ID to each person with computer access
  - *Requirement 9:* Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
  - *Requirement 10:* Track and monitor all access to network resources and cardholder data
  - *Requirement 11:* Regularly test security systems and processes
- **Maintain an Information Security Policy**
  - *Requirement 12:* Maintain a policy that addresses information security

Source: PCI Security Standards Council

OK, that list doesn't sound too intimidating, at least on the surface. It even sounds reasonable! What business wouldn't want to implement these requirements? (And that is the first "loaded question". More on this to follow.) Of course, we all know that the "devil is in the details" and there are lots of very specific details. (More on the details to follow, as well.) **The bottom line is that implementing the entire set of requirements is a huge challenge to the very largest enterprises and a difficult challenge to those businesses that are smaller.**

The largest enterprises have great expertise at all levels – but the scope of their information systems sprawl is very large. This creates the "huge challenges". **Implementing the requirements broadly can require a huge effort, depending a lot on the underlying systems architecture(s) and the number and types of locations in which IT infrastructure is placed.** Smaller enterprises have a problem of less expertise and experience in doing all-encompassing information security (in comparison to their bigger brethren) but also may suffer from the complications of systems architecture and locations (albeit usually on a smaller scale).

This brings us to the first loaded question about *who wouldn't want to implement these requirements?* The answer is simple: *only a fool*. The litigation rodeo has already begun. Companies of all sizes are being targeted for failing to handle credit card transactions competently to protect the privacy of the customer. A simple violation of printing the whole credit card number, with its expiration date, on a transaction receipt, might subject the company to a class action suit.[1] This is just one example of hundreds of potential vulnerabilities (i.e., violations) that might be discovered by your auditors, your customers, their lawyers, or your worst enemies, those looking to perpetrate fraud on a grand scale. (See *The Challenge of Presumption* in the box in the upper right corner of this page.)

A lot of PCI DSS just seems like common sense, until you go about planning for and implementing all of the requirements across your enterprise, large or small. While the devil may be in the details, the challenge likely is going to be exacerbated many times by the IT infrastructure that you now have in place. I'm sure that you don't want to hear this, but for several decades, we have been optimizing infrastructure under the wrong set of parameters. Yes, they may have seemed right or even been right for the times, but that was before the institution of PCI DSS and other information protection standards, from compliance to archival. This is the real focus of this bulletin – understanding what systems architecture has to do with the scope of the challenges of implementing PCI DSS successfully.[2]

There are conclusions that need to be put up front, in this management summary. They will be discussed on the following pages.

1. **Widely-distributed systems and data stores usually bring many**

The Challenge of Presumption

In legal matters, we often hear the phrase "presumed innocent until proven guilty". **With respect to the requirements of PCI DSS, it seems that an enterprise is "presumed guilty until proven innocent", with a few important exceptions.** This is really important. Being presumed to be guilty can be almost as bad as actually being negligent. While the burden of presumption is on you, your stock can drop, your customers can go elsewhere, and you are subject to a number of inquiries that might be painful and costly. If you are found to be negligent, then you probably are required to pay the costs of forensics, fines, financial losses by those affected, the costs of remediation, and the costs of dispute resolution.

You are presumed guilty unless you can prove that you have complied with all of the requirements. In order to prove compliance, you need to survive an audit by a certified auditor. If you haven't addressed the requirements of PCI DSS, you are in big trouble. If you haven't addressed and corrected any known shortcomings, you are in even bigger trouble. (Ignorance isn't bliss but it might be only a little better than failing to correct known vulnerabilities, i.e., leaving open the bank vault door.)

[1] As has happened in litigation with which the author is familiar.

[2] If you want to read a tutorial on enterprise security, see *The Challenge of Enterprise Security* in the April 5, 2007, issue of Clipper Notes, which is available at http://www.clipper.com/research/TCG2007050.pdf.

security implementation and compliance complications, when compared to fewer (more centralized) systems and data stores.

2. **Using different security solutions (on different platforms) adds greatly to the complexity** of achieving coverage (in general), in effectively managing the ongoing effort, and in auditing the processes and systems.
3. **A centrally-controlled security solution, therefore, may be the most effective and the most efficient solution.**
4. **The security solution is the most important application in the enterprise.** The highest availability is required for the security solution. Additionally, it is critical for all important business activities (e.g., you can't process credit card transactions without adequate security) plus you can't run any applications if you can't isolate applications from inappropriate users and also isolate confidential data from "wandering" applications and unapproved users.
5. **No platform can do this better than an IBM Mainframe, *System z9*.**[3] While this is an important realization, this paper is not focused on why this is true, at least directly. It is the nature of the security problems and the requirements of the solution that point to the Mainframe. The details about how the System z9 delivers the best solution are the subject of a second bulletin.[4]

Read on to see some of the details about PCI DSS and to understand these five conclusions.

Why Many Have Been Headed in the Wrong Direction

This section is about more than PCI DSS, but it applies just the same.

Part 1 – The Pendulum Swings Back

For several decades, many enterprises have been expanding servers outward, pushing thousands of PC server instances into the extended (distributed) enterprise, although many have returned into data centers since the turn of the 21st Century, when an era of recentralization began, initially focused largely on storage systems. More recently, the trend of server consolidation has reached significant activity levels, largely for four reasons.

1. Aging servers (especially those of the one-application-per-server variety) were, in most cases, severely underutilized, yet needed to be replaced because they were costly to maintain and manage.
2. Multi-core architectures have pushed a lot more processing power and memory in each instance of a new Intel Architecture (IA) server.
3. Server virtualization on IA servers, primarily through VMware, enables these larger servers to be partitioned into several-to-many virtual servers.
4. The cost of electricity and cooling has become a focal point and the inefficiency (underutilization) of older servers and the power-hungry and hot higher-core count new servers screamed for shared solution (i.e., virtualization of new servers).

These represent a significant change in IT thinking for many IT organizations; whether or not this is recognized is a further issue. Here's why.

The new, bigger, shared IA64 (mostly) servers, whether rackmounted or as blade systems, are each a *large system* by earlier standards. If your older (circa 2000) 500MHz dual-processor servers were only used 20% of the time (i.e., 20% utilization factor), you probably could consolidate 20 or more of these servers into one quad-processor, dual-core system (with a total of eight cores running at 2 GHz each). If you work out the math, you were using 200 MHz in the old system (20% times 1GHz) and, with the new server, you should be able to use half of the capacity or 8 GHz (50% utilization at 16

[3] For an update on Mainframe mythology see *The Clipper Group Captain's Log* dated May 23, 2006, entitled *Mainframe Mythologies Live On - Setting the Record Straight*, which is available at http://www.clipper.com/research/TCG2006038.pdf.

[4] See *PCI DSS Compliance and System z – A Combination that Makes Sense* in **The Clipper Group Navigator** dated October 31, 2007, and available at http://www.clipper.com/research/TCG2007094.pdf.

GHz total), with room to spare, since this works out to be 40 times more powerful than the earlier servers. The point here isn't the math but the fact that **you are now running 10, 20, or even 40 applications on a single server, a trend that is going to continue.**

This is a *scale-up* kind of operational challenge in *scale-out* sheep's clothing. It is not the same as before when there was one app on each server. Large systems thinking is required, especially when you realize that you may want to dynamically manage hundreds of these new servers (which are getting larger with each year) that are running thousands of operating systems images with applications. All of a sudden, the beauty of running a scale-up solution with shared resources and vibrant partitioning (i.e., virtualization of a higher order)[5] begins to make sense (once again for those of us who are old enough to know better, but a first-time realization for many).

Back to the PCI DSS part of this problem. **If you can imagine managing security on hundreds or thousands of servers and providing a useful audit trail as part of that process, you hopefully now begin to see the value of doing this on as few servers as possible. Certainly, a single and broad point of security control (of course, on a highly-available and very flexible server) is very attractive when compared to the chaos of doing this across hundreds or thousands of physical servers and thousands or tens of thousands of virtual servers.** This is one of the whack-yourself-on-the-side-of-your-head conclusions for which Homer Simpson would respond "Duh!"

Part 2 – The Pendulum Swings Deeper

At the same time, businesses have been opening themselves up for all kinds of end-user, partner, and greater internal interaction and transactions. You no longer can hide behind the cloak of anonymity; your internal processes are exposed, quite intentionally, almost everywhere, especially if you do business over the public Internet. You have no choice but to do so and this is the reason why the problem is so much bigger today.

[5] For example, in most scale-up (SMP) environments, the partition size can be made a fraction of a core or a multiple of cores, including a fraction (such as 3.5 cores). This means that the partition is truly without physical encumbrances, i.e., doesn't care where it resides or over how many cores and processors it is extended.

Some Guidelines to Ponder

1. The system with the most virtualization probably is the superior solution architecturally.
2. The system with the best virtualization probably is the most efficient and, concomitantly, the most effective.
3. The system with the most flexibility in dynamically provisioning assets (think "virtual resources for virtual servers") probably is the superior solution operationally.
4. The system with the most extensible capacities, in its largest instance, probably can offer the lowest cost per unit of resources.
5. The system with the highest-availability may be required, even if it costs more to implement.
6. The system with the most connectivity within the system (as opposed to externally between system components) probably has the lowest networking costs.
7. The system with the most policy-driven automation probably has the lowest cost of administration and operation.
8. The system with the most "open" approach to applications may have the widest applicability in the larger enterprise.
9. The system with the best end-to-end security solution (for, say, PCI DSS) trumps all others.
10. The system with the fewest components is a lot easier. Why take on responsibility for planning, building, wiring, and connecting hundreds or thousands of servers together when you might be able to get a preassembled and test solution one a single box or a small number of boxes?
11. The system designed to use the least amount of energy while doing the most work (energy efficiency) probably is the right system to keep Data Center costs from escalating as the cost of energy rise year after year.

Source: Excerpted from *Roddenberry, Einstein and the Dinosaur — Considering the Unfathomable in IT Optimization* in *The Clipper Group Captain's Log* dated October 8, 2007, and available at http://www.clipper.com/research/TCG2007091.pdf.

Part 3 – The Pendulum Swings Faster

We've all heard about "Internet years", a misnomered takeoff on "light years". We all know that a year is a year. The concept of Internet years is loaded with the implication that things happen quickly. The pace of change in IT technology, new information and application offerings, and broadened, worldwide availability is faster now than any time in history. What worked before may not scale up to the on-demand requirements of today's business world. When you add in new (or additional) security, privacy, and compliance requirements, the distance to the goal line surely has increased from where you were before.

Compounding Parameters

Securely Managing Applications is Key

Few folks are accessing enterprise data directly. Almost everyone comes through

Key Mainframe Security Capabilities

Security Built-In by Design

- **Enforced Workload Isolation** - Executables only accessible to authorized users
- **Storage Protection Keys** - Controls access to protected storage and prevents unauthorized data access

Security through virtualization

- **Virtual servers on a single mainframe via Logical Partitions (LPAR)** - provides up to 60 isolated system images with flexible dynamic provisioning of hardware resources, with the highest Common Criteria certification for server virtualization – *EAL5*
- **Virtual network in the server** - Provides an integrated TCP/IP network through system memory, enables a "Data Center" inside a box with a mixture of z/OS and Linux images, provides highly secure connection – no external network exposed

System z Security

- **Security-rich holistic design** to help protect system from malware, viruses, and insider threats, encryption solutions to help secure data from theft or compromise, addresses compliance needs with more confidence.
- **World-class Access Control (RACF)** enables application and database security without modifying applications. Can reduce security complexity and expense by central security process that is easy to apply to new workloads or as user base increases which tracks activity to address audit and compliance requirements. Integrates with distributed system security domain.

Network Security

- **Policy-based z/OS intrusion prevention** services
- **Perimeter defense - a *DMZ on Linux on System z with c*entralized firewall** policy management and firewall workload balancing

Network Encryption

- **Satisfies pervasive regulatory requirements and data security policies**
- **Application-based encryption** (with SSL and TLS) with encryption acceleration
- **End-to-end network encryption (with IPsec)** - can create a secure tunnel for selected network traffic (VPNs), with specialty engine support to reduce the cost of adding IPSec protection
- **File transmission encryption including IPsec or SSL protected FTP**; OpenSSH
- **z/OS Encryption Facility** for file level encryption

Scalable, secure digital certificate hosting

- **Enables a Certificate Authority solution** (no need to pay a third party CA for certificates**)**

Encryption solutions

- **Encryption infrastructure** that includes server-based encryption acceleration, tamper-resistant key processing, and key management
- **Encryption solutions** for databases, tape, file and network

Source: IBM

application programs or utilities of one sort or another. Thus, it is important to manage and provide secure access to all applications. If you can do this from a single point of control, your challenge is manageable. If you have many points of control, maintaining security is much more difficult. In addition, the ability to audit across applications becomes much more difficult or even impossible without human involvement. If an application on one server calls for selected data on a second server, whose user ID is going to be recorded in the second server's security log? It will be the server or application making the request that will be recorded and not the user who made the request transparently through another server or servers. If you can imagine this scenario in a highly-decomposed (granular) application environment (think SOA) then you can see the auditing nightmare building a rat's nest of interrelationships that must be manually traversed.

Data Security is Important Too

If you thought that applications were an operational and auditing nightmare, just think about what is required to control and record access to data files and objects distributed across (i.e., operationally owned by) tens of thousands of virtual servers images.

Each Network Connection Adds to the Maze

Now, add the complexity of all of the networks (cabling, switches, routers, etc.) required to attach all of the servers together and to all of the "virtually attached" storage. Each one is a potential point of infiltration. By limiting the number of servers and storage arrays that need to be connected, the problem is made simpler. If you could do it a lot of the networking between applications and data with a single computer (i.e., without having to go through external networks), securing the networks is more easily attained. **What is needed is end-to-end control. This is best done with fewer of independent points of control (servers).**

A Really Important Conclusion

If you already have a Mainframe at the center of your IT infrastructure (i.e., running your most important workloads, including transaction processing and databases), you're already going to have to do all of the work needed to bring your System z environment, applications, data, etc., into compliance with PCI DSS. **Once you've gone to the trouble of doing this, think how much easier it will be to do more, properly-secured work on the Mainframe, especially with its baked-in security, isolated partitions, advanced virtualization, internal networking, etc., rather than on some other platform.** (See the text box on the previous page entitled "Key Mainframe Security Capabilities".) While it may cost a little more, and that, in itself, is always very debatable, it will be a lot easier to consolidate and protect work there than anywhere else.

If you don't have a Mainframe but are committed to centralized databases, *Linux*, *Java*, SOA and/or *WebSphere*, there's an option here that might make your future a lot simpler, especially with respect to securing the data and IT infrastructure end to end. Don't fall for the mythology; take a closer look at why the Mainframe may be the best vehicle to achieving your PCI DSS goals.

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Mike Kahn **is Managing Director and a founder of The Clipper Group.** Mr. Kahn is a veteran of the computer industry, having spent more than three decades working on information technology, spending the last decade and a half at Clipper. For the vendor community, Mr. Kahn specializes on strategic marketing issues, especially for new and costly technologies and services, competitive analysis, and sales support. For the end-user community, he focuses on mission-critical information management decisions. Prior positions held by Mr. Kahn include: at International Data Corporation - Director of the Competitive Resource Center, Director of Consulting for the Software Research Group, and Director of the Systems Integration Program; President of Power Factor Corporation, a Boston-based electronics firm; at Honeywell Bull - Director of International Marketing and Support; at Honeywell Information Systems - Director of Marketing and Director of Strategy, Technology and Research; with Arthur D. Little, Inc. - a consultant specializing in database management systems and information resource management; and, for Intel Corporation, Mr. Kahn served in a variety of field and home office marketing management positions. Earlier, he founded and managed PRISM Associates of Ann Arbor, Michigan, a systems consulting firm specializing in data management products and applications. Mr. Kahn also managed a relational DBMS development group at The University of Michigan where he earned B.S.E. and M.S.E. degrees in industrial engineering.

- ***Reach Mike Kahn via e-mail at MikeKahn@clipper.com or via phone at (781) 235-0085 Ext. 121. (Please dial "121" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager**, *Clipper* **Notes**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.