

An ILLUMANT White Paper



PCI Compliance for Higher Education Institutions

WRITTEN BY

WAYNE SISK

DATE

OCTOBER 2008

PCI and the University

A university, unlike retail corporations, is unique in the way it processes credit card information in the sense that card processing functions often manifest in numerous shapes and sizes, and they are run by disparate management teams throughout each campus. Despite the distributed management of the payment processing functions, ultimately the university as a whole is responsible for protection of all card member data transacted according to the PCI standard. It is important to consider this all-important factor when approaching PCI compliance at a university or university system.

Part I – What You Should Know about PCI

PCI is the commonly used short acronym for the Payment Card Industry Data Security Standard (PCI DSS) which sets the requirements for maintaining an acceptable level of data security when actively engaged in handling payment card data. This standard is sponsored and supported by many of the major credit card providers via the PCI Security Standards Council, which has the following mission:

The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.

Ultimately this mission affects all entities, universities, governments, and corporations alike, in their handling of payment card data for any of the five major payment card brands under the auspices of the PCI Data Security Standard.

General Concerns with the Standard

The principles and requirements espoused by PCI are for the most part accepted as “best practices”; however, in reality, compliance with these standards and actual effective implementation of them may not be the same. While the standard seeks to insure the highest level of security for card holder data, technology and technological threats move so swiftly that entities wishing to comply with the standard must often do more than the minimum to meet the goal of data security and integrity.

It has become clear that PCI compliance in itself is not a silver bullet. Several entities certified as PCI compliant have experienced security breaches involving payment card data. Worse, many card issuers have spread the liability to other partner entities in the transaction processing chain.

The key to successfully protecting payment card data is to incorporate PCI compliance as part of an overall data protection program and to bolster that program with protection measures which exceed the PCI standard as required based on a proper risk assessment. Organizations should also clearly understand that security protection measures can mitigate risks but never completely remove them.

The Essence of PCI DSS

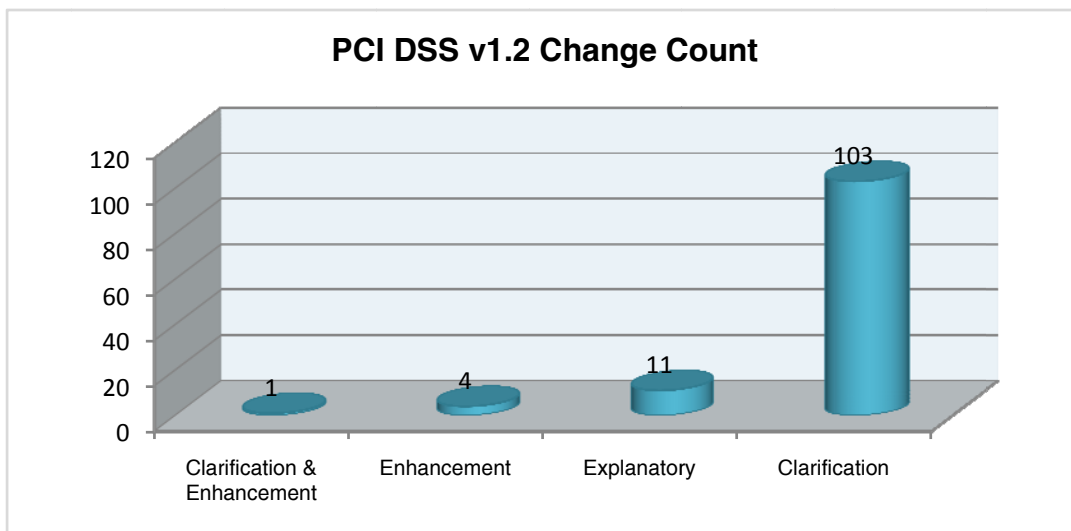
At its core, there are six primary principles, and twelve accompanying requirements in the PCI DSS, around which the specific elements of the DSS are organized. These cover the technical and logistical aspects of data security:

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

These principles form the basis of compliance with PCI and should be applied wherever card holder data is transacted, processes or stored.

What's New with PCI DSS

While there were a great many (119) changes made to the standard on October 1, 2008, most were clarifications and explanations added to make the standard less susceptible to erroneous interpretations. Only five were actual enhancements.



Moreover, two of the enhancements were to the appendices. This low number of enhancements clearly demonstrates that the standard should have few significant effects on the entities that are required to comply with the standard and the auditing and consulting companies that support such efforts.

Part II – PCI for Higher Education

For higher education institutions (HEIs) looking to comply with the PCI DSS, it is instructive to understand what other HEIs are doing.

Data from an online survey from the Treasury Institute provides insights as to how other HEIs are approaching PCI implementation.

What Other HEIs are Doing

Assessment of the Problem

- Where is the data?
 - Often it is in an un-segmented network and far too vulnerable to the threat of unauthorized access.
 - Within multi-campus institutions, all campus and merchant areas need to be identified.
- Who has access?
 - Often access is well controlled for granting initial access but fails when that access is transferred and when employees exit the company.
 - There is insufficient monitoring of employees and their access privileges.
- Is the card holder data encrypted?
 - If it is not encrypted, it is typically in a secure network zone. However, backup data and hot second site business continuity installations are often at risk.
- Is there a vulnerability management program in place?
 - Often antivirus technology is made available, but its use is not mandated.
 - Often systems, applications, and databases are not designed with security in mind.
- Is there a network monitoring program in place? Are the networks tested for vulnerabilities?
 - Network monitoring and testing is often nonexistent.
- Are all required policies and procedures in place?
 - Often incomplete and/or weak policies are relied upon. A policy and procedure maturity analysis can identify weaknesses, as well as missing security policies and procedures.

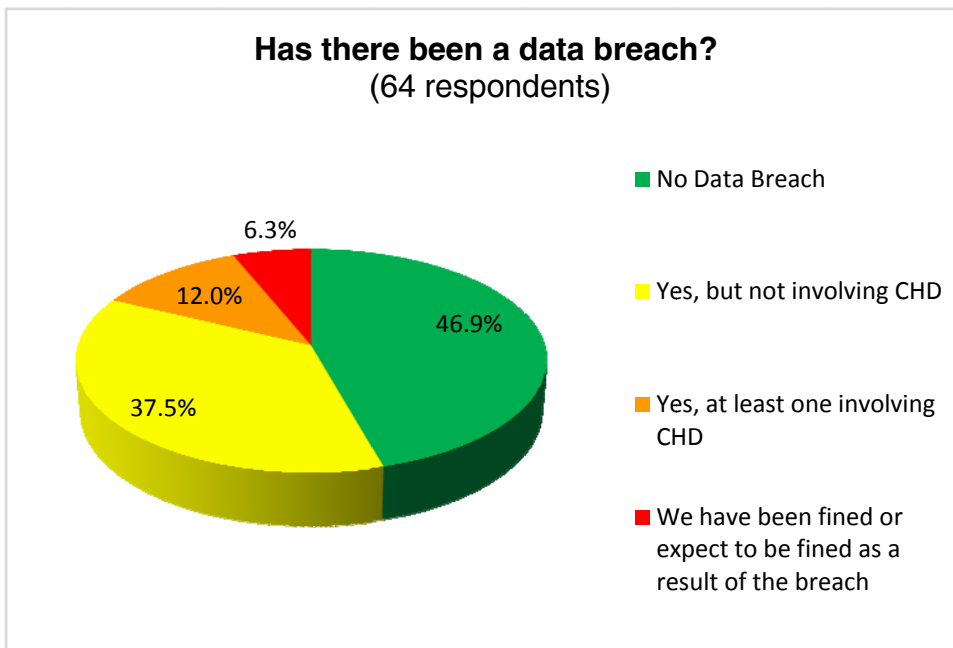
Planning and Prioritization

Identifying all potential card holder data sources helps to provide the bigger picture and is a crucial first step in terms of protecting such data. Most HEIs have indicated the need for the centralization of card holder data wherever possible, allowing for the demarcation of a secure network zone for the card holder data, thus also limiting what needs to be in scope for PCI certification.

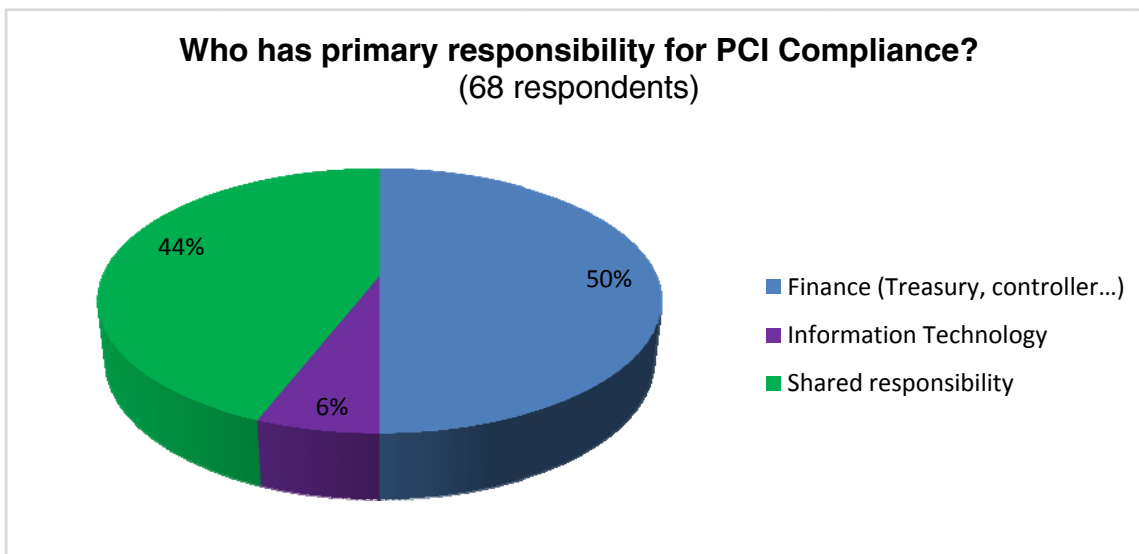
This process can also be used to identify and protect other sensitive data.

Typically the relocation of major servers to a secure and restricted network zone is a significant win, both in terms of easing performance and for un-scoping as much of the network as possible from the PCI DSS remediation efforts.

Statistics from the Treasury Institute



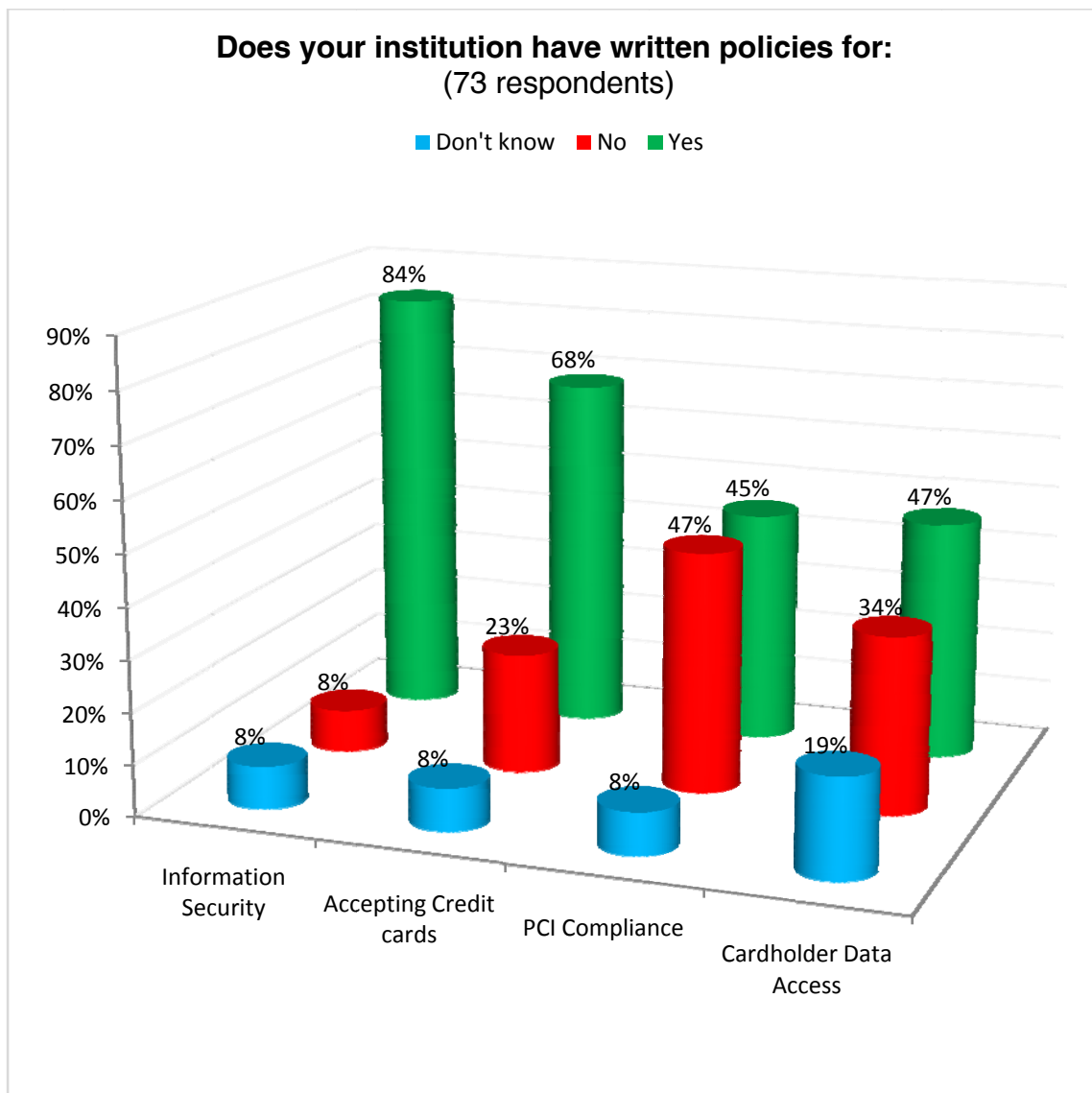
Over 50% of the respondents reported having had some class of data breach in the past 3 years, with 12% involving Card Holder Data (CHD).



According to the Treasury Institute survey:

“44% explained that no single department in their institution controlled their compliance effort, but rather that it was truly a shared responsibility often involving Audit, Purchasing, Legal, and other areas in addition to Finance and IT”

This indicates no conclusive position on who ought to have control over the process; however, in Illumant's experience, it is critical that policies have backing at the highest level of management to insure effective implementation.



Most intuitions indicated having at least a data security policy. However, in Illumant's experience, most institutions have policies with limited maturity and incomplete content. This is reflected in the increasing lack of policies beyond Information Security.

How Illumant Can Help

With a full suite of security analysis tools and a staff experienced in implementing security at all levels and for many requirements in addition to PCI DSS, Illumant can assist any organization, including Universities, seeking to implement and even exceed the PCI DSS requirements. Our experts can:

- Determine compliance requirements based on the volume of credit card transactions and payment processing infrastructure
- Technically assess the current state of PCI compliance
 - Assess network vulnerabilities
 - Assess data risk
 - Assist in vulnerability management programs
 - Assess and test access control programs
 - Monitor and test networks
- Recommend improvements and solutions for meeting requirements
 - Implement improvements and solutions, including review and revision of security policies and procedures
- Deploy technical security measures

Illumant has spent many hours developing the tools to evaluate and implement security across many requirements, including PCI DSS. Please contact us today and allow us to share our deep expertise with you as you explore complying with PCI DSS.

About the Author

Wayne Sisk spent 22 years at Space Systems LORAL (Formerly Ford Aerospace) in the Space Systems Division as a Sr. Designer, CAD Applications Engineer, IT Manager, and Regulatory Compliance Manager. Since leaving Space Systems LORAL he has been a consultant to over 25 clients, focusing on IT governance, security, audit preparation, and internal audit. He is currently a Sr. Consultant at Illumant, LLC, a security and compliance consultancy.



ILLUMANT

2672 Bayshore Parkway
Suite 505
Mountain View, CA 94043
Phone: +1 650.961.5911
Fax: +1 650.961.5912

www.illumant.com

ABOUT ILLUMANT

Illumant is a trusted strategic and tactical risk management advisor to Fortune 500 companies, higher education institutions, and other public and pre-public enterprises.

Leveraging best practices and deep knowledge of governance, risk management, compliance, and information technology, we partner with our clients to assess and solve critical business problems. Whether the focus is on initiatives driven by regulatory compliance, corporate mergers and acquisitions, or operational pain points, Illumant plays a major role in helping clients consistently meet their objectives.