Royal HOLLOWAY SERIES 2012

Can PCI DSS Compliance Be Achieved in a Cloud Environment?

Organisations are considering whether to run PCI DSS-based systems in a cloud environment. The security controls in the cloud may be sufficient to achieve compliance, but doing so may not be cost effective or practical.

BY PATRICK DURKIN AND GERAINT PRICE

TechTarget

Royal Holloway University of London

Can PCI DSS Compliance Be Achieved in a Cloud Environment?

TODAY, CLOUD COMPUTING is being marketed as the solution to the majority of an organisation's IT needs. Combining this with the growth of e-commerce, it seems beneficial for organisations to use a cloud service's flexibility to meet its business requirements. However, before moving IT services to the cloud, an organisation must consider the contractual, legal, and regulatory obligations it has to the protection of data.

The storing and processing of data may require compliance to laws and standards such as the Data Protection Act, government standards and PCI DSS. When the data is hosted within an organisation's own environment, or in a dedicated private hosting solution, system boundaries can be relatively easily defined. This is not the case when using shared resources such as a cloud service. How can an organisation be assured of where its data actually is? Who has access to the data, network traffic and system administration interfaces? How can unauthorised access be detected and how are data confidentiality and integrity services provided?

Whilst these questions should be considered in any environment, the problems are compounded when using cloud services. This is due to the different levels of administration, resource separation and data destruction.

DEFINING CLOUD COMPUTING

"Cloud" is an abstract idea that has been accepted by the IT industry. Cloud computing has been adopted by many to describe various services provided, typically on an on-demand, pay-as-you-go basis by a service provider to a customer, and accessed via the Internet. It usually includes five essential characteristics:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Cloud computing is offered to consumers under three service models, usually described as:

- **Software** as a Service (SaaS)
- **Infrastructure** as a Service (IaaS)
- **Platform** as a Service (PaaS)

Cloud services may be:

- **Public**–multi-tenanted, or
- **Private**–dedicated to a single customer

Combining cloud service models and hosting models is known as a hybrid cloud model.

The use of the metering can facilitate the understanding of the true IT requirements of an organisation and its cost on a department by department basis. This is now marketed to an organisation as IT as a Service (ITaaS).

Independent of cloud computing, moving from self-hosted IT services to outsourced IT services has been a business model for some time now. Two primary economic implications are:

- A shift of capital expenditure (Capex) to operational expenditure (Opex)
- The potential reduction in Opex when operating the IT services

This shift from Capex to Opex can lower the financial barriers for the initiation of a new project. Cloud computing removes the investment commitment to dedicated hardware for customers and improves resource utilisation for service providers.

The difference in economics between private and outsourced hosting models and the cloud model is due to better cost structures for cloud infrastructures. The primary reason is simply the economics of volume.

INTRODUCING E-COMMERCE

E-commerce is the buying and selling of products or services via the Internet. Associated electronic payment methods have evolved from those within the physical commerce system and consequently have much in common with each other. Electronic money transfers are not new technology. Banks have been using electronic transfers since the 1960s and bank customers have been able to withdraw cash from ATMs since the 1970s.

When using electronic payment systems, the transaction process requires communication between the user, merchant and card issuer. Since e-commerce commonly uses the internet as a communication channel, transaction communications must be protected from eavesdropping and manipulation to ensure the confidentiality and integrity of the transaction details. The payment card data will also be vulnerable if an attacker can access component parts of an e-commerce system. So communication between these parts must also be protected to ensure end-to-end confidentiality and integrity of the transaction details.

THREATS TO E-COMMERCE

Organised crime has realised the value of payment card details stored online. So the threat of unauthorised disclosure of payment card data via web and online services has now become a reality. The UK National Security Council has stated that attacks on computer networks and systems represent one of the biggest emerging threats to the UK. Cybercrime–illegal activity using computer systems and networks–has now been recognised by the courts for some time. This has enabled law enforcement authorities to act and deter such activities. The law applies to people, not technologies. Therefore, once the perpetrator is identified, a crime committed via the Internet can indeed lead to prosecution and imprisonment.

THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

The PCI DSS was jointly created in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express. In 2006, the PCI Security Standards Council (PCI SSC) was launched to provide the ongoing development, management, education and awareness of the security standard.

The goal of PCI DSS is to encourage merchants and service providers to protect payment card data. The DSS affects any company or organisation that accepts, processes, transmits or stores payment card details. It comprises a minimum set of requirements intended to reduce the risk and

provide a holistic approach to the security of the Card Data Environment (CDE).

Currently PCI DSS has no legal status and can only be enforced by contractual methods. The PCI Security Standards Council does not impose any consequences for non-compliance and there are no standardised penalties. However, payment card brands attempt to enforce compliance through differential processing fees, fines and other financial penalties.

VIRTUALISATION AND PCI DSS

In 2011 the PCI Security Standards Council issued an information supplement: Virtualization Guidelines. This provides guidance on the use of virtualisation technologies in a CDE. There are four simple principles associated with the use of virtualisation in CDEs:

1. **If virtualisation technologies are used** in a CDE, PCI DSS requirements apply to those virtualisation technologies.

2. **Virtualisation technology introduces** new risks that must be assessed.

3. **Implementations of virtual technologies** can vary greatly.

4. **There is no one-size-fits-all method or solution** to configure virtualised environments to meet PCI DSS requirements.

Of these four principles, (3) and (4) are applicable to all implementations of CDEs. So we concentrate on the aspects of (1) and (2) which are specific to virtualisation. These principles can be combined into:

- Virtualisation technologies have to be risk-assessed and controls implemented to meet at least the requirements of PCI DSS.

The PCI SSC Virtualization Guidelines list 11 factors for consideration. A few examples of the factors are:

- **Vulnerabilities** in the physical environment apply in a virtual environment
- **Information leakage** between virtual components
- **More than one function** per physical system
- **Maturity** of monitoring solutions
- **Lack of** separation of duties

Whilst not a definitive list, it provides a starting point for understanding the concerns of the PCI SSC regarding virtualisation technologies. The PCI SSC includes various recommendations for controls and best practices that should facilitate PCI DSS compliance. The recommendations include:

- **Evaluate** risks associated with virtual technologies
- **Restrict** physical access
- **Implement** defence in depth
- **Isolate** security functions
- **Enforce** least privilege and separation of duties

The PCI SSC Virtualization Guidelines also include barriers to security that cloud computing introduces. A few examples of the barriers are:

- The distributed architecture of cloud environments adds layers of technology and complexity to the environment.
- Public cloud environments are designed to be public Internet facing.
- The infrastructure can be dynamic and boundaries between tenant environments may be fluid.
- The hosted entity has limited or no visibility into the underlying infrastructure and related security controls.

Although all the factors, recommendations and barriers included in the Guidelines are valid, there are repetitions that could be consolidated. Table 1 summarises the PCI SSC's areas of concern and places them into categories that encompass the individual factors, recommendations and barriers.

As the risk assessment shown in Table 1 should be included as part of an Integrated Safety Management System (ISMS), all of the concerns behind the headings listed in **TABLE 1** could be consolidated into the four groups:

- Hypervisor architecture and security controls
- Physical security
- Monitoring and audit
- ISMS and governance

The considerations for the two groups of physical security and ISMS and governance would be the same for virtualised and non-virtualised envi-

TABLE 1.
Categorising of the Factors and Recommendations of the PCI SSC

PCI DSS VIRTUALIZATION GUIDELINES	PROPOSED CATEGORIES
The 11 factors can be categorised into four groups:	• Hypervisor architecture and security controls • Physical security • Monitoring and audit • Information Security Management System and governance
The general recommendations which are virtualisation specific can be categorised into three groups:	• Hypervisor architecture and security controls • Monitoring and audit • Risk assessment
The recommendation for mixed mode environments can be categorised as:	• Hypervisor architecture and security controls
The recommendations for cloud computing environments can be categorised into three groups:	• Hypervisor architecture and security controls • Monitoring and audit • Risk assessment

ronments hosting a CDE. Whilst monitoring and audit also apply to both environments there are additional considerations for virtualised environments due to the shared hosting environment. Hypervisor architecture and security controls would only apply to virtualised environments. So, for a virtualised environment to comply with the PCI DSS, it is the two groups of the hypervisor architecture and security controls, and the monitoring and audit capabilities which must provide sufficient controls to meet the PCI DSS requirements. We will look at these two categories next.

HYPERVISOR ARCHITECTURE AND SECURITY CONTROLS

There are two types of hypervisors. A type I hypervisor is installed directly onto the hardware and is known as a bare metal hypervisor. A type II hypervisor is installed over an operating system which provides the interface to the hardware. Type I hypervisors have significant advantages over type II, namely:

- No performance degradation from running through a host operating system
- No threat of associated vulnerabilities in the hosting operating system

- Simpler design with only the running of VMs to consider

Let us consider the VMware ESXi as a case study to illustrate the security controls available within hypervisor technologies. ESXi is a type I hypervisor. From a security perspective, it has three major components:

- The virtualisation layer
- Virtual machines
- The virtual networking layer

The virtualisation layer is designed to run virtual machines (VMs). The VMkernel acts as a bridge between the hardware resources and the VMs. Isolation between the VMkernel and VMs is possible by utilising the security capabilities presented by CPU hardware, paging and ring architectures.

Labo. Ur, ommodiorum quis verero tenempostet fugiand igent, quaecusam iumet apelit et reperoresto quidelit et re iundae quiaestiat es nonsecae labo. Iliquia

The physical memory of the host system is used by all VMs. It is imperative that sufficient controls are in place to prevent attacks on the cardholder data being stored in memory. In a virtualised system, the guest operating system maintains page tables just as the operating system in a native system does. In addition, the VM monitor (VMM) maintains an additional layer of mapping. This is the mapping of VM physical page numbers to host hypervisor physical page numbers. Because of the extra level of memory mapping introduced by virtualisation, the VMkernel can effectively manage memory presented across all VMs. ESXi also utilises Intel XD and AMD NX support to mark writeable areas of memory as non-executable.

The virtual network security architecture is controlled by the VMkernel. Just as the VMkernel prevents VM's from directly communicating, it also provides network isolation. The VMkernel also provides the bridge between the hardware resources and the vSwitch, which is a component that manages the virtual network connecting together various VMs and the outside world. A virtual switch, by design, cannot leak packets directly to another virtual switch. The only way for packets to travel from one virtual switch to another is under the following circumstances:

- The virtual switches are connected to the same physical LAN.
- The virtual switches connect to a common VM, which could be used to transmit packets.

To verify that no common virtual switch paths exist, it is possible to check for shared points of contact by reviewing the network switch layout in the vSphere Client.

MONITORING AND AUDIT CAPABILITIES

Most hypervisors will support logging to a syslog server and Simple Network Management Protocol (SNMP) traps. In addition to syslog and SNMP services, ESXi provides an additional interface for third party agents that use the following protocols:

- Common Information Model Extensible Mark-up Language (CIM XML)
- Web Services for Management (WSMAN)

These management services provide the interfaces to obtain the required monitoring and audit information.

So it seems that the basic concerns of the PCI SSC regarding virtualisation can be addressed within ESXi, providing ESXi itself can be trusted. The Common Criteria provide an internationally recognised model for the evaluation of products. The highest level usually attained by commercial products is known as EAL4. ESXi has passed evaluation at the EAL 4+ level of assurance. So some trust can be placed in ESXi.

Further trust of the hosting virtualisation system can be achieved by the use of Trusted Platform Module (TPM) technology to protect the VMkernel from tampering and corruption. Trust implies that an entity will always behave in the expected manner for its intended purpose. This means that if a known entity is operating and the properties of the entity are known, the party relying on that entity can make an informed decision whether to trust the entity. The role of the trusted platform is always to work in the same way and to report the status of the platform accurately.

The Trusted Computing Group (TCG) provides the specifications for the Trusted Platform Module (TPM). The TPM is a computer chip that can securely store authentication data (such as passwords, certificates, and encryption keys) and Platform measurements (that help ensure that the platform remains trustworthy). The TPM can be used with Intel Trusted

eXecution Technology (TXT) to provide an accurate comparison of all the critical elements of a system's launch environment against a known good source. TXT creates a cryptographically unique identifier for each approved launch-enabled component of ESXi. This is stored within the TPM. TXT then uses hardware-based enforcement mechanisms to block the launch of any code that does not match the approved code.

Thus, systems hosting the CDE can offer a greater level of protection when using TPM and TXT technologies to provide attestation of the integrity of the VMkernel and the VMs.

With a correctly configured host system and CDE it should therefore be possible to achieve PCI DSS compliance in a cloud environment. This would be further facilitated if the service provider offered the cloud service only to applications and systems that were also configured to a level of security with at least the equivalent of that required by the PCI SSC.

However, whilst it might be possible to achieve PCI DSS compliance in a cloud-hosted environment, in most cases it seems to be impractical and not cost effective. The reasons include, but are not limited, to:

- The additional controls and applications would require expert security knowledge and support
- The extra key management and logging networks will also require bandwidth and additional processing power for the encryption services protecting the network traffic
- The problems with agreeing about liability and the cost of proving the party at fault in the case of unauthorised disclosure

There are further concerns that are not limited to payment card data, but to any data that requires protection whilst hosted in the cloud. Among these are:

- Departments and overzealous staff may become frustrated with internal IT services and independently move data or applications to a cloud service
- A thorough investigation and risk analysis of a cloud service would need to be performed to understand:
  - The cloud service environment
  - The security controls of the hosting platform

- The scope of any audits or certifications (such as ISO 27001 or SAS70)
- The reliability of the company and staff

- The integrity of audit logs is still not guaranteed

In conclusion, if an organisation were considering cloud services to host a PCI DSS compliant e-commerce solution, a hybrid system seems best. Specifically, this hybrid system would use cloud services for the web services but a dedicated service for payment processing which is, for example:

- Privately hosted by the merchant, or
- Hosted by a third party, or
- Provided by a payment service such as PayPal. ■

ABOUT THE AUTHORS:

Patrick Durkin has worked within the information security industry for the past 15 years. He specialises in information security consultancy and the delivery of security enterprise architecture solutions. After completing his MSc at Royal Holloway in 2011, he joined the HP ESS Security Architecture and Cyber Practice.

Geraint Price is a lecturer in information security at Royal Holloway. His research interests include secure protocols, public key infrastructures, denial of service attacks and resilient security.