



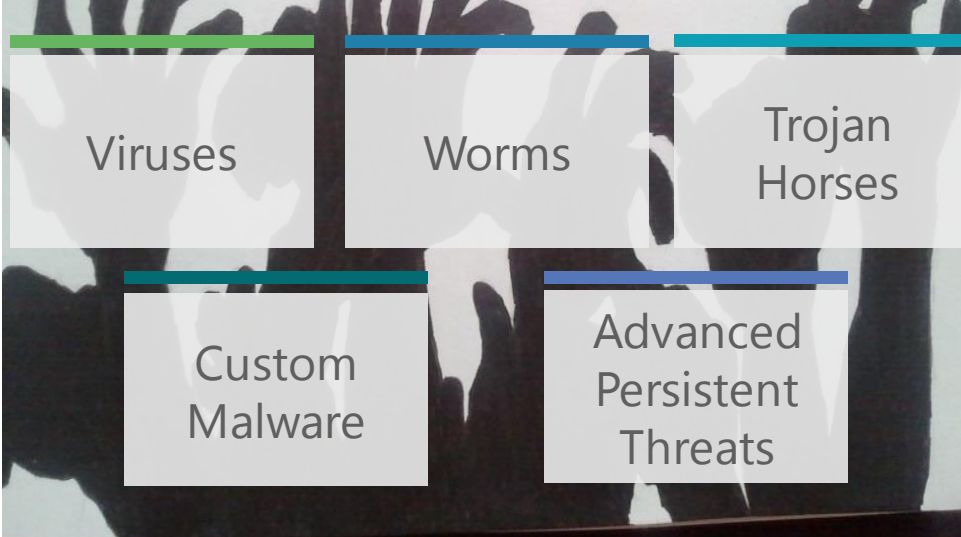
Business training is all about ways you can get involved with the Council to help influence the industry.

## Update from the PCI Security Standards Council

Troy Leach, CTO, PCI Security Standards Council



# Evolution of Cyber Attacks



- Viruses
- Worms
- Trojan Horses
- Custom Malware
- Advanced Persistent Threats

# Modern Malware Hides Itself



Guiding open standards for global payment card security

## Top Mistakes Revealed by Forensic Audits

<p><i>Weak or default passwords</i></p> 	 <p><i>Lack of employee education</i></p>
<p><i>Security deficiencies introduced by third parties</i></p> 	 <p><i>Slow self-detection</i></p>

Source: 2013 Trustwave Global Security Report



Guiding open standards for global payment card security

## A Multi-layered Approach is Needed



Guiding open standards for global payment card security

## PCI Standards are the Foundation

*With version 3.0, PCI DSS is more mature than ever, and covers a broad base of technologies and processes such as encryption, access control, and vulnerability scanning to offer a sound baseline of security.*

*PCI DSS has made comprehensive security controls more commonplace in larger organizations. Therefore, the organizations become more difficult to compromise.*

Source: 2013 Trustwave Global Security Report



VERIZON 2014  
PCI COMPLIANCE  
REPORT



Guiding open standards for global payment card security

## PCI DSS, PA-DSS 3.0 – Key Themes

**Education Awareness**

**Flexibility**

**Security as a Shared Responsibility**

Make PCI your compass, not your roadmap



Guiding open standards for global payment card security

*At a Glance...*

- 12 core security principles of PCI DSS remain the same
- Several new sub-requirements that will impact PCI DSS security efforts
- Future implementation dates provided for more significant changes
- Clarified PCI DSS Applicability
- Enhanced testing procedures to clarify level of validation expected for each requirement
- Aligned language between requirements and testing procedures for consistency
- Instructions for Report on Compliance (ROC) reporting now separate ROC reporting template

## Maintaining Compliance

### Best Practices for Implementing PCI DSS to Stay Secure

- Focus on security not compliance
- PCI DSS is not a once-a-year activity
- Don't forget about people



Guiding open standards for global payment card security

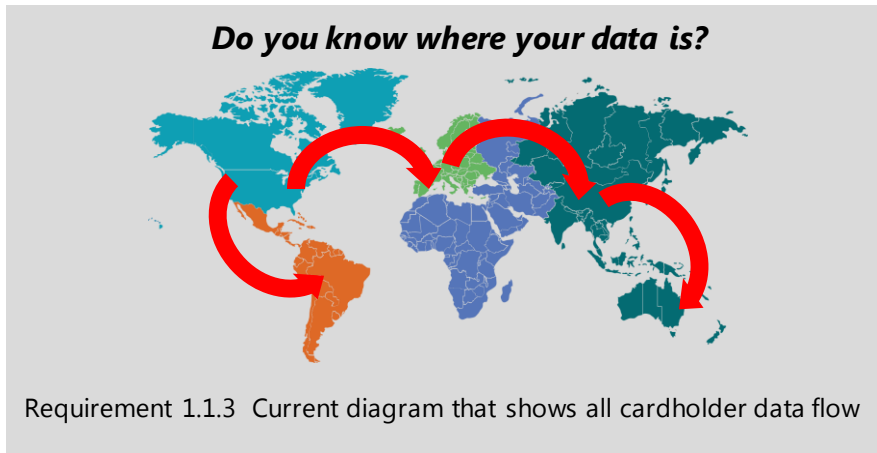
## Understanding Intent of Requirements

PCI DSS Requirements	Testing Procedures	Guidance
1.1.2 Current diagram that identifies all networks, network devices, and system components, with all connections between the CDE and other networks, including any wireless networks	<p>1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.</p> <p>1.1.2.b Interview responsible personnel to verify that the diagram is kept current.</p>	<p>Network diagrams describe how networks are configured, and identify the location of all network devices.</p> <p>Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.</p>
1.1.3 Current diagram that shows all	1.1.3.a Examine data-flow diagram and interview personnel to	Cardholder data-flow diagrams identify the location



Guiding open standards for global payment card security

## Impactful Changes – Requirement 1.1.3



Guiding open standards for global payment card security

## Physical Security for POS Devices



### 9.9 Protect devices that capture payment card data from tampering and substitution

- Maintain an up-to-date list of devices
- Periodically inspect device surfaces to detect tampering or substitution
- Provide training for personnel to be aware of attempted tampering or replacement of devices



Guiding open standards for global payment card security



## Penetration Testing and Effective Scoping



- 11.3** Implement a penetration testing methodology
- 11.3.4** If segmentation is used, perform penetration tests to verify that the segmentation methods are operational and effective.



Guiding open standards for global payment card security

## Security as a Shared Responsibility

<b>Guidance</b>	<ul style="list-style-type: none"> <li>• Outsourcing PCI DSS responsibilities</li> </ul>
<b>Requirement 8</b>	<ul style="list-style-type: none"> <li>• Service providers use unique credential per customer</li> </ul>
<b>Requirement 12</b>	<ul style="list-style-type: none"> <li>• Service providers acknowledge responsibility</li> </ul>



Guiding open standards for global payment card security

## Service Provider Requirements

- Maintain program to monitor Service Providers PCI DSS status
- Maintain which requirements are managed by each service provider
- Service provider acknowledges in writing their responsibility to protect cardholder data



Guiding open standards for global payment card security

## Important Dates for v3.0 PCI DSS

Version 3.0 was effective on 1 January 2014

Version 2.0 is valid until 31 December 2014

Check our website for SAQs, FAQs, Prioritized Approach

Feedback period kicks off at Community Meetings

**Do not mix and match**



Guiding open standards for global payment card security



## ***Technology and Emerging Payments***

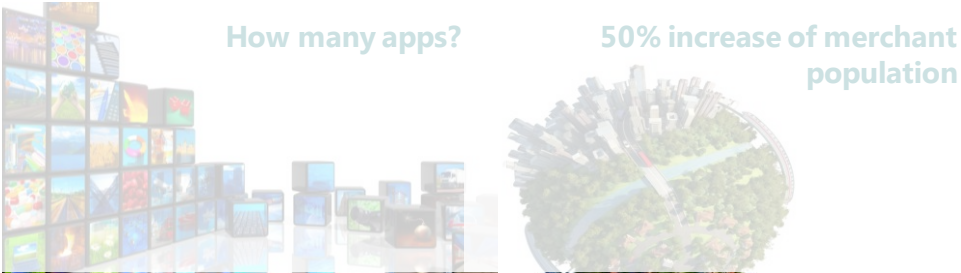
Cloud computing reduces total cost of ownership but at what expense?

Mobile provides new payment alternatives but is it 'smart'?

New technology emerging to remove sensitive data



# Market Today



**PCI** Security Standards Council  
Guiding open standards for global payment card security

# Mobile Payment Acceptance

- PCI Standards focus on merchant-acceptance
- Mobile payment acceptance still evolving
- Understand risk and use PCI SSC resources



**PCI** Security Standards Council  
Guiding open standards for global payment card security

## Mobile Guidelines and Best Practices



### Guidelines published 2012-2013

- PCI Mobile Payment Acceptance Guidelines for Developers
- PCI Mobile Payment Acceptance Guidelines for Merchants as End-Users
- Accepting Mobile Payments with a Smartphone or Tablet



Guiding open standards for global payment card security

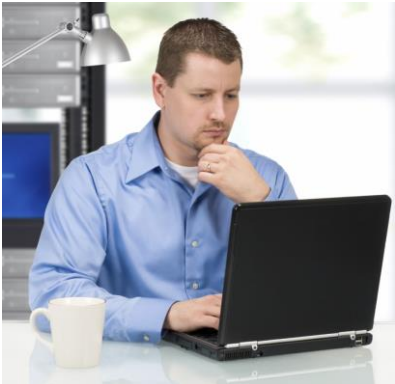
## Why Mobile Guidance, Not Standards



Guiding open standards for global payment card security



*Shared Responsibility*

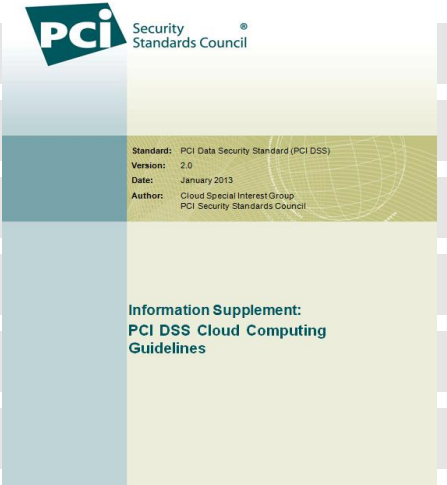


Cloud provider



Cloud customer (client)

## Cloud Computing Guidelines

Different cloud types	
Role of cloud customers and providers	
Considerations for PCI DSS	
Scoping and segmentation	
Compliance Challenges	
Risks and Security Challenges	



Guiding open standards for global payment card security

## Key Recommendations

-  Cloud computing is still evolving and is yet to be standardized
-  Outsourcing management of security controls does not equate to outsourcing of PCI DSS responsibility
-  Understand scope for both parties
-  Due diligence, contractual agreements (SLAs), and ongoing monitoring are critical



Guiding open standards for global payment card security

# Where the Footprint Begins



**66% of data breaches, the organization didn't know the data was on the compromised system**  
VERIZON DATA BREACH INVESTIGATIONS REPORT



Guiding open standards for global payment card security

# Ways to Reduce the Footprint

**Reduce the need or ability to store or transmit cardholder data**



Business process for retention



P2PE



Tokenization



Standards for global payment card security



# EMV Chip Helps Reduce Face-to- Face Fraud



## Even **EMV Chip** Needs PCI

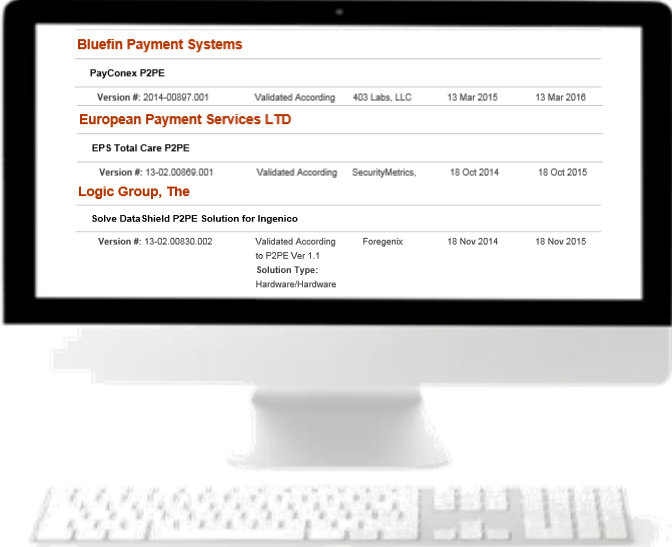


# Terminal Security



Guiding open standards for global payment card security

# Point-to-Point Encryption



Bluefin Payment Systems				
<b>PayConex P2PE</b>				
Version #:	2014-00897.001	Validated According	403 Labs, LLC	13 Mar 2015 13 Mar 2016
<b>European Payment Services LTD</b>				
<b>EPS Total Care P2PE</b>				
Version #:	13-02.00869.001	Validated According	SecurityMetrics,	18 Oct 2014 18 Oct 2015
<b>Logic Group, The</b>				
<b>Solve DataShield P2PE Solution for Ingenico</b>				
Version #:	13-02.00830.002	Validated According to P2PE Ver 1.1	Foregenix	18 Nov 2014 18 Nov 2015
		Solution Type:	Hardware/Hardware	



Guiding open standards for global payment card security

### *What is a PCI P2PE Solution?*

PCI PTS approved devices with SRED

PCI P2PE validated applications and processes

Listed by PCI SSC

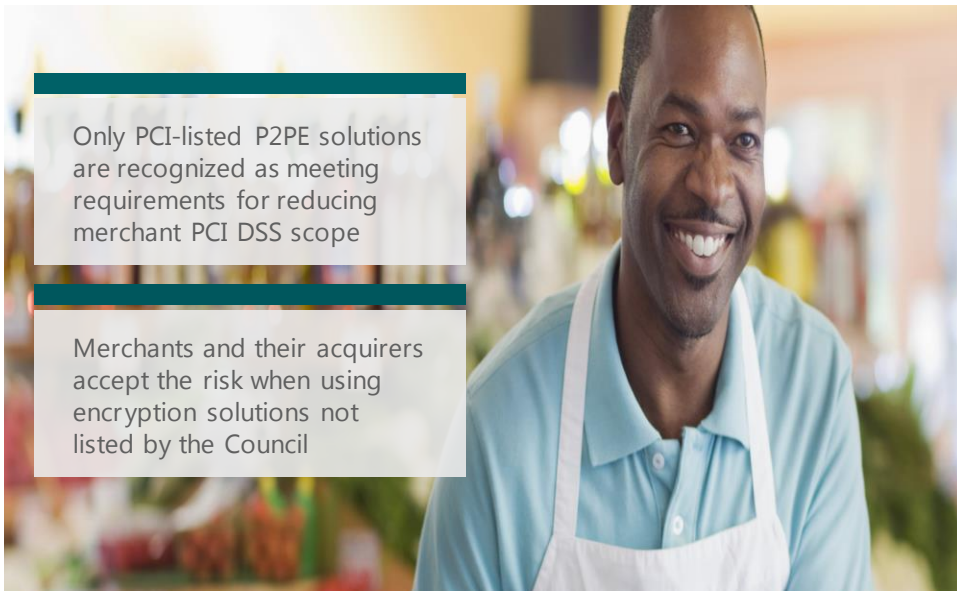


Guiding open standards for global payment card security

## *P2PE and Merchants*

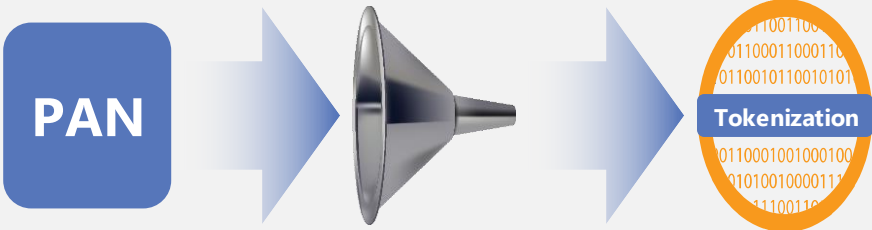
Only PCI-listed P2PE solutions are recognized as meeting requirements for reducing merchant PCI DSS scope

Merchants and their acquirers accept the risk when using encryption solutions not listed by the Council



# Tokenization

**Work on tokenization standards has begun**



Guiding open standards for global payment card security

# The Formula for PCI Success



Guiding open standards for global payment card security

*Questions?*



Security Standards Council®



**Please visit our website at  
[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)**



Guiding open standards for global payment card security