New PCI DSS Version 3.0: Can it Reduce Breaches?

Dharshan Shanthamurthy, **CEO**, SISA Information Security Inc.

Core Competencies – C11

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

SISA Information Security

Formal Risk Assessment Specialists

- Authors of PCI Risk Assessment Guidance Document
- PCI Qualified Security Assessor (PCI QSA)
- Payment Application Qualified Security Assessor (PAQSA)
- Point to Point Encryption Encryption (P2PE QSA)
- Payment Forensics Investigator (PFI)
- Securing organizations in over 30 countries

www.sisainfosec.com

Dharshan Shanthamurthy

CISA, CISSP, PCI QSA, PA-QSA

- Lead and Proposer for the PCI Risk Assessment Guidance Document
- Amongst the first PCI Qualified Security Assessors of the PCI Council
- OCTAVE Authorized Trainer from Software Engineering Institute, Carnegie Mellon University

2014 Fall Conference - "Think Big"

Session Objective

- Payment Card Industry Ecosystem
- Frauds/Breaches
- Understand the PCI DSS Version 3.0
- Solution to Breaches – PCI DSS Formal Risk Assessment

Mode: Interactive (so please ask feel free to ask questions as I speak)

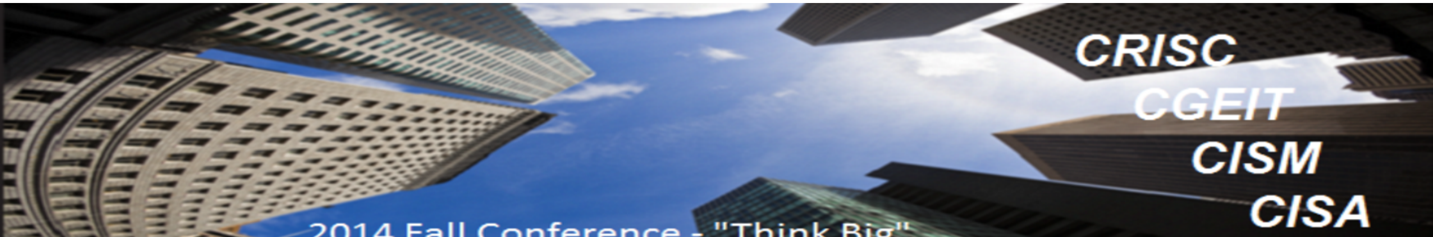
PAYMENT CARD INDUSTRY (PCI) ECOSYSTEM

Some Facts

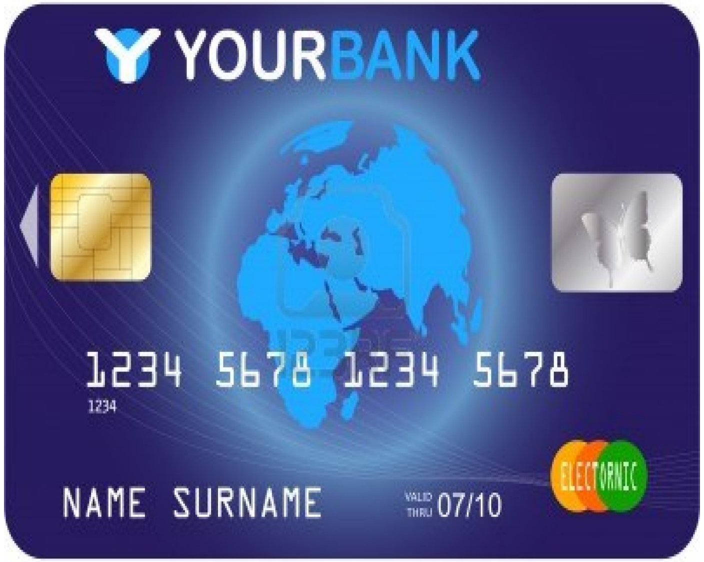
NUMBER OF CARD TRANSACTIONS – **10,000** TRANSACTIONS PER SECOND

NUMBER OF NON CASH PAYMENTS IN 2013 – **333 BILLION**
CARD PAYMENTS – 181 BILLION

IF EACH OF THE 7 BILLION ON THE PLANET HAD A CARD THEY WOULD HAVE USED IT ATLEAST **19 TIMES**



The Protagonist



Primary Account Number PAN

EMV CHIP

HOLOGRAM

CARDHOLDER NAME

EXPIRY DATE

PAYMENT BRAND LOGO

TRACK and CHIP

- Track 1 Data
- Track 2 Data

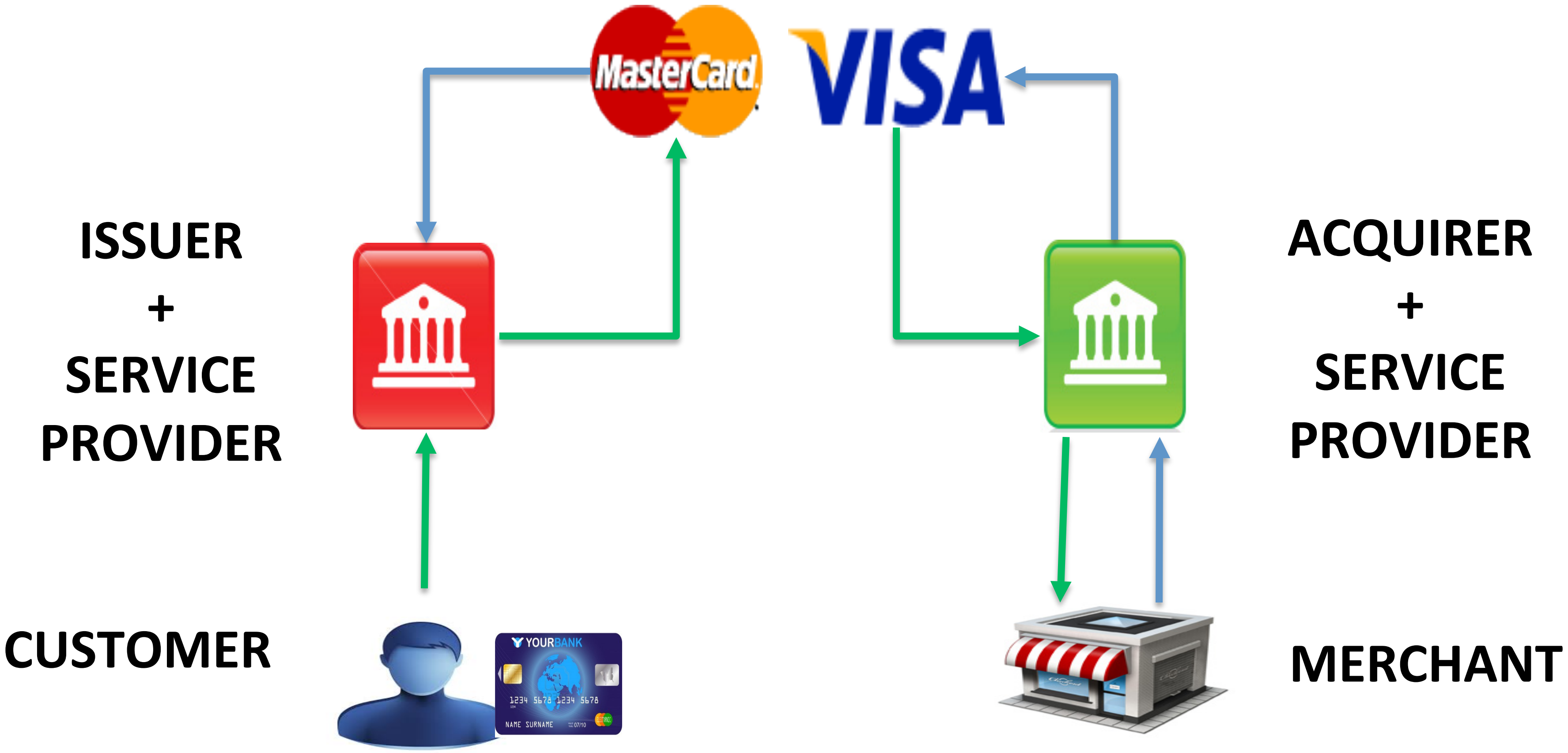
Only Track 2 is used for financial transactions

- Added Security Measures
- Whole lot of banking features

The Who is Who

PAYMENT BRANDS	MasterCard VISA AMERICAN EXPRESS JCB DISCOVER NETWORK
BANKS	citi Bank of America RBS The Royal Bank of Scotland CHASE
MERCHANTS	Google play STARBUCKS COFFEE® BEST BUY ebay™
SERVICE PROVIDERS	Google wallet PayPal™ amazon webservices™ MasterCard Worldwide MIGS

Transactions – Card Present



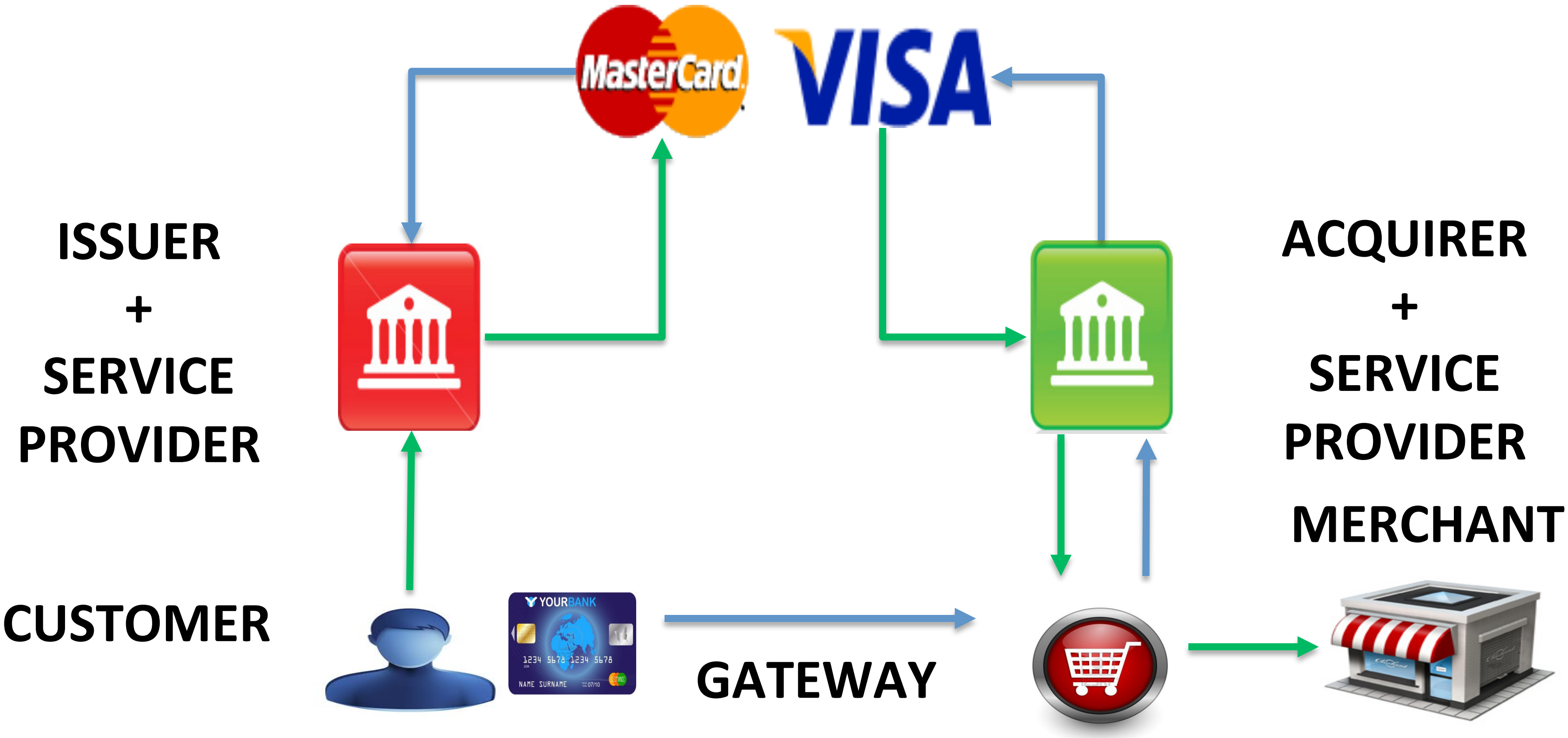
ISSUER
+
SERVICE
PROVIDER

ACQUIRER
+
SERVICE
PROVIDER

CUSTOMER

MERCHANT

Transactions – Card Not Present



ISSUER + SERVICE PROVIDER

ACQUIRER + SERVICE PROVIDER

MERCHANT

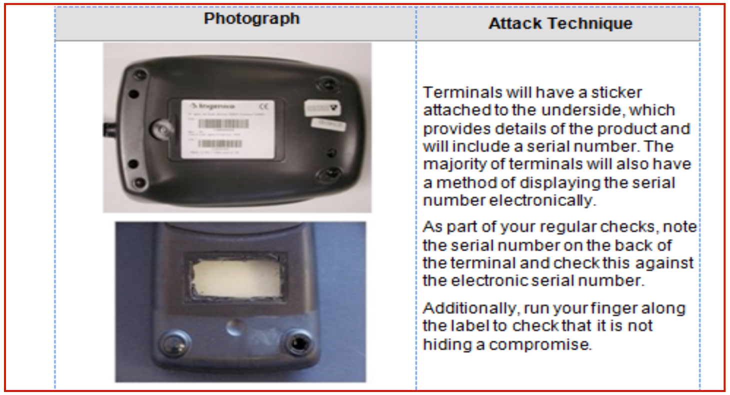
CUSTOMER

GATEWAY

TOP INHIBITIONS FOR USING CARDS

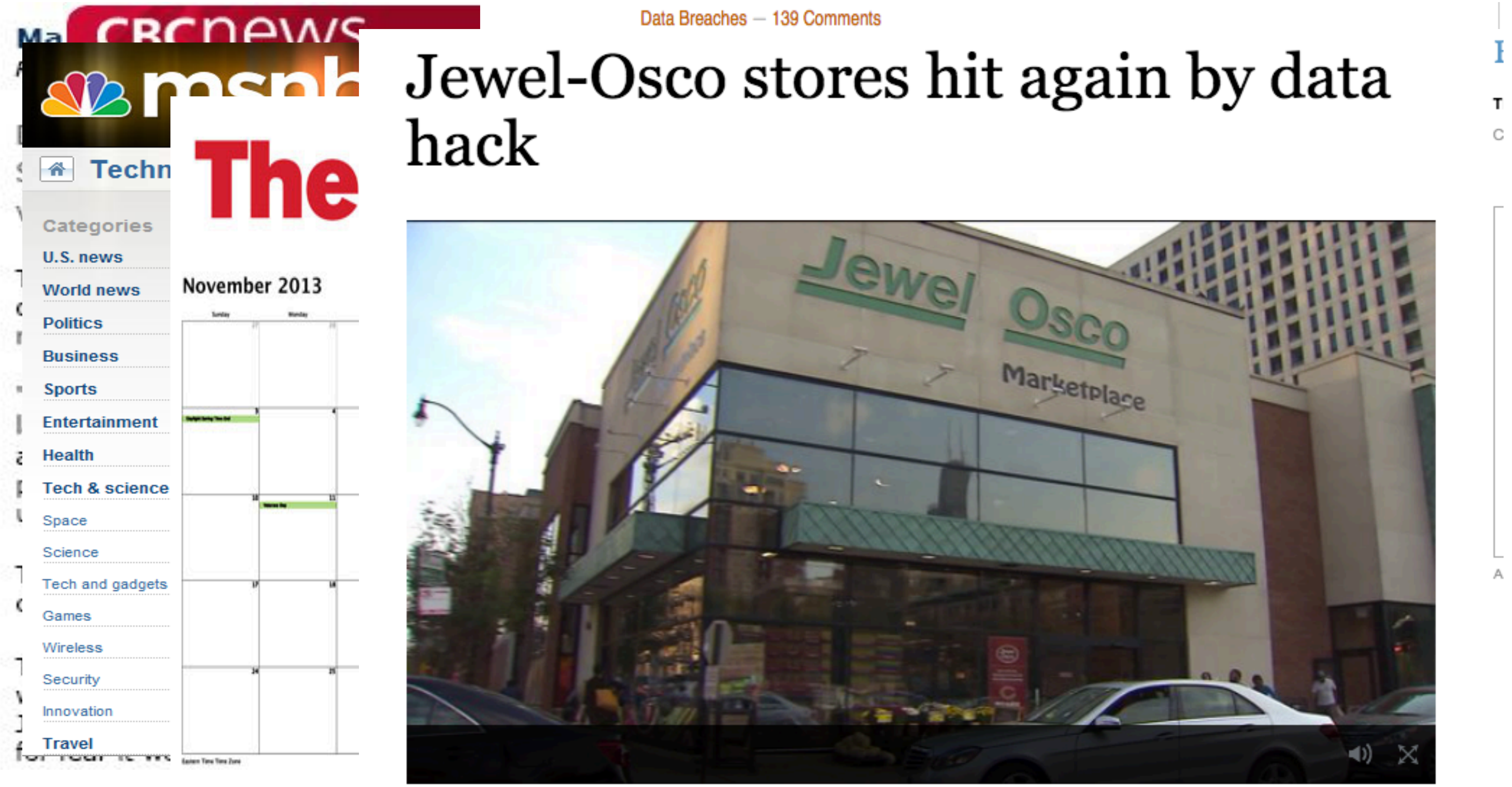
Payment Card Fraud Evolution

1983	Re-embossed counterfeit fraud
1988	Re-encoded counterfeit fraud
1989	Card not present fraud/ fraud applications
1991	Never received issued fraud
1992	Merchant fraud
1994	Identity Theft
2000	Skimmed counterfeit
2002	Communications interception
2007	Wireless/ Chip sniffing and card counterfeit/ Fake terminals
2010-14	Server Hacking/Malware/Memory Scrapping



Photograph	Attack Technique
	Terminals will have a sticker attached to the underside, which provides details of the product and will include a serial number. The majority of terminals will also have a method of displaying the serial number electronically. As part of your regular checks, note the serial number on the back of the terminal and check this against the electronic serial number. Additionally, run your finger along the label to check that it is not hiding a compromise.

Today’s Risks



Categories
- U.S. news
- World news
- Politics
- Business
- Sports
- Entertainment
- Health
- Tech & science
- Space
- Science
- Tech and gadgets
- Games
- Wireless
- Security
- Innovation
- Travel

November 2013

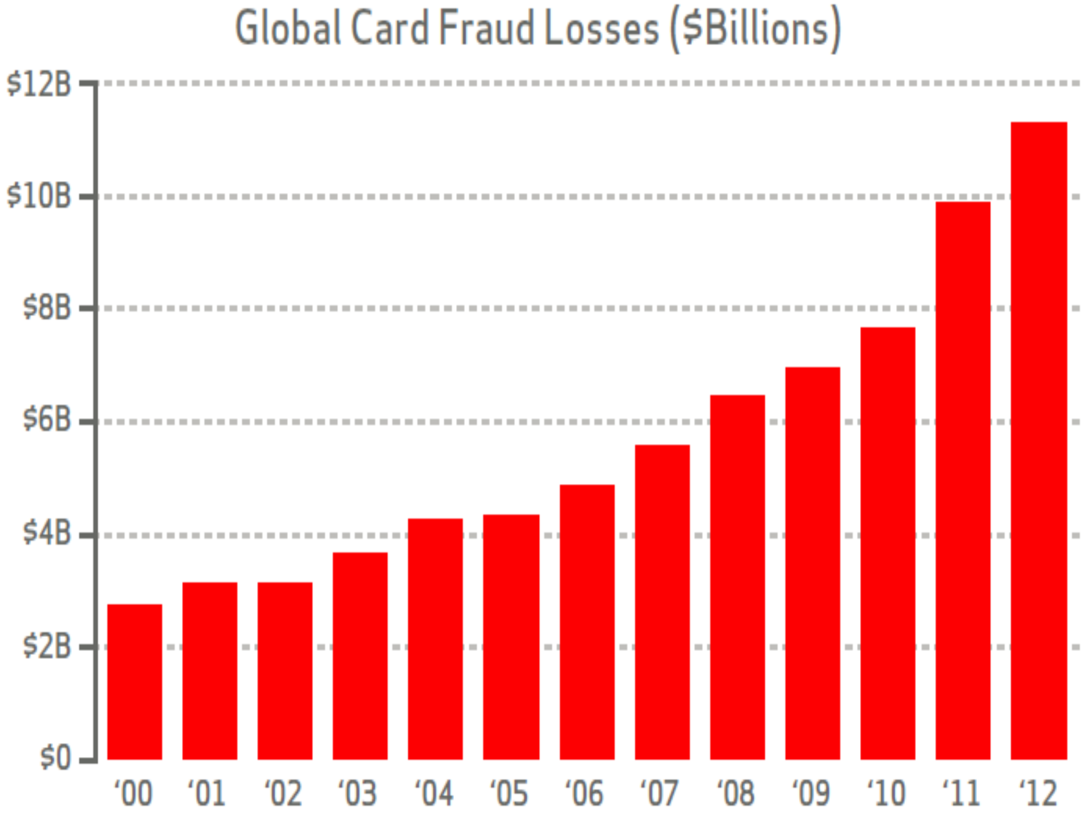
Data Breaches — 139 Comments

Jewel-Osco stores hit again by data hack

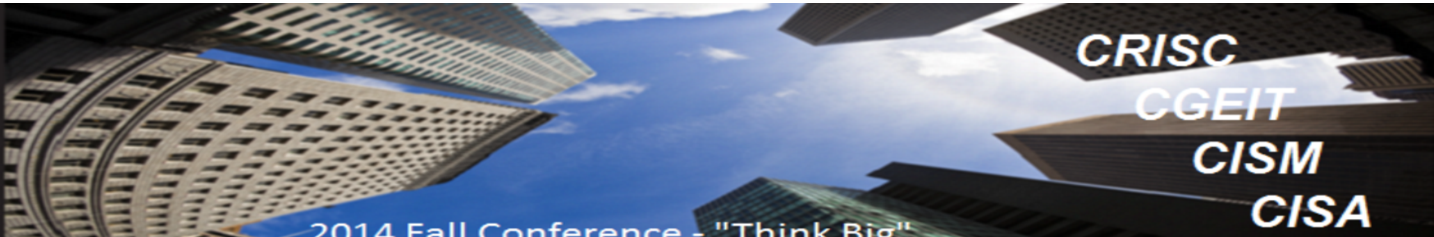
What is at Stake

It's been estimated that 70% of attacks are on small businesses[1], and that more than 40% of customers who have been victims of fraud stop doing business with the merchant where the fraud occurred[2]. 60% of small businesses breached close within six months[3].

1. 2012 Verizon Data Breach Investigations Report
2. Javelin Strategy and Research, June 2009
3. Symantec 2013 Internet Security Report


Global Card Fraud Losses ($Billions)

PAYMENT CARD INDUSTRY DATA SECUIRTY STANDARD (PCI –DSS) VERSION 3.0



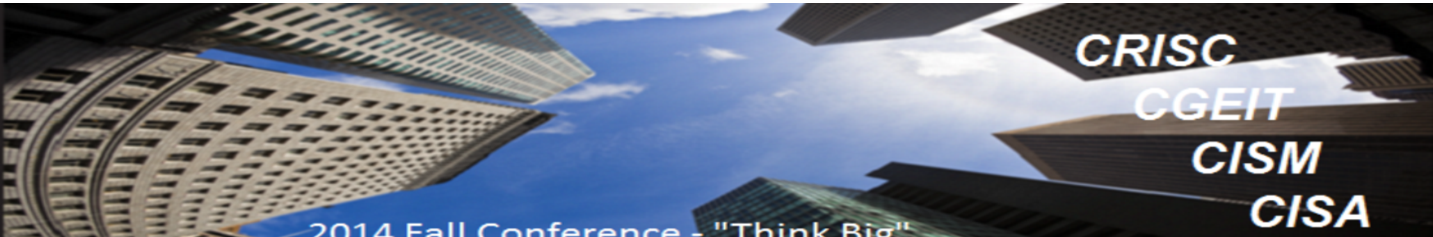
Do I need PCI DSS?

PCI-DSS Compliance applies to any entity that

- **Stores** Card Holder Data
- **Processes** Card Holder Data
- **Transmits** Card Holder Data

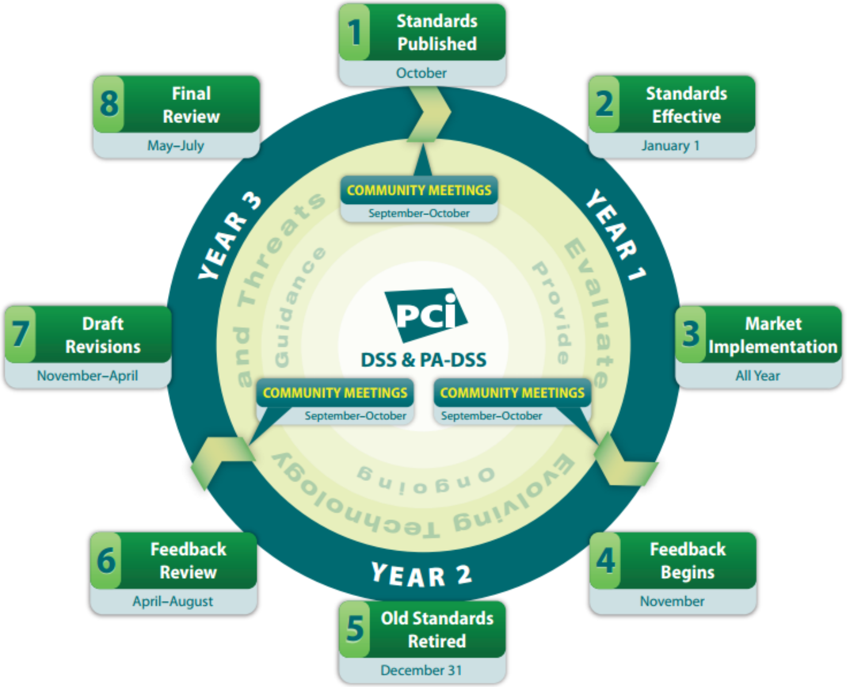
Account Data consists of cardholder data and sensitive authentication data

- **Entities** include, but not limited to:
  - **Merchants**
  - **Acquirers**
  - **Issuers**
  - **Service Providers**
  - **Trusted Third Parties**

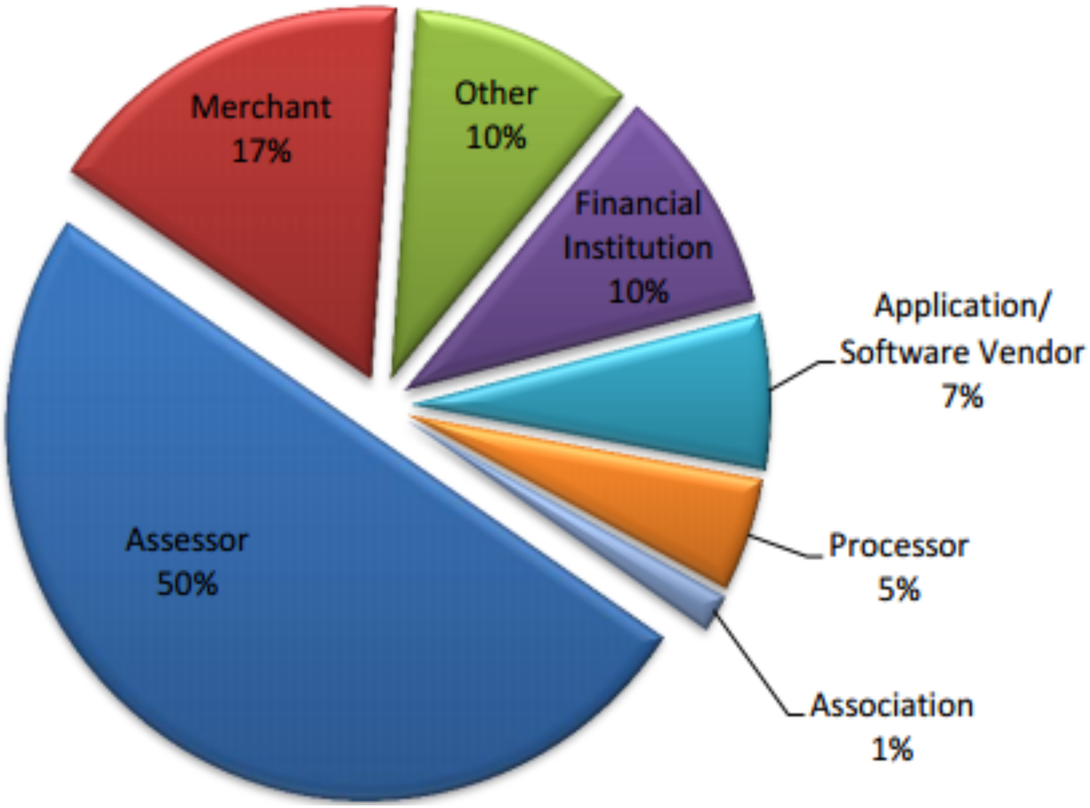


3 YEAR LIFE CYCLE

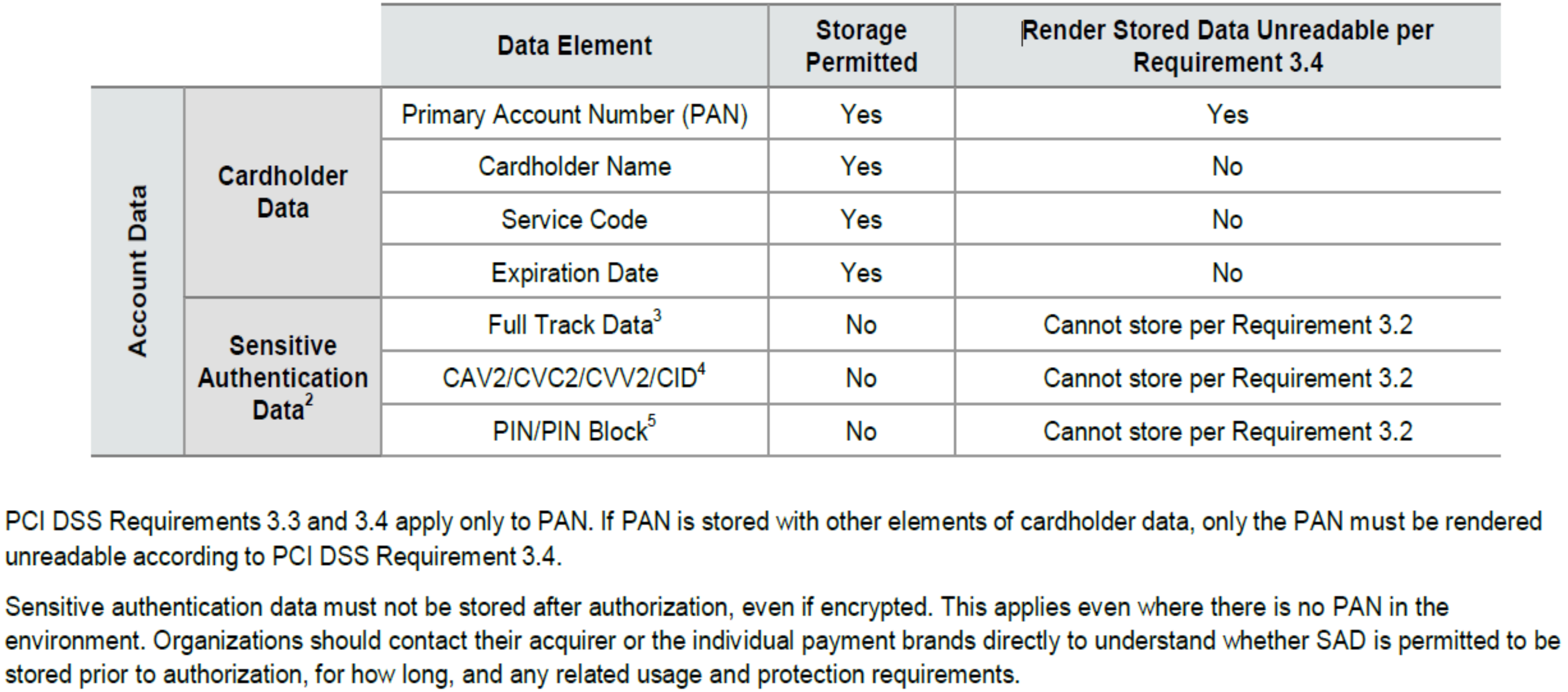
PCI Security Standards Council™



Feedback on v2.0



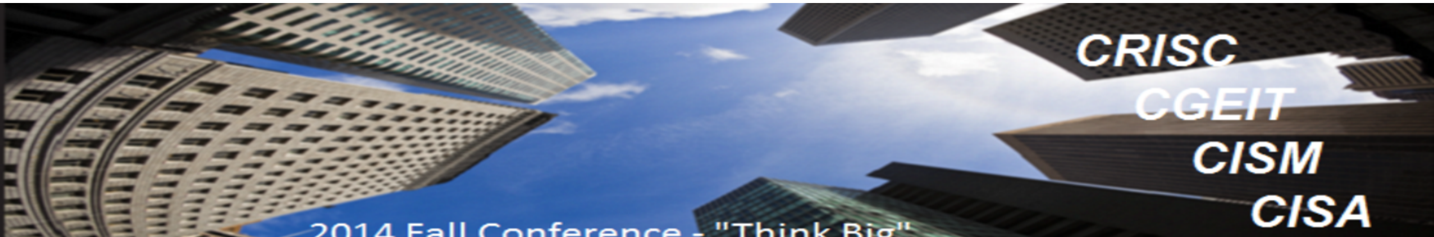
The most important slide



		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[2]	Full Track Data[3]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID[4]	No	Cannot store per Requirement 3.2
		PIN/PIN Block[5]	No	Cannot store per Requirement 3.2

PCI DSS Requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

Sensitive authentication data must not be stored after authorization, even if encrypted. This applies even where there is no PAN in the environment. Organizations should contact their acquirer or the individual payment brands directly to understand whether SAD is permitted to be stored prior to authorization, for how long, and any related usage and protection requirements.



Clarification on requirements

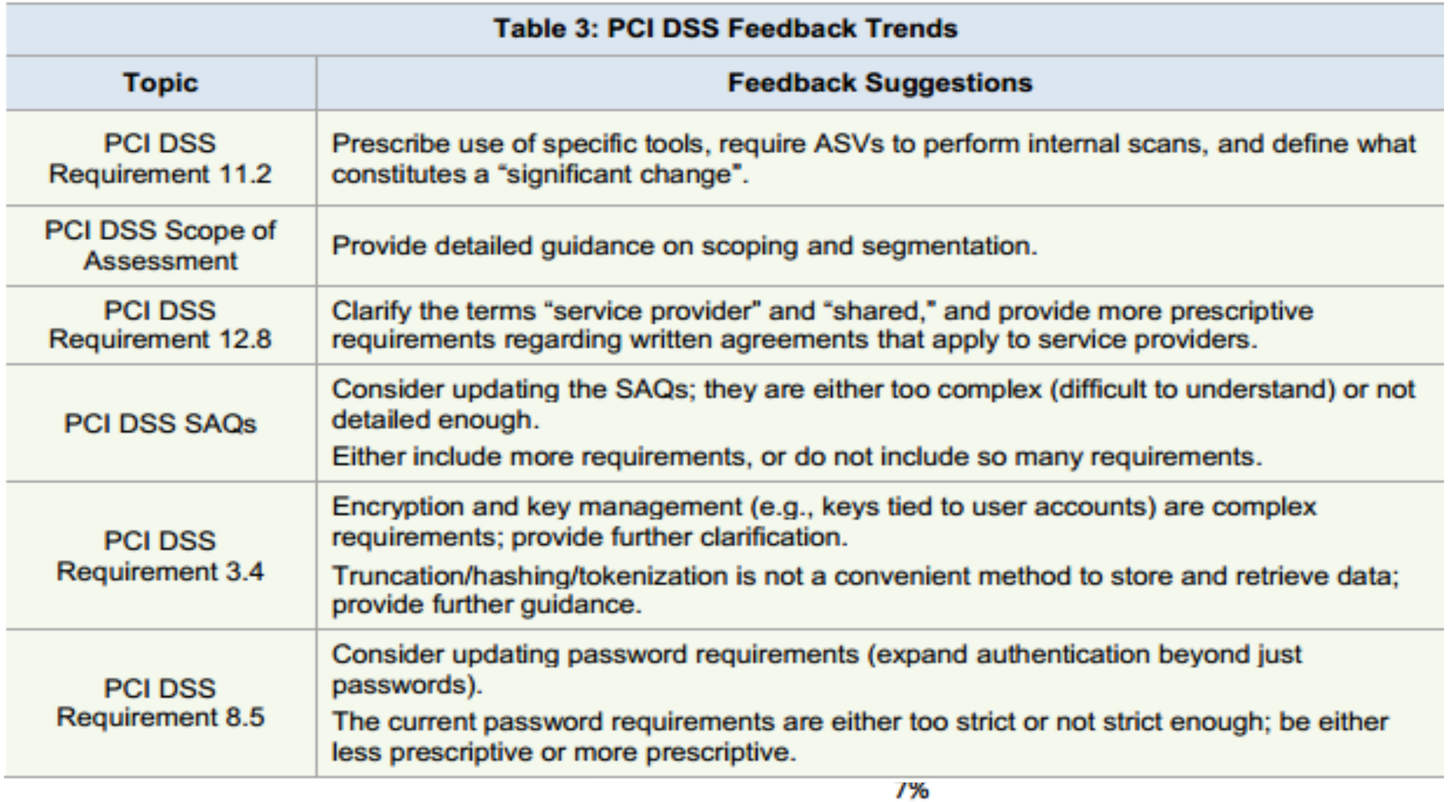
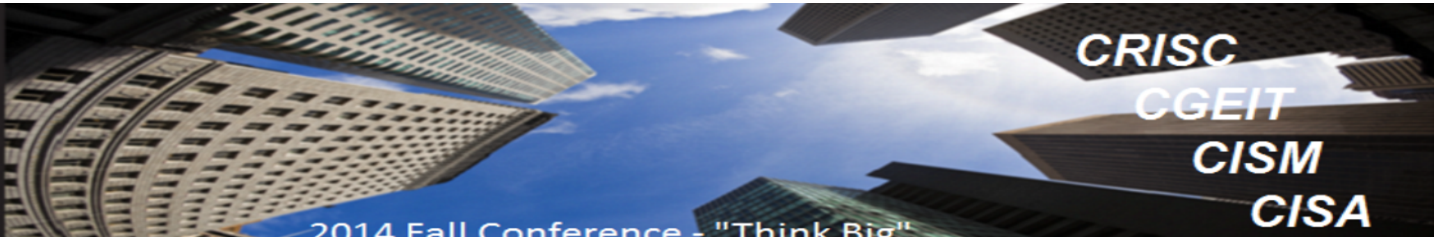


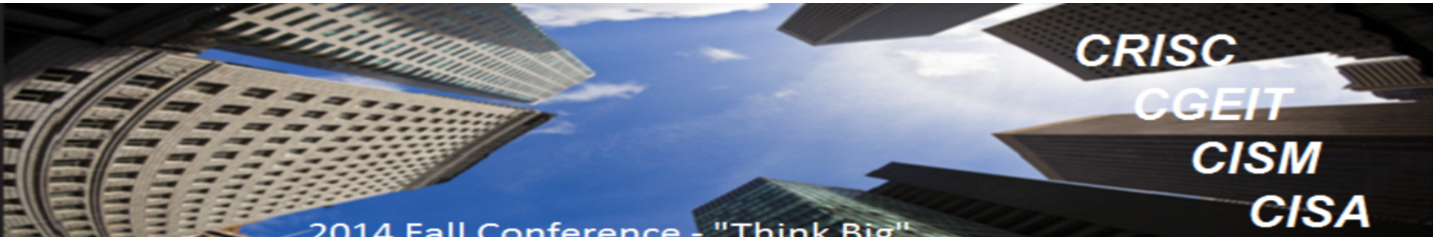
Table 3: PCI DSS Feedback Trends	
Topic	**Feedback Suggestions**
PCI DSS Requirement 11.2	Prescribe use of specific tools, require ASVs to perform internal scans, and define what constitutes a "significant change".
PCI DSS Scope of Assessment	Provide detailed guidance on scoping and segmentation.
PCI DSS Requirement 12.8	Clarify the terms "service provider" and "shared," and provide more prescriptive requirements regarding written agreements that apply to service providers.
PCI DSS SAQs	Consider updating the SAQs; they are either too complex (difficult to understand) or not detailed enough. Either include more requirements, or do not include so many requirements.
PCI DSS Requirement 3.4	Encryption and key management (e.g., keys tied to user accounts) are complex requirements; provide further clarification. Truncation/hashing/tokenization is not a convenient method to store and retrieve data; provide further guidance.
PCI DSS Requirement 8.5	Consider updating password requirements (expand authentication beyond just passwords). The current password requirements are either too strict or not strict enough; be either less prescriptive or more prescriptive.

7%



12 requirements - What's New!

- Clarity and explanation of requirements
- More elaborate testing procedures for Assessors
- Updated section to focus on assessment process rather than documentation.
- Focus is on Security and not Just Compliance – through formal risk assessment

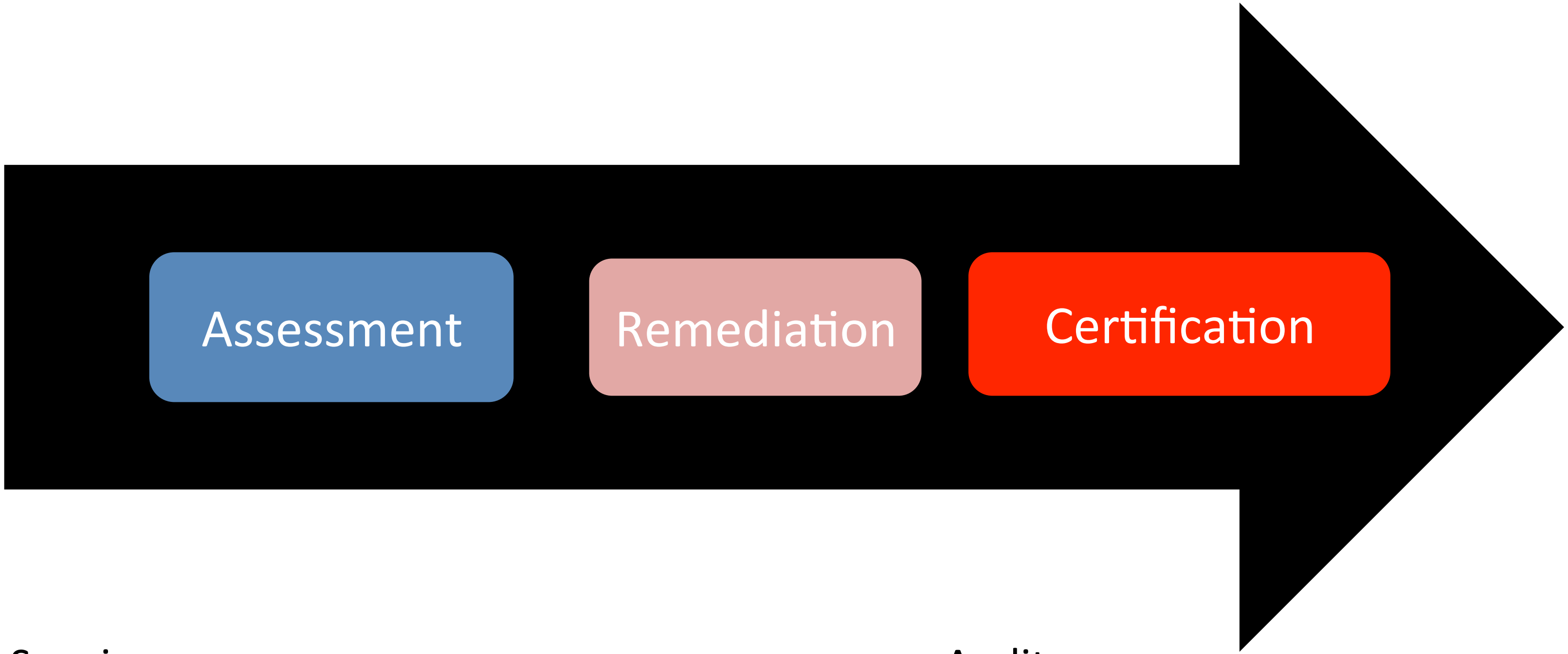


Scoping Segmentation and Sampling

- **Scope -** Any system component or device located within or connected to the Cardholder Data Environment.
- **Segmentation -** Segmentation is not filtering based on router/switch rules. It is actual isolation
- **Sampling –** Emphasis on ‘Representative Sampling’

SOLUTION for BREACHES –
PCI FORMAL RISK ASSESSSSMENT
(12.2 OF PCI VERSION 3.0)

PCI-DSS Certification



Assessment

Remediation

Certification

Scoping
PCI Risk Assessment
Gap Analysis

Mitigation
Milestone Reviews

Audit
Report on Compliance
Certificate of Compliance

Formal Risk Assessment

- Risk Assessment is a process of identifying all threats and vulnerabilities that affect the Cardholder Data Environment (CDE)
- Risk Assessment is mandatory as per Requirement 12.2
- Approved methodologies include ISO 27005, OCTAVE, NIST SP 800-30
- You need to identify all possible risk scenarios that affect the CDE.
- Take is Business As Usual activity and not a one time measure

Plan a Formal PCI Risk Assessment

- Asset is Cardholder data and systems components in CDE (cardholder data environment)
- Account Data identification
  - Cardholder data scanner
  - Dataflow Diagram
  - Identify all payment channels
  - Account Data Matrix
- Scoping and Network Segmentation
- Identify all the Risk Scenario which can impact confidentiality of the cardholder data and CDE
- Address the RISKs: 4T's (Treat, Tolerate, Transfer and Terminate)
- Document/Report

ISACA
Trust in, and value from, information systems
San Francisco Chapter
CRISC
CGEIT
CISM
CISA
2014 Fall Conference - "Think Big"

Scope

Asset

Threat

Vulnerabilities

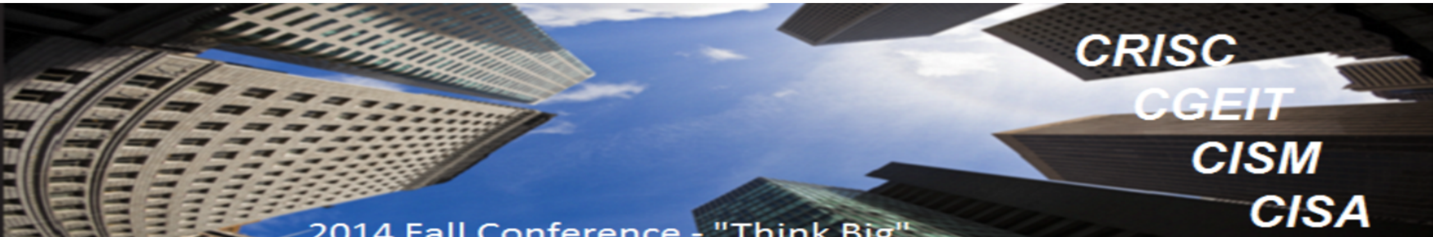
Risk Profiling

Risk Treatment Plan

Results Documentation

Scope

- **Physical Location – building, room, etc.**
- **Data Center**
- **Business Process**
- **Business Division**



Scope

Asset

Threat

Vulnerabilities

Risk Profiling

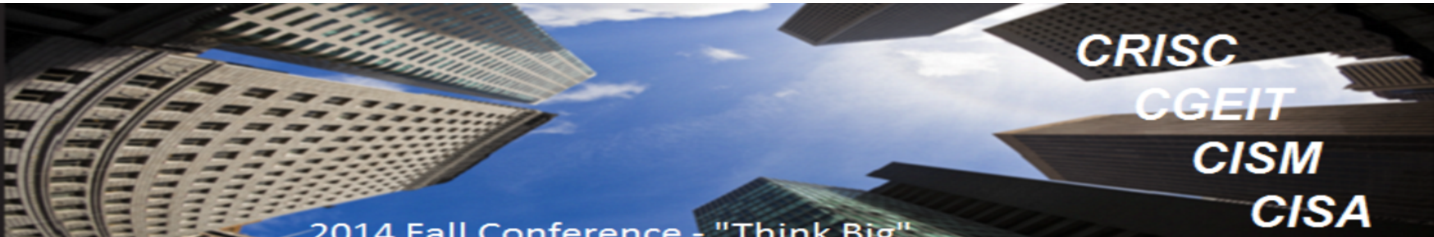
Risk Treatment Plan

Results Documentation

Asset

- Cardholder Data
- Sensitive Authentication Data
- Business Processes
- Interactive Voice Response
- Web Payments (Merchants)
- Customer Services – Call Centers

- *Asset is measured in terms of Asset Value*

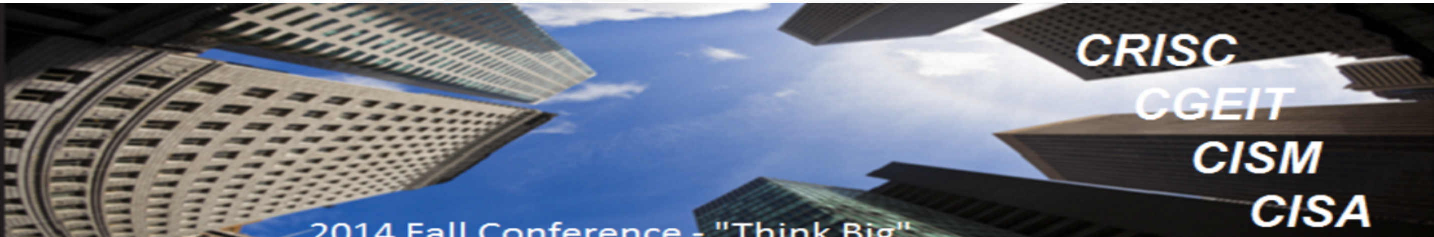


- Scope
- Asset
- Threat
- Vulnerabilities
- Risk Profiling
- Risk Treatment Plan
- Results Documentation

Threat

- **Threat is an actor which can potentially harm the asset. The threat can be accidental or deliberate.**

- *Threat is measured in terms of Likelihood of Threat (LHOT)*



Scope

Asset

Threat

Vulnerabilities

Risk Profiling

Risk Treatment Plan

Results Documentation

Vulnerability

- **How a weakness in technology or organizational process can be exploited by a threat.**

- *Vulnerability is measured as Level of Vulnerability (LOV)*

ISACA
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

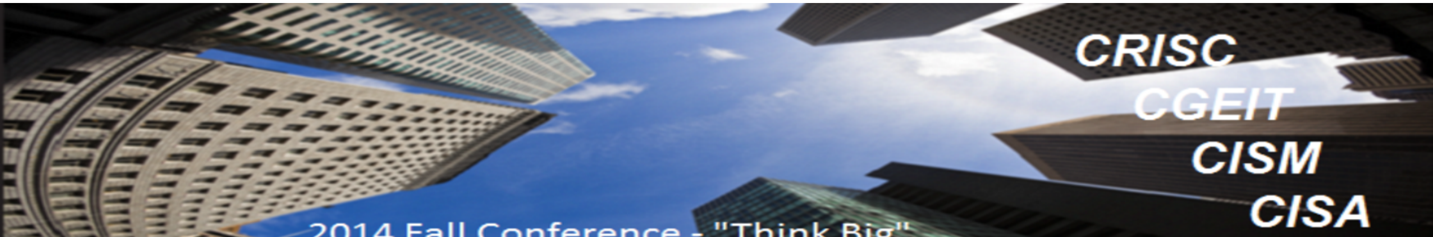
- Scope
- Asset
- Threat
- Vulnerabilities
- **Risk Profiling**
- Risk Treatment Plan
- Results Documentation

Risk profiling

Measure of Risk = f(Asset Value, LHOT, LOV)
Calculated after taking Risk Evaluation and Risk Acceptance Criteria into account
Existing Controls

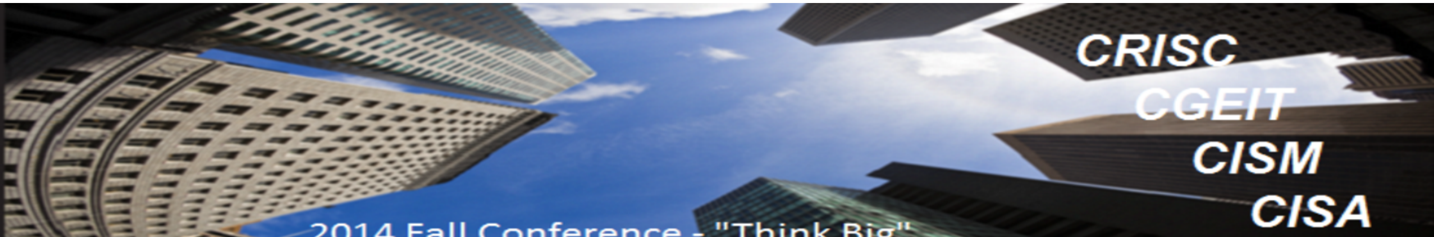
Revised Measure of Risk = Risk Score after Applying New Controls

Measured in terms of Measure of Risk (MOR) and Revised Measure of Risk (RMOR)



Sample Risk Evaluation Criteria

	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8



Risk Treatment Plan

- Scope
- Asset
- Threat
- Vulnerabilities
- Risk Profiling
- **Risk Treatment Plan**
- Results Documentation

- **Treat/Tolerate/Terminate/ Transfer**
- **Take Action if Treat/Transfer**
- **Take Approval if Tolerate/ Terminate**

Note: PCI requirements are minimum set of requirements. Any risk treatment cannot go below what is prescribed by PCI DSS.

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

Risk Assessment Report

Scope

Asset

Threat

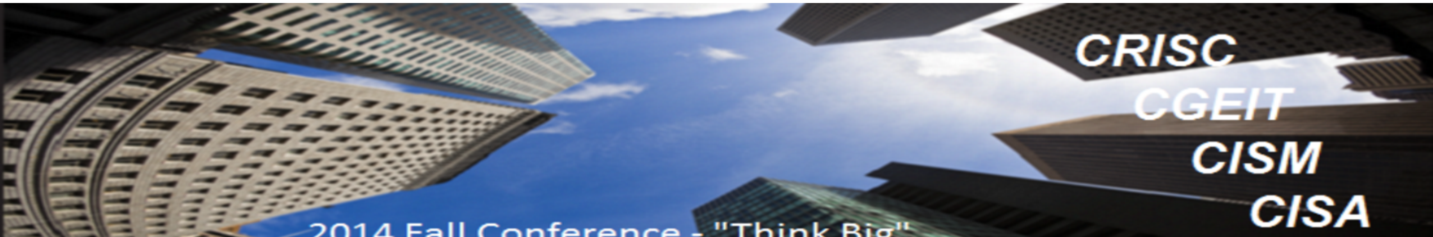
Vulnerabilities

Risk Profiling

Risk Treatment Plan

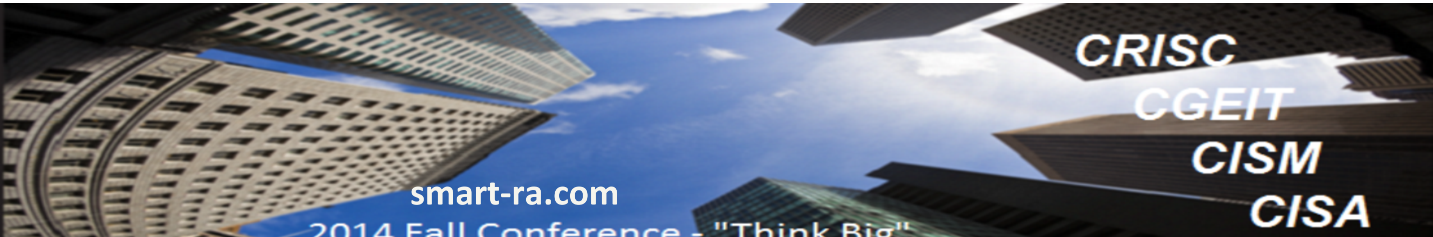
Results Documentation

- Document A-T-V Combination with the associated Risk
- Calculation of Risk
- RTP
- Action Taken



Case Study

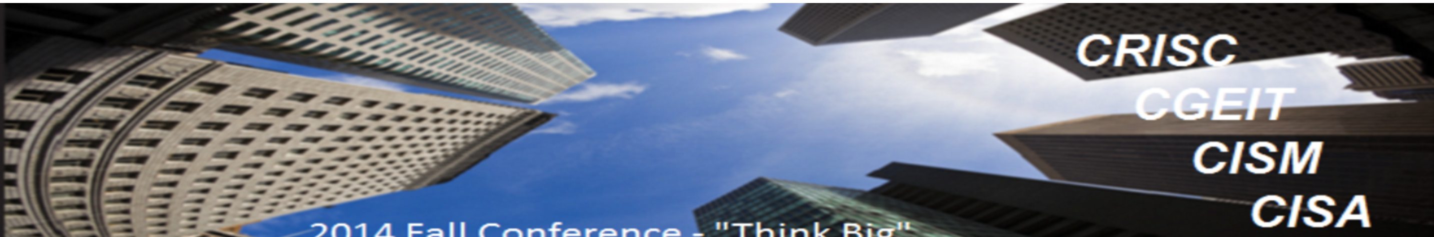
- Company Background – Wise Bank
- PCI Related Environment – Payment Channels include:
  - i. Online store
  - ii. Retail outlets
  - iii. Self service kiosks
  - iv. Payments over mobile
  - v. Drop Boxes
  - vi. Call Center



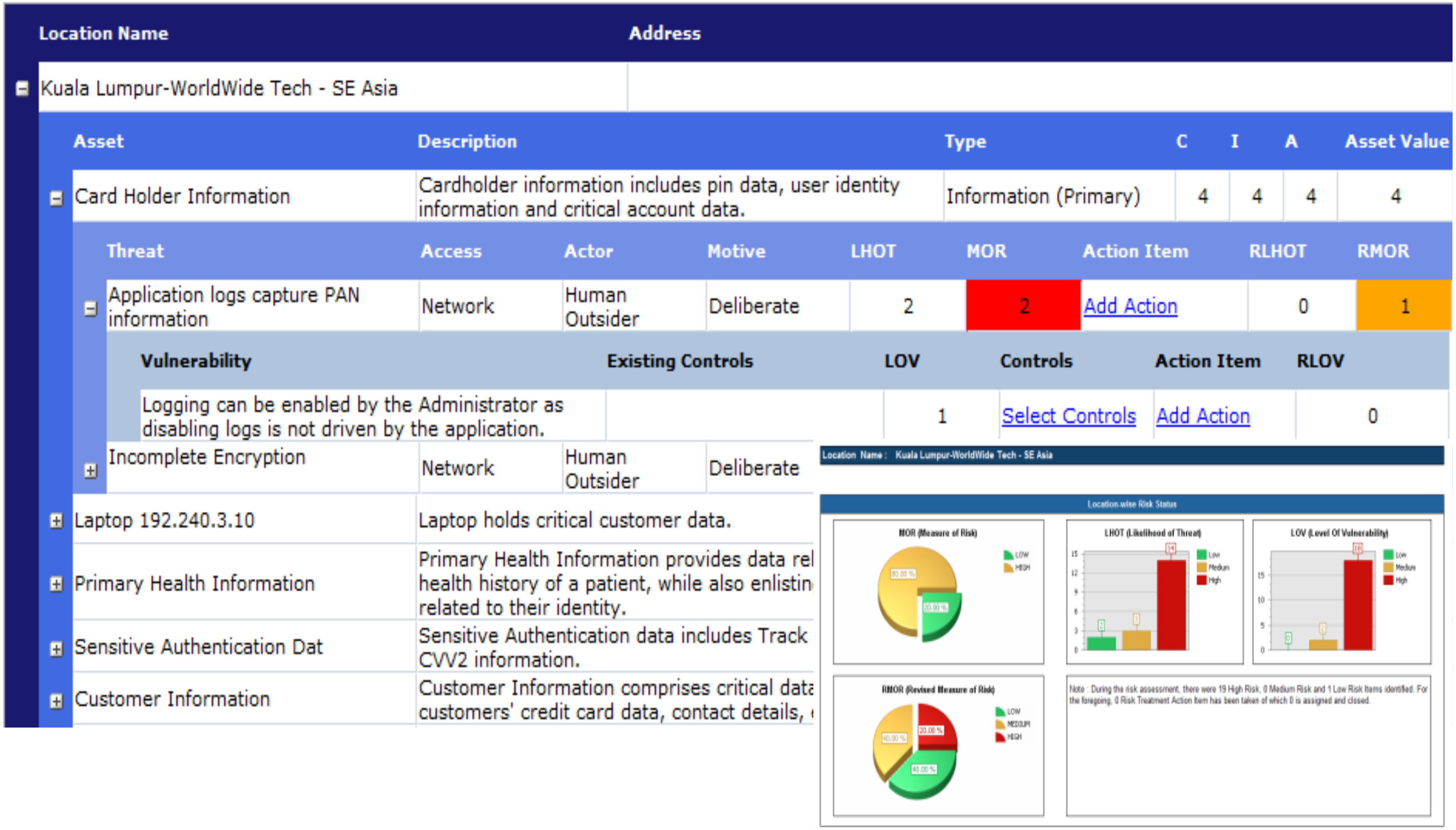
Example for 'A-T-V'

Asset Name	Threats	Vulnerabilities	Risk
Online Payment Process **Supporting Assets:** Apache Web Server EOS App Server Oracle 10G DB	Insider Sniffing the traffic Threat Properties Insider – Deliberate LHOT: High	App Server to Database Server in clear. LOV: Medium	High High

RTP	Action
Treat	Encrypt traffic from App Server to Database Server



Results Documentation



Location Name	Address
Kuala Lumpur-WorldWide Tech - SE Asia	

Asset	Description	Type	C	I	A	Asset Value
Card Holder Information	Cardholder information includes pin data, user identity information and critical account data.	Information (Primary)	4	4	4	4

Threat	Access	Actor	Motive	LHOT	MOR	Action Item	RLHOT	RMOR
Application logs capture PAN information	Network	Human Outsider	Deliberate	2	2	Add Action	0	1

Vulnerability	Existing Controls	LOV	Controls	Action Item	RLOV
Logging can be enabled by the Administrator as disabling logs is not driven by the application.		1	Select Controls	Add Action	0

Threat	Access	Actor	Motive
Incomplete Encryption	Network	Human Outsider	Deliberate

Asset	Description
Laptop 192.240.3.10	Laptop holds critical customer data.
Primary Health Information	Primary Health Information provides data rel health history of a patient, while also enlistin related to their identity.
Sensitive Authentication Dat	Sensitive Authentication data includes Track CVV2 information.
Customer Information	Customer Information comprises critical data customers' credit card data, contact details,

Location Name : Kuala Lumpur-WorldWide Tech - SE Asia

Location-wise Risk Status

Note : During the risk assessment, there were 19 High Risk, 0 Medium Risk and 1 Low Risk Items identified. For the foregoing, 0 Risk Treatment Action Item has been taken of which 0 is assigned and closed.

Get a feel of Risk Assessment?

Search “SISA Assistant” and sign up for FREE

E-mail: dbs@sisainfosec.com

SISA Information Security Inc.

440, North Wolfe Road, #85,

Sunnyvale, CA 94085