Regional Forum on Cybersecurity in the Era of Emerging Technologies
&
the Second Meeting of the "Successful Administrative Practices"-2017
Cairo, Egypt 28-29 November 2017

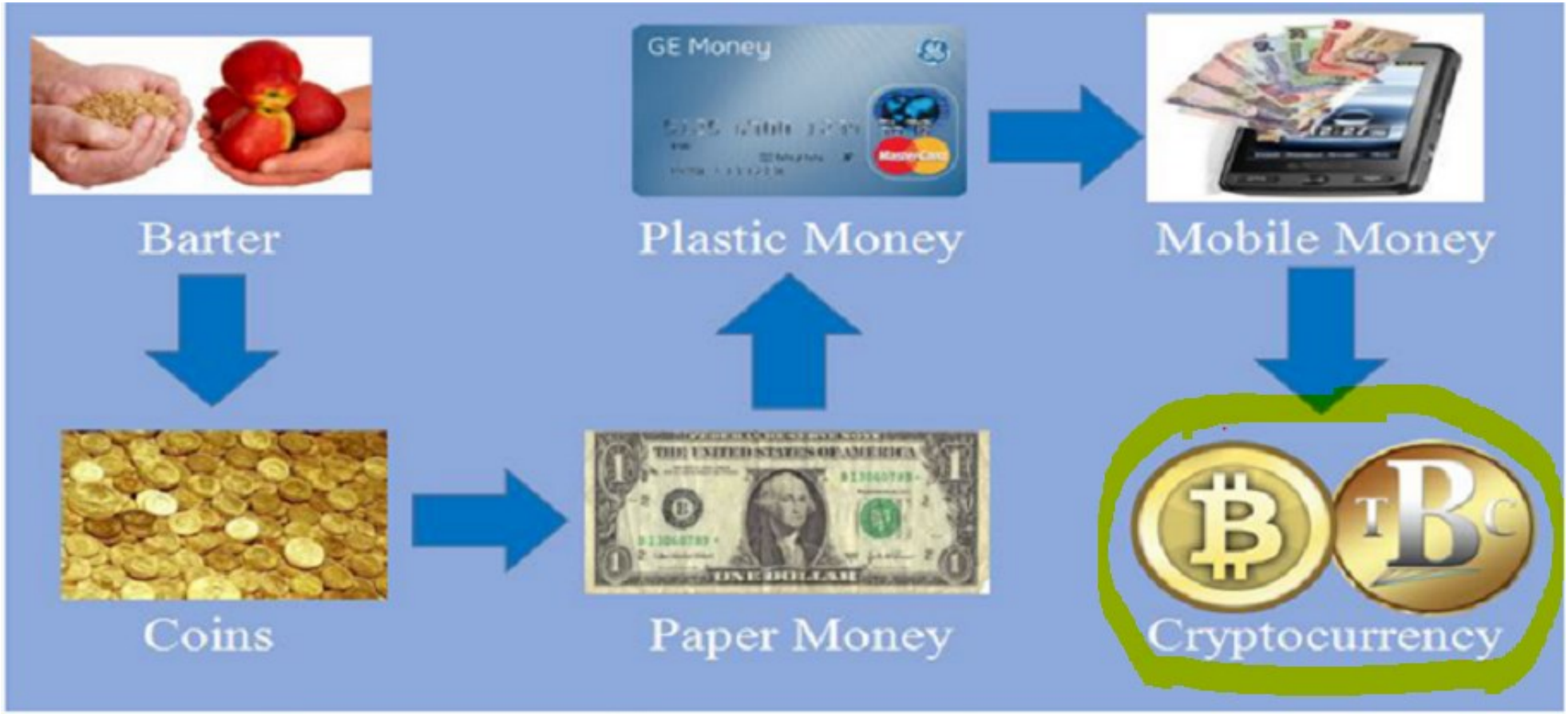
Critical Infrastructure Protection in Financial Sector

Hisham Mohamed Aly
Information Security Risk Manager – Emirates NBD

Agenda

1	Evolution of Economy
2	Defining Market Problem
3	Critical Infrastructure Protection & Security Standards
4	Défense in depth
5	Recommendations

Evolution of Economy



Defining the Market Problem

THE EFFECTS OF CREDIT CARD BREACH ON RETAIL BUSINESS ARE DAUNTING

70% of breached businesses are out of business within one year of the attack

1 in 6 small businesses will suffer a credit card breach in the next 24 months

98% Breaches originate from organized criminal groups

210 Average days between intrusion and detection

Types of Breaches

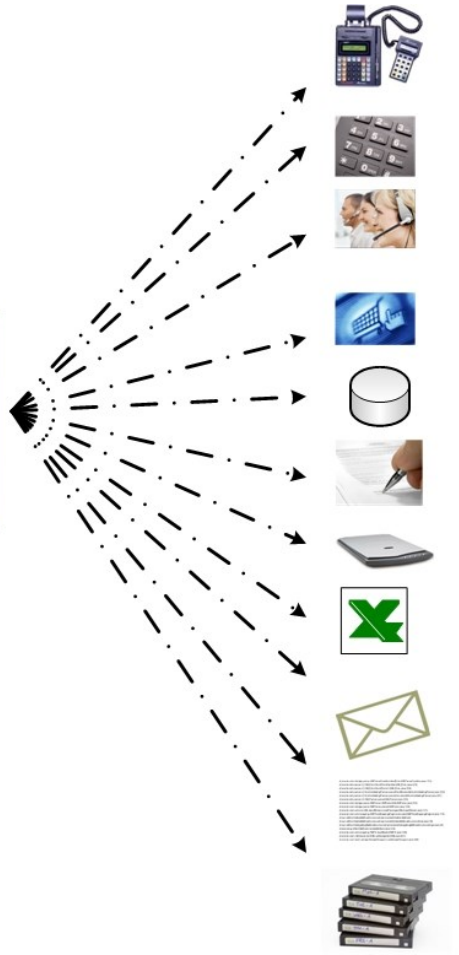
Physical Breach

Electronic Breach

Skimming

CHD – it gets everywhere!!!!

Just a few places I have found CHD recently!



Point of Sale

IVR

Contact Centres

E-Commerce

Databases

Paper contracts

Scanned docs

Spreadsheets

Email

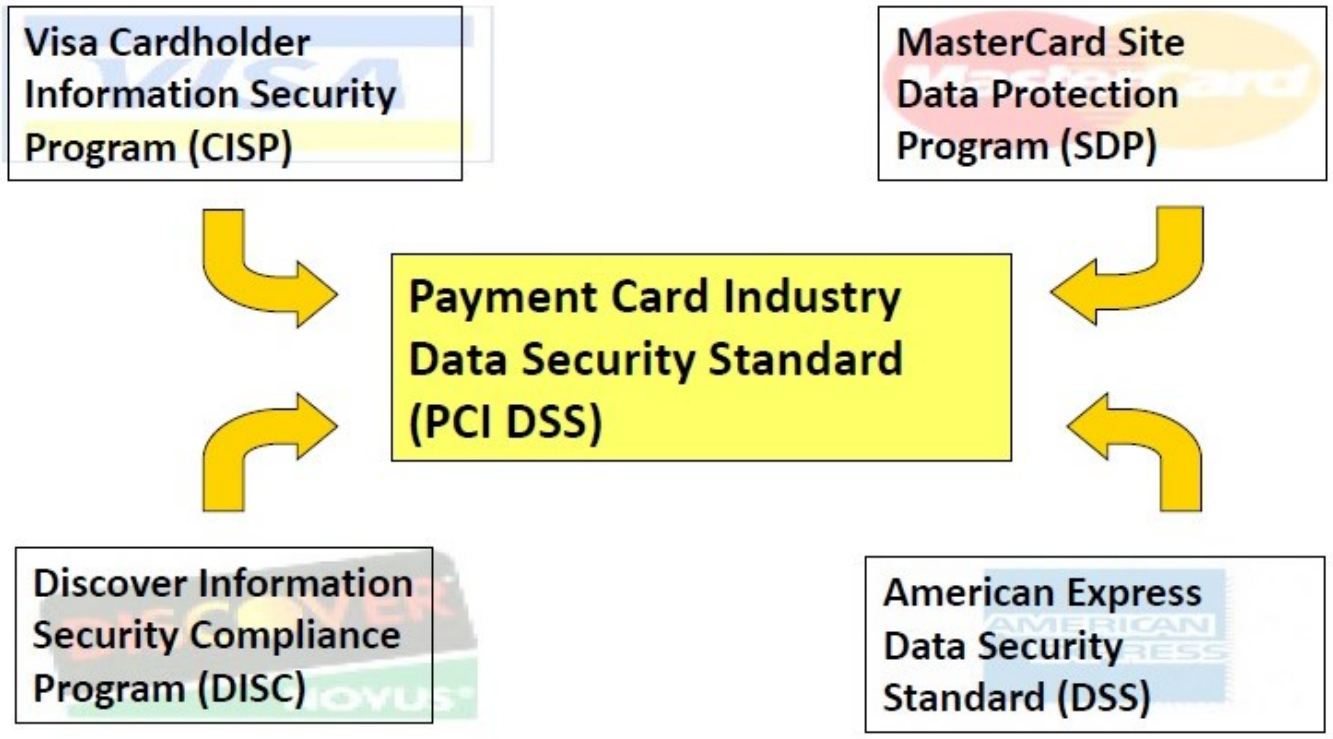
Logs

Backups

Security Standards PCI Vs ISO 27K

Features	PCI DSS	ISO 27K
Compliance Mandates	Compliance Mandatory	Compliance Voluntary
Scope	Storing , Processing or transmit CHD	Optional
Degree of Compliance	Complying with all requirements is mandatory	Standards Voluntary
Separation of Systems	High	Low
Degree of Flexibility	Low	High

PCI
Historical Overview



- **PCI DSS and related security standards** are administered by the **P**CI **S**ecurity **S**tandards **C**ouncil, which was founded by American Express, Visa, MasterCard and Discover Financial Services.
- **PCI** is a family of data security standards that is intended to secure processing infrastructure of payment industry
- **PCI DSS** applies to all entities that store, process, and/or transmit card holder data

PCI Standards

- **PCI DSS** covers security of the environments that store, process, or transmit account data
  - Environments receive account data from payment applications and other sources (e.g. acquirers)
- **PCI PA-DSS** covers secure payment applications to support PCI DSS compliance
  - Payment application receives account data from PIN-entry devices (PEDs) or other devices and begins payment transaction
- **PCI P2PE** covers encryption, decryption, and key management requirements for point-to-point encryption solutions
- **PCI PTS - POI** covers the protection of sensitive data at point-of-interaction devices and their secure components, including cardholder PINs and account data, and the cryptographic keys used in connection with the protection of that cardholder data
- **PCI PTS - PIN** covers secure management, processing and transmission of personal identification number (PIN) data during online and offline payment card transaction processing
- **PCI PTS - HSM** covers physical, logical and device security requirements for securing Hardware Security Modules (HSM)
- **PCI Card Production** covers physical and logical security requirements for systems and business processes associated with card personalization, PIN generation, PIN mailers, and card carriers and distribution.

15th December 2004	• these companies aligned their individual policies and released version 1.0 of the Payment Card Industry Data Security Standard (PCI DSS).
September 2006	• the PCI standard was updated to version 1.1 to provide clarification and minor revisions to version 1.0.
October 2010	• Version 2.0 was released • Expires on December 2014
November 2013	• Version 3.0 was released
April 2015	• Version 3.1 was realeased

What is PCI Compliance?

- Definition – Payment Card Industry Data Security Standard (PCI-DSS)
- Set up in 2004 by Visa, MasterCard, American Express, Discover, and JCB to reduce the risk of credit card theft and transfer liability to merchants
- Requires mandatory adoption by all businesses that store, process, or transmit credit/debit card data

PCI-DSS Compliance Benefits

Direct Benefits

Secure System (Network, OS, DB, APP)

Increase Data Confidentiality

Customer Trust

Improve Reputation

Improve Business

Indirect Benefits

Better prepared to comply with other regulations such as ISO27001 etc.

Ability to identify ways to improve the efficiency of IT infrastructure

Corporate security strategy

PCI DSS Goals and Requirements

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

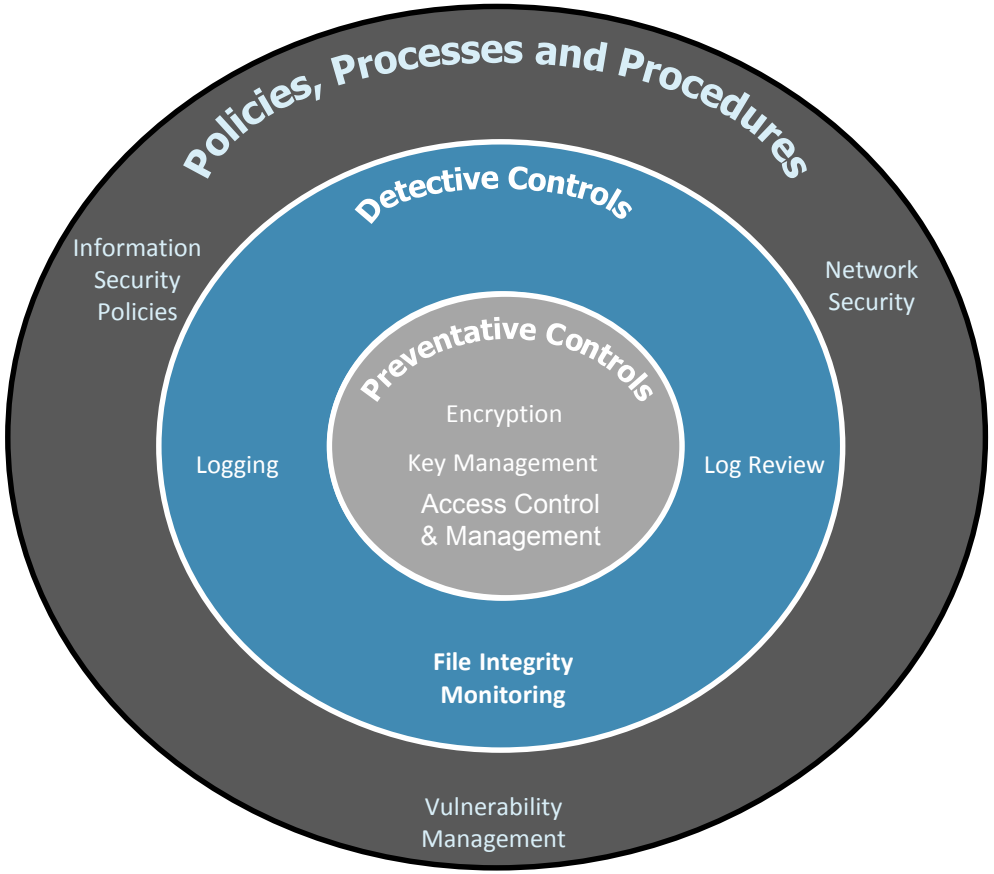
How does the PCI DSS map to your IT environment?
Defense in Depth

PCI Data Security Standard v3.0
Requirements for Compliance

- Build & Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Maintain an Information Security Policy
- Regularly Monitor & Test Networks

PCI Strategy

Key Focus Areas for PCI Compliance



Recommendations

- 3rd Party patching
- Endpoint Security
- Clear Policies , Procedures & Standards
- Security Awareness
- Documentation
- Inventory Management
- Risk Assessment for all Products

Thank You