Forum Presentations

Speaker	Presentation
	**Mrs. Hana A. Al Razzouqi:** **Securing Payments**
	**Ms. Stephanie Czák:** **Innovation and Security in Retail Payments: The European Experience**
	**Mr. Harish Natarajan:** **Legal, Regulatory and Oversight Arrangements for Securing Payments in the Cyber World**
	**Mr. Abdulla Al-Ajmi:** **Securing Payments in GCC Net**
	**Mr. Majed Al Adwani**: **Moving from Cyber Security to Cyber Resilience**
	**Professor Benjamin G. Edelman:** **Bitcoin, Electronic Currency, and Non-Traditional Payment Vehicles**
	**Approach Mr. Rolf von Rössing:** **European Cyber Security Strategy and Related Directives: a Legislative and Regulatory**
	**Mr. Andras Cser:** **Tackling Mobile Fraud: The Next Frontier**

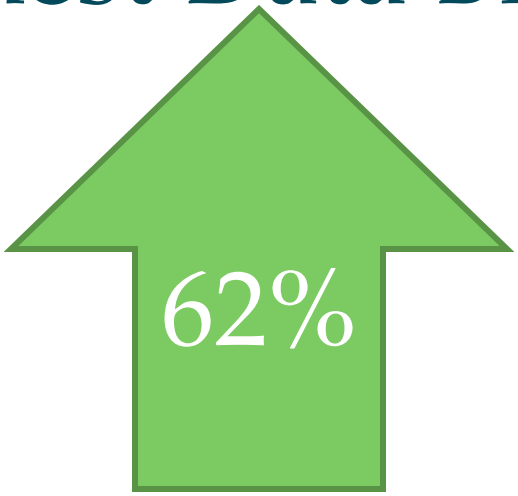
Securing Payments…

Hana Razzouqi
Executive Director, IT & Banking Operations
Central Bank of Kuwait
Sunday, 16th November 2014

Financial Sector is the main focus for cyber criminals

Symantec Report

2013 Financial Sector had the highest Data Breaches



Financial Sector is the main focus for cyber criminals

Verizon :2013 will be remembered as

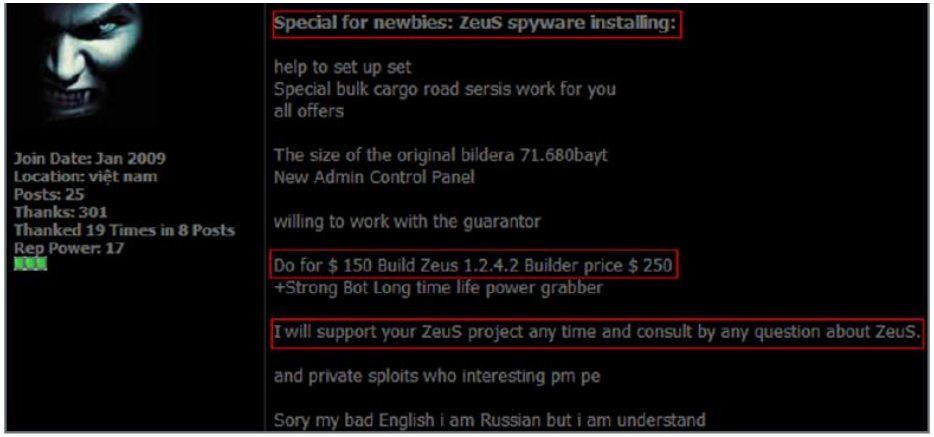
"year of retailer breach"

A year of transition from geopolitical attacks to large scale attacks on payment card systems

Cyber threats are evolving

Fraud-as-a-service

Malware-as-a-service



DDOS-as-a-service

Service	2011 Price	2012 Price	2013 Price
DDoS attack: • Lasts 1 hour • Lasts 24 hours	 US$4–10 US$30–70	 US$2–25 US$15–60	 US$2–60 US$13–200

High cost to detect, recover, investigate, and manage the incident

What's happening in Kuwait?

Card payments channel was valued at KWD 16 billion ($56.4 billion) in 2013

Smart Civil ID used as supplement to withdraw cash and pay fuel prices

Pay with your mobile

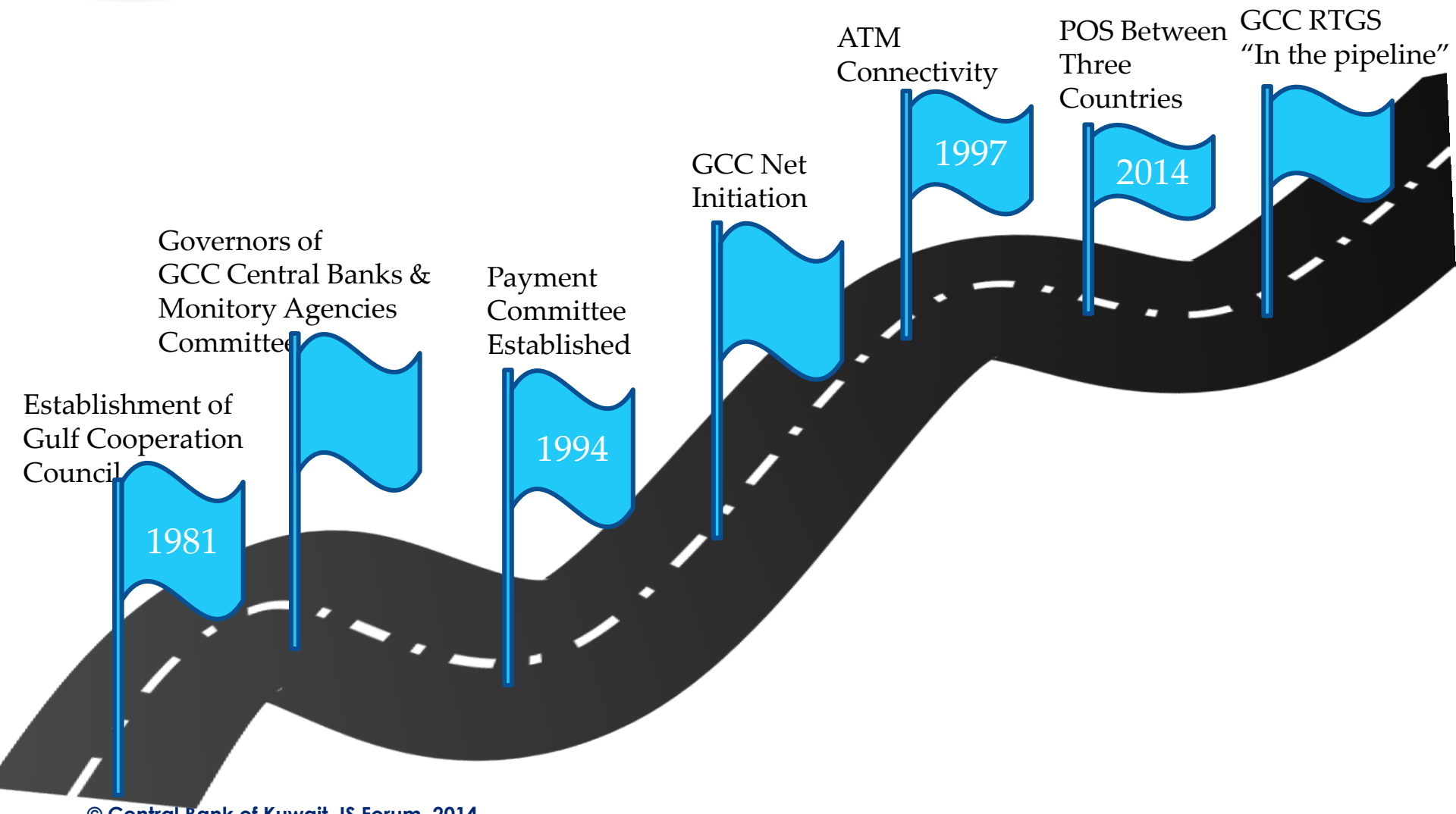
Regulatory Challenge

International Standards for Payment Systems and Operational Risk Management

EMV compliance since 2010

Electronic Transaction Law No. 20 , issued in 23rd Feb 2014
Articles 29 & 31

Payments among the GCC Countries



GCC Governors' Directives

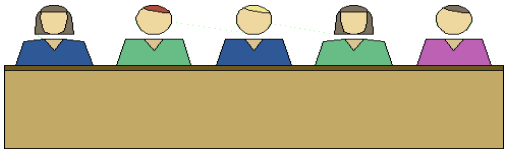
Information Security as a permanent item on the Payments committee agenda

Annual Information Security Forum organized by the respective GCC state of presidency

Today's Forum

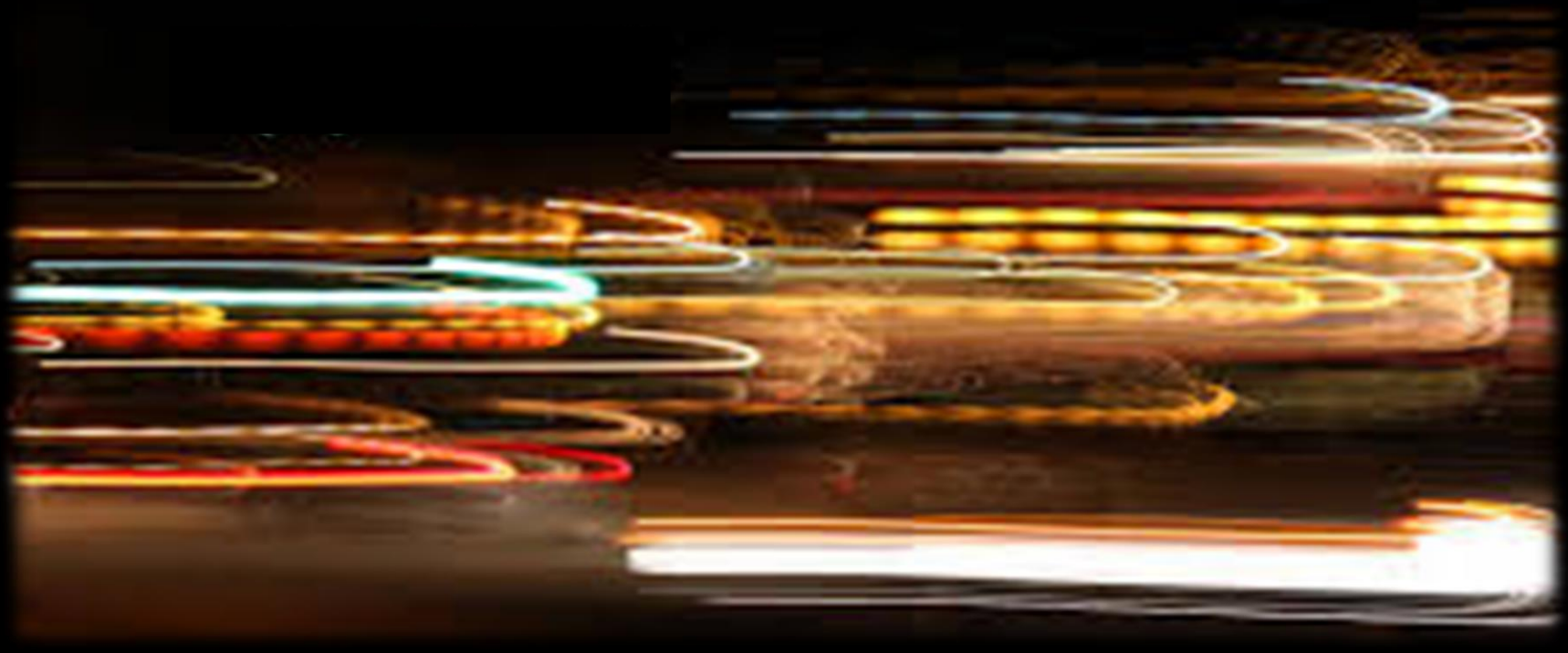
1. Threats to online, mobile, and cross-border payments
2. Cyber laws & regulations
3. Research & future trends in cyber security & Fraud Prevention

Panel Discussions



Round Table Sessions

Enjoy the *Professional Ride*



Innovation and Security in Retail Payments: The European Experience

Stephanie Czák
Senior Market Infrastructure Expert /European Central Bank
Central Bank of Kuwait
Sunday, 16th November 2014

Challenges of innovative retail payments for overseers

- Scope, Effective power and capacity
- Complexity of technology & services or organisational structure
- Market development & convenience vs. security & customer confidence
- Standards & Harmonisation
- Cooperation

Choices of regulatory approaches

Self-regulation

Overseer contributes to industry standards /self-regulation

Industry self-assessments /certifications

Moral suasion

Oversight standards /recommendations

Assessments by the overseer

Statistical monitoring

Incident reporting

Regulation /Supervision/Enhanced Monitoring

Legal requirements & fines

Licensing

Onsite inspections

Transaction level-based or real-time monitoring

Eurosystem objectives for payment instruments oversight

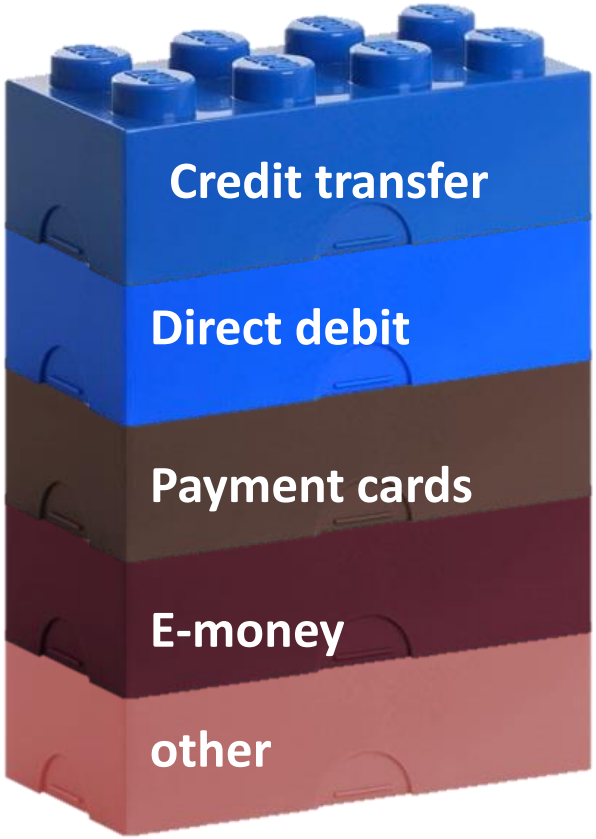
Ensuring efficiency

Issues of (potential)
overall scheme wide relevance / impact

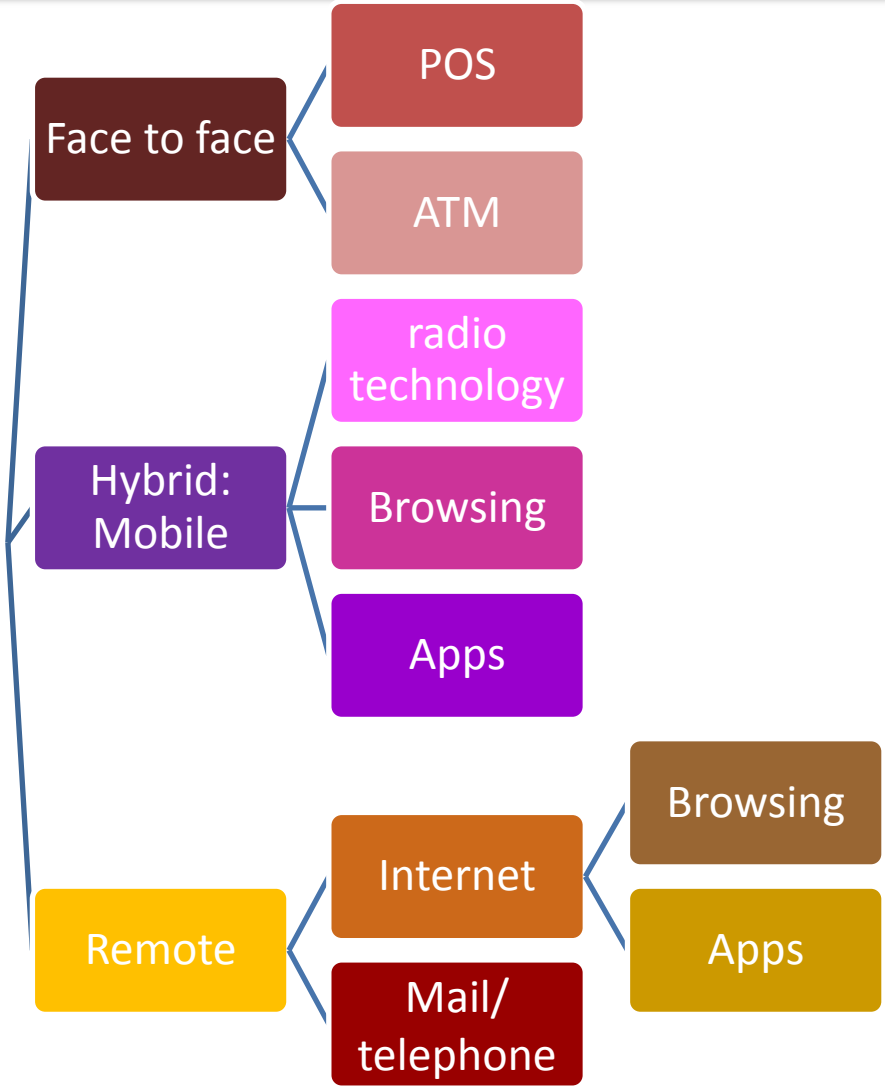
Maintaining public confidence

Scope of the oversight of retail payment instruments

Type of instrument



Access channel



Harmonised Eurosystem standards for payment instruments (→ moral suasion)

I. Have a sound legal basis under all relevant jurisdictions;

II. Ensure that comprehensive information, including appropriate information on financial risks, is available to the actors;

III. Ensure an adequate degree of security, operational reliability and business continuity;

IV. Have effective, accountable and transparent governance arrangements;

V. Manage and contain financial risks in relation to the clearing and settlement process.

European Forum on the Security of Retail Payments (SecuRe Pay)

The Forum

- Cooperation between central bank overseers and supervisors of payment service providers
- Observers: European Commission, Europol

Scope

- Electronic retail payment services, payment instruments and payment service providers

Mandate

- Facilitate common understanding among authorities
- Make recommendations, guidelines, technical regulatory standards

Typical security related considerations in the risk of new services 1/3

What needs to be protected?

- Financial assets and rights of the user
- Sensitive payment data (information that can be used to conduct fraud)
- Level playing field
- General trust in payment services and the currency (e.g. risks for existing infrastructures and services)

Typical security related considerations in the risk of new services 2/3

Who should be regulated?

- Example virtual currencies

Inventor(s)

Issuer(s) /Scheme governance authority

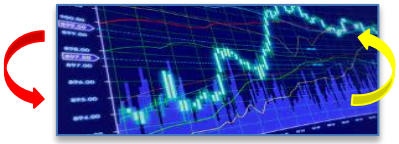
Users

Merchants

Processor(s)

Wallet providers /custodian

Exchanges



Technical service providers (non-core)

Investment product providers

Typical security related considerations in the risk of new services 3/3

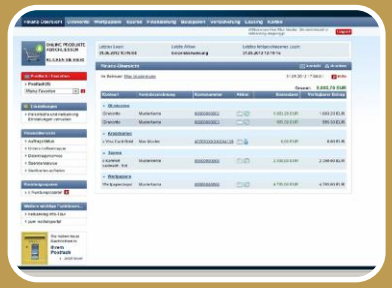
Where are the main payment security related problems

- Lack of sound governance of the service provider (e.g. legal set-up, risk management, monitoring and reporting, audit)
- Poor procedures (e.g. KYC, authentication and distribution of related tools, protection of sensitive information, access management)
- Problems related to the design, developments, management of hardware & software components
- Transmission of data via (e.g. internet, radio technology)
- Customer information and education

Relevant SecuRe Pay work

Security of internet payments

- Final Recommendations (01/2013)
- Assessment Guide (01/2014)
- EBA Guidelines (Oct/2014)



Payment account access services

- Final Recommendations as input for upcoming EBA Guideline (03/2014)
- ECB legal opinion on the review of the payment services directive (01/2014)

Security of mobile payments

- Draft Recommendations (11/2013)
- Pending revised Payment Services Directive (Q1/15)

Outlook

Policy

- Mobile payments (continued)
- E-wallet solutions
- Support of the European Banking Authority in the implementation of the mandates coming from the Payment Services Directive 2 (e.g. third party access to payment accounts, secure authentication and communication protocols, reporting of major incidents)

Oversight implementation

- Continuous oversight on card payment schemes. Next assessment focus: internet payments security
- Assessment of the European direct debit scheme (SEPA direct debit)


Many thanks for your attention!

Information Security Forum
SECURING PAYMENTS IN THE CYBER WORLD

Legal, Regulatory and Oversight Arrangements for Securing Payments in the Cyber World

Harish Natarajan
Payment Systems Development Group

Information Security Forum – Securing Payments in the Cyber World
Kuwait City
16 November 2014

WORLD BANK GROUP
Finance & Markets

Agenda

1. Public Policy Objectives in Payment Systems
2. Ongoing trends in payment systems and implications from security perspective
3. Legal, Regulatory and Oversight
4. Conclusion

Public Policy Objectives

- It is widely accepted that public policy objectives with respect to national payments system are:
  - Safety
  - Reliability
  - Efficiency
- Securing the payment systems is key to ensuring that the above public policy objectives are met.
- Need to achieve the right balance amongst these objectives.

Trends in Payment and Settlement systems

- Increasing use of internet technologies for all types of payment and settlement systems.
- Continued rise in usage of electronic payment mechanisms and entry of new payment service providers.
- Ongoing trend of increase in usage of outsourcing and entry of new players in the payments and settlement systems value chain.
- Increasing regulatory attention to operational reliability with implications on capital requirements.
- High degree of Anonymity achievable by certain new payment mechanisms make it attractive for use as payment mechanism for illicit activities.
- Technological developments also enable new risk management measures – fraud analytics; digital escrow mechanisms; and, de-linking of authorization from purchase.

Volume of global non-cash payments: Different sources, different figures

BCG
THE BOSTON CONSULTING GROUP

2012 (est.):
364 bn transactions

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

2013 (est.):
365.5 bn transactions

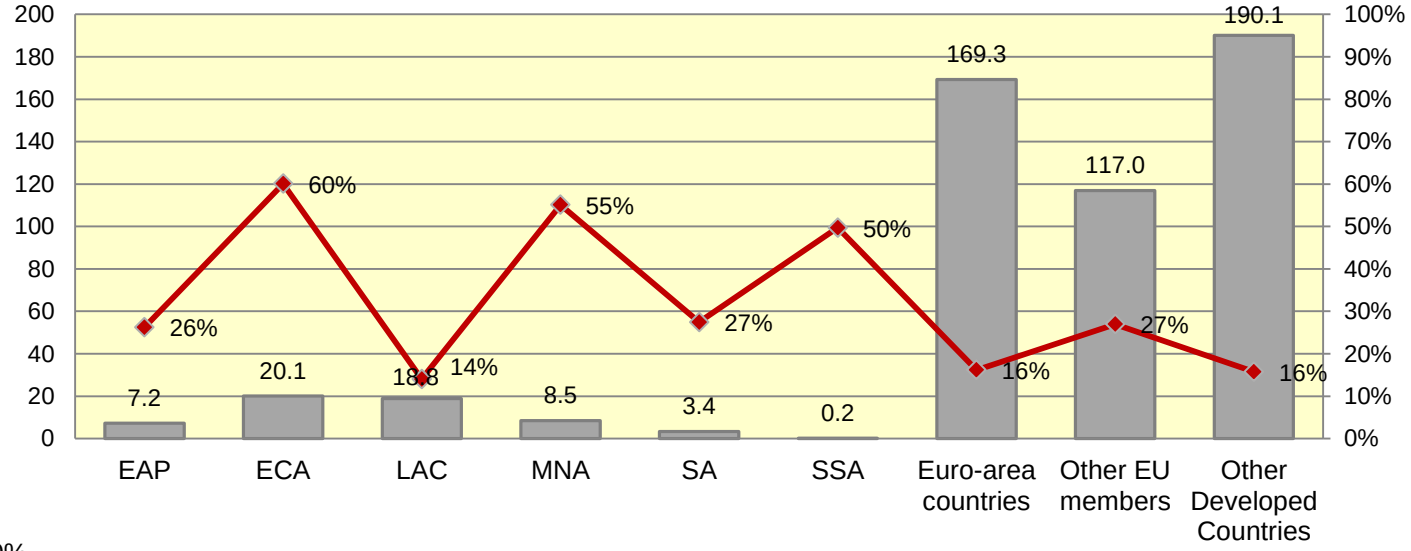
But agreement on the general trend:

Growth of non-cash payments outperforms growth in real economy

**Sources: Capgemini World Payments Report 2014, and Boston Consulting Group's Global Payments 2013*

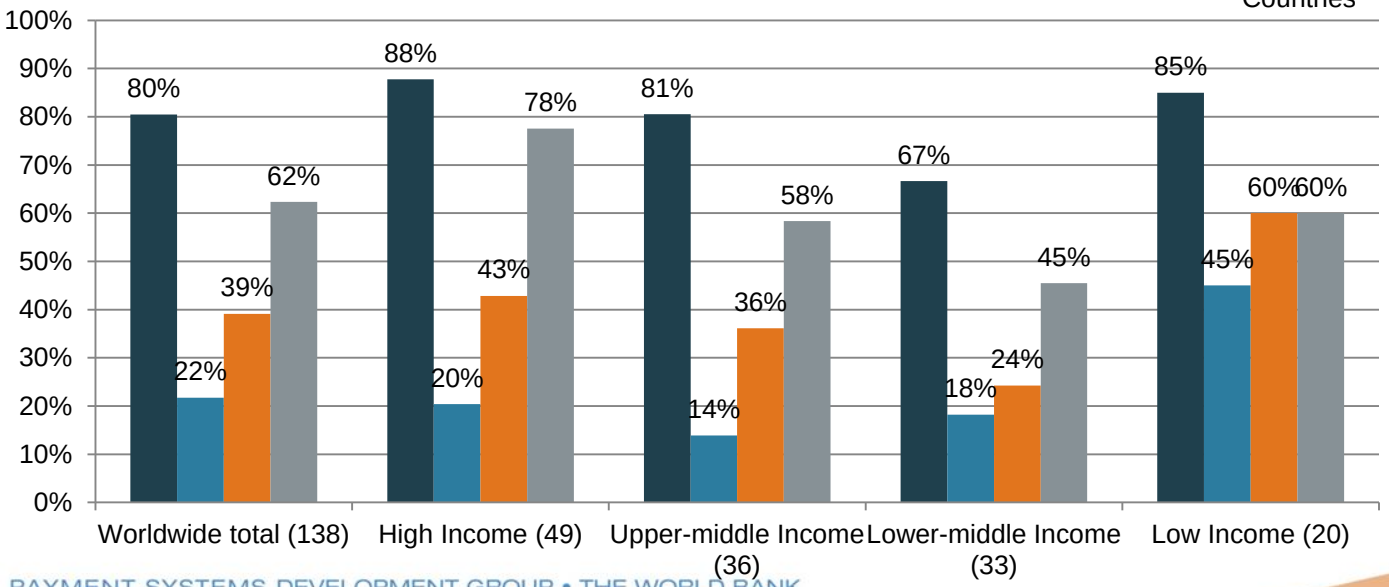
Trends for innovative retail payment products

Global Payment Systems Survey (preliminary findings)



Retail cashless transactions per capita (2009)

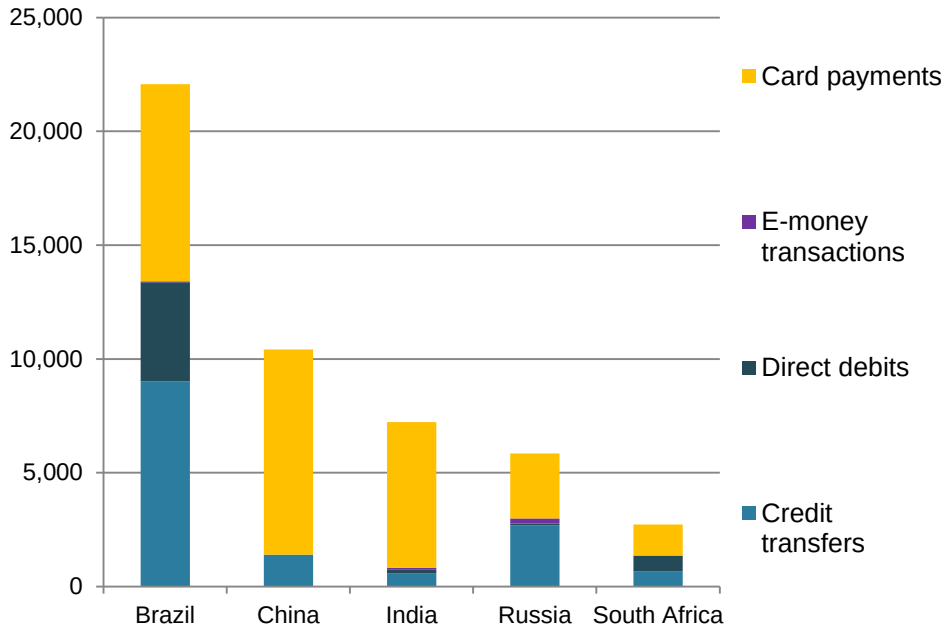
- Average number of per capita cashless transactions
- Growth 2009 vs. 2006



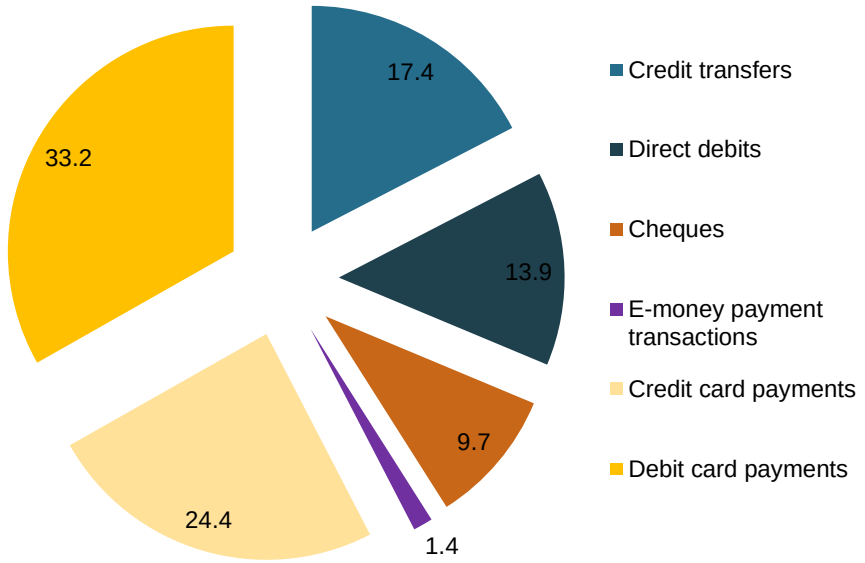
- Are growing
- Account for more than 5% of traditional electronic retail payments
- Are growing at a faster rate than traditional electronic retail payments
- Are being used for payments, and not just for safekeeping of money

Relative importance of payment instruments in CPMI countries (CPMI statistics)

1) Electronic payment transactions by type of instruments in select CPMI countries, 2012 (millions, total for the year)**



2) Use of payment instruments by non-banks: relative importance of payment instruments, in number of transactions in CPMI countries* (2012)



**Source: CPMI, 2013.
Please note, direct debits nav for China. E-money nap for China and South Africa

*% of total number of transactions, based on available data. Please note, e-money transactions nav for 7 CPMI countries. Source: CPMI, 2013

Increasing Role of Non-banks - Classification of non-banks

Front-End Service Provider

- Provides services to Payers or Payees in association with / On Behalf of Payment Service Provider (PSP)
- Examples: Agents, Payment Gateways

Back-End Service Provider

- Provides services to the PSP
- Examples: Operation of IT infrastructure, Customer service Center

Payment System Operator

- Operates a payment system for participating payment service provider
- Examples: Operator of Card Switch, ACH

Independent provision of payment Service

- Offers services to payers and payees independently
- Examples: Mobile Money, Remittance Service Provider

Not the only way of classifying
Similar entities could organize themselves differently in different situations
There could be potential overlaps

7 Global Trends in Retail Payments

Based on a research conducted by Innopay on behalf of the World Bank

1. The mobile revolution
2. Identity at the heart of payments
3. Unbundling of payment and authorization
4. Payment contexts are becoming real time
5. Person-to-person payments digitizing
6. Emergence of continents on the web
7. Big data

Retail payments: the potential of "disruptive innovation"

"As early as 2020, such instruments as e-money accounts, along with debit cards and low-cost regular bank accounts, can significantly increase financial access for those who are now excluded"
Jim Yong Kim

M-Pesa launches in Romania on March 9, 2014, for the first time in Europe., following the launches in Egypt, India, Lesotho and Mozambique, over the past 12 months

On September 9, 2014, Apple announces Apple Pay - supports credit and debit cards from the three major payment networks, American Express, MasterCard and Visa, issued by the most popular banks

PayPal has 143m active accounts and handled $180 billion in payments last year

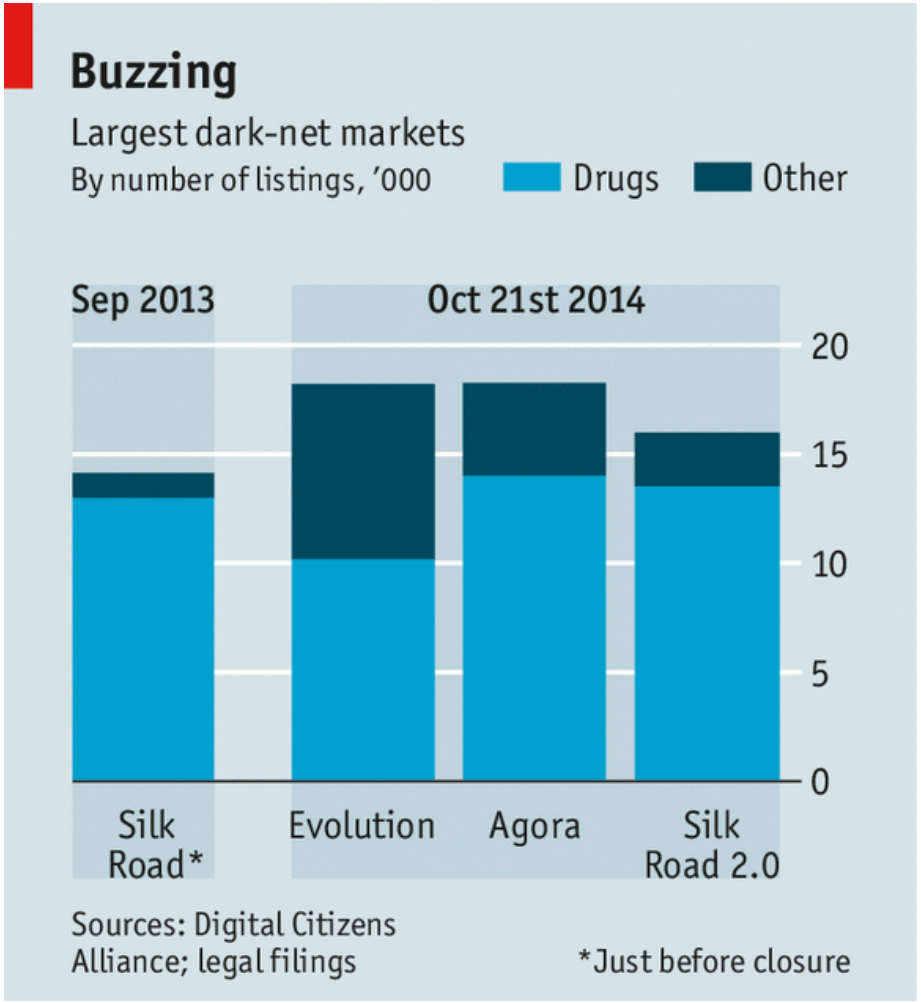
Alibaba

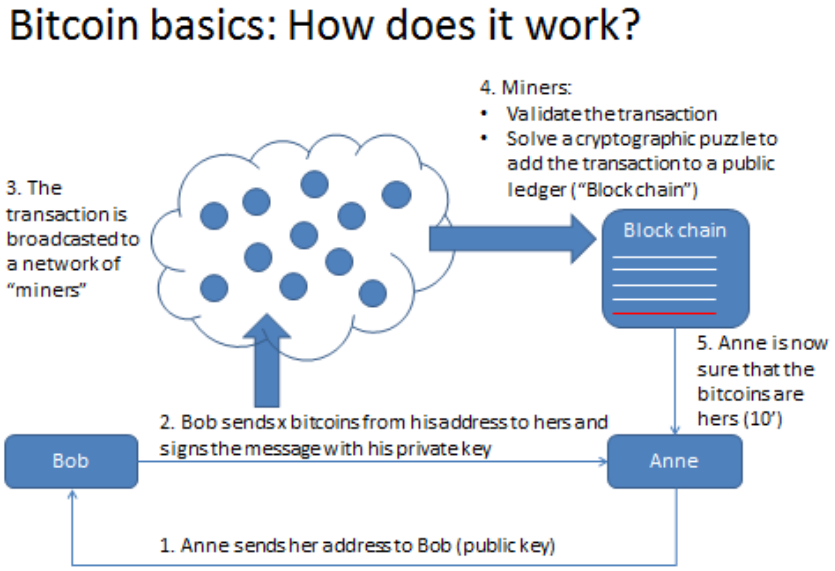
- In over 1/3 of the countries surveyed in the GPSS, non-banks issue non-cash payment instruments**
  - Mobile operators are mostly active in low / lower-middle income countries, mainly SSA, SA, EAP
  - Postal network has a stronger role in European countries and higher income
  - Credit cooperatives offer non-cash payments in slightly less than 30% of the countries, followed by MFIs
  - The overall picture is not yet clear: unspecified "other" NBFIs found to be equally relevant
- Although indirect access to RTGS is more common, it emerges that supervision often translates in NBFIs being granted direct access (either with or without access to credit credit) . Direct access of ACH infrastructure is mainly the prerogative of banks***

**Preliminary results; **Ongoing analysis will establish the extent to which this figure may be underestimated ; ***Bank ownership and specific risk control requirements considered as the main factors*

Amazons of the Darknet ?

Title of a story in the Economist





Source: Economist

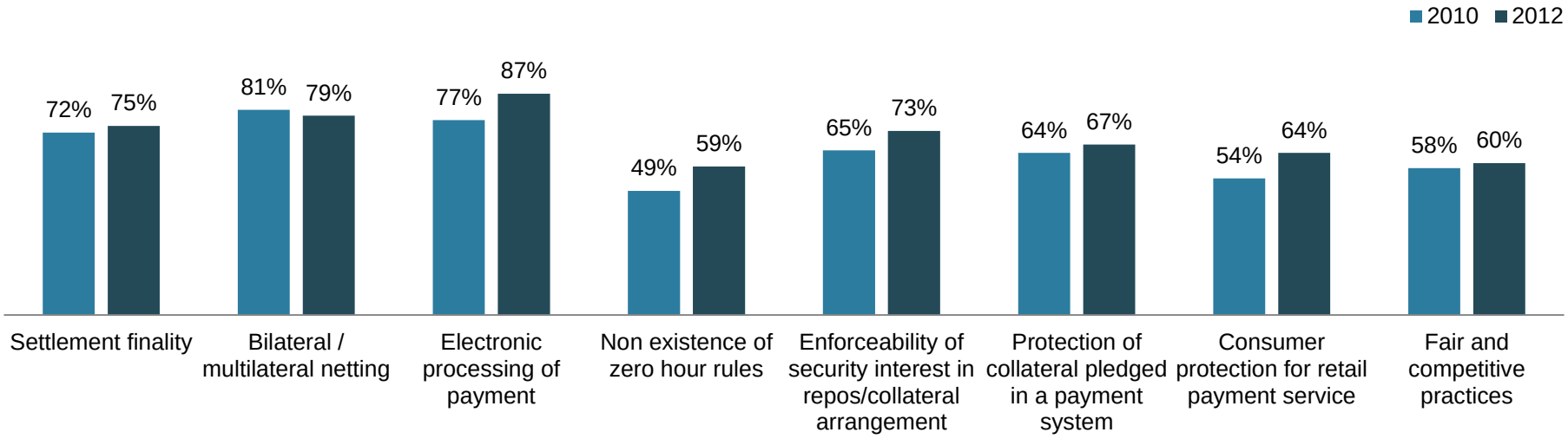
Legal aspects with specific relevance to ePayments

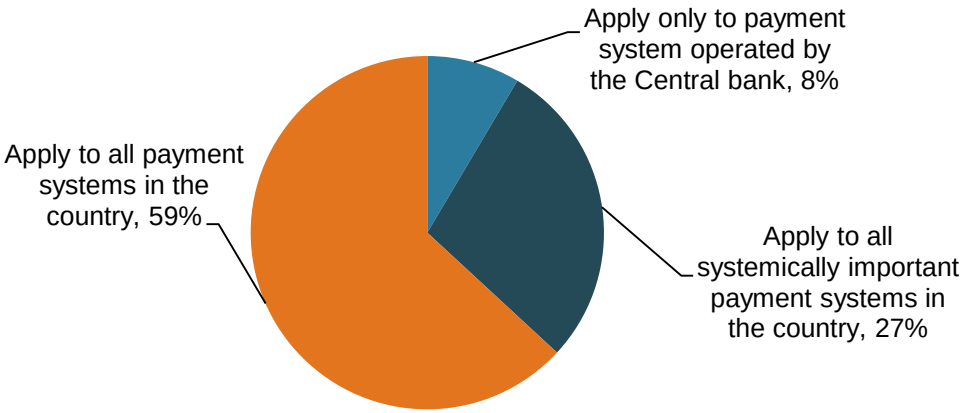
- **Electronic transactions and signatures**
- **Cybercrime**
- **Consumer protection**.
- **Data protection**
- **Information security**

Source: UNCTAD Publication, Harmonizing Cyber Law and Regulations.

Depth and reach of legal protections

Payment systems concepts covered in the legal framework





Applicability of payment systems concepts in the legal framework

**Based on GPSS Preliminary Findings*

Oversight of National Payments System

- **Oversight of the National Payments System is the key tool for public authorities to ensure continued safety, reliability and efficiency of the NPS**.
- Oversight is different from Supervision and Market Surveillance.
- Strategic framework for Oversight:
  - Objective
  - Scope
  - Standards
  - Tools
  - Organizational arrangements
  - Collaboration framework

- The pre-eminent standard for systemically important payment systems; and, securities market infrastructures is the CPSS-IOSCO Principles of Financial Markets Infrastructure.
- There is a dedicated principle for operational reliability which encompasses Information security. The CPSS-IOSCO can also be a useful framework for retail payment systems as well.

Operational Risk - PFMIs

Risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by an FMI. These operational failures may lead to consequent delays, losses, liquidity problems, and in some cases systemic risks. Operational deficiencies also can reduce the effectiveness of measures that FMIs may take to manage risk, for example, by impairing their ability to complete settlement, or by hampering their ability to monitor and manage their credit exposures.

An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls.

Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity.

Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.

Source: CPSS-IOSCO Principles for Financial Market Infrastructures, BIS 2012.

Operational Risk – PFMIs (contd..)

- Comprehensive physical and information security policy that addresses all potential vulnerabilities and threats.
- Have policies effective in assessing and mitigating vulnerabilities in its physical sites from attacks, intrusions, and natural disasters.
- Have sound and robust information security policies, standards, practices and controls that instill an appropriate level of confidence and trust in the FMI by all stakeholders.
- Policies, standards, practices and controls should include identification, assessment and management of threats and vulnerabilities.
- Data should be protected from loss and leakage, unauthorized access and other processing risks.
- Security objectives and policies should confirm to commercially reasonable standards for confidentiality, integrity, authentication, authorization, non-repudiation, availability and auditability.

Source: CPSS-IOSCO Principles for Financial Market Infrastructures, BIS 2012.

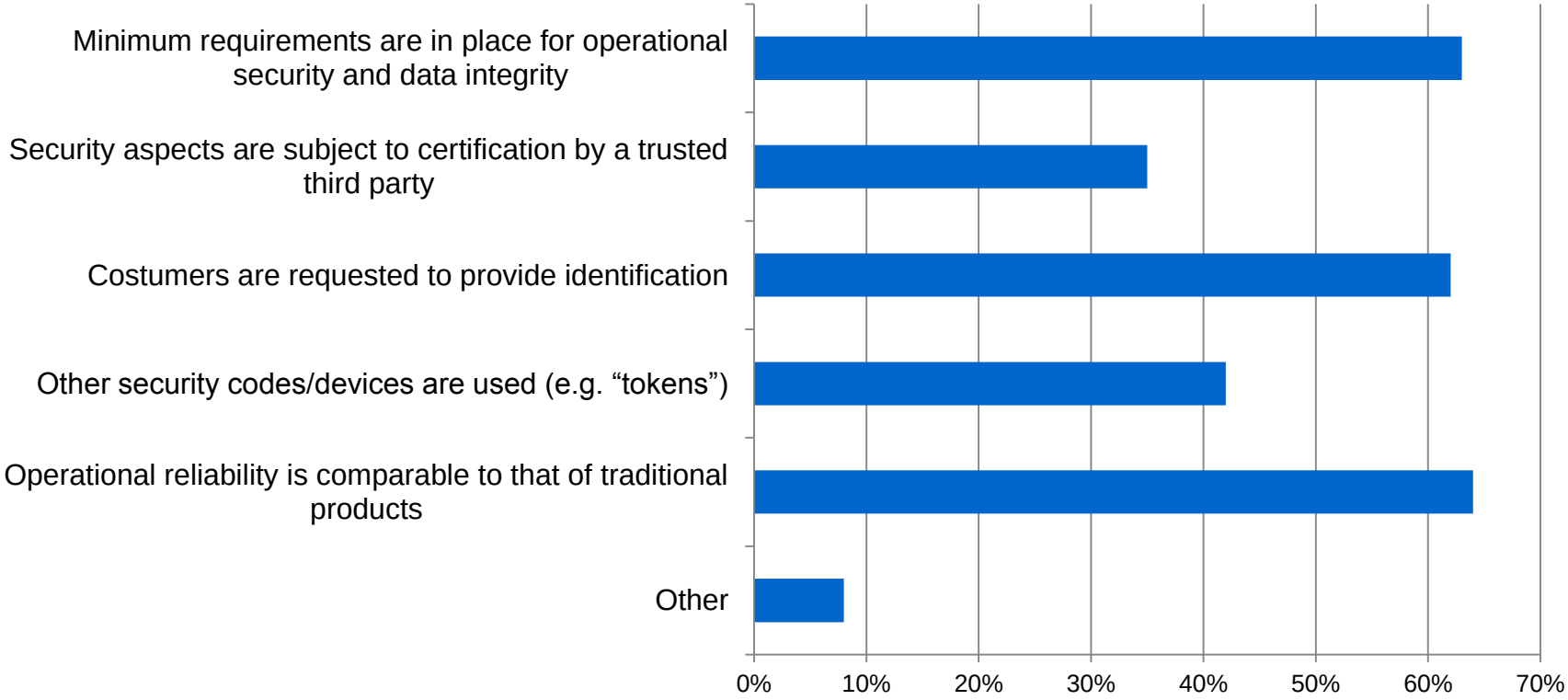
ECB – Assessment guide for internet payments

- General Control and Security Environment
  - Governance
  - Risk Assessment
  - Incident Monitoring and Reporting
  - Traceability
- Specific Control and security measures for Internet Payments
  - Initial customer identification information
  - Strong customer authentication
  - Enrollment for and provision of authentication tools and software
  - Log-in attempts, session timeout and validity of authentication
  - Transaction Monitoring
  - Protection of sensitive payment data
- Customer awareness, education and communication
  - Customer education and communication
  - Notifications and setting limits
  - Customer access to information on status of payment initiation, and execution

Key public policy considerations and regulatory responses for virtual currency schemes

- Designed to make transactions non-traceable, combined with other tools like anonymous website hosting, can be abused for payment for illicit and unlawful activities – Several instances encountered already.
- Lack of clarity on legal treatment consequently unregulated.
- Tax treatment
- Consumer protection
- Volatility in price/exchange rate
- Governance of Public Ledger System
- Regulatory responses thus far:
  - In general, no outright ban, as per se not violating any law
  - Apply AML/CFT regulations to intermediaries like exchanges, wallet providers
  - Treatment as an asset for tax purposes
  - Advisory from central banks on nature of such schemes and that these are not guaranteed and are distinct from bank deposit and currency
  - Restrictions on involvement of banks in activities related to these
  - Explore applicability of money transfer laws/regulations to entities involved in these
  - Explore applicability of securities exchange laws/regulations to the exchanges and other trading facilities

Security and risk management in innovative payment products



- Regulators’ involvement in setting minimum requirements for security, data integrity and operational reliability is lower in high income countries as a whole, although there is a significant contrast between EU countries with a percentage higher than the worldwide figure, and ODCs with the lowest percentage
- Regulator involvement in this specific issue is higher across low income countries, especially in the SSA region

Concluding Remarks

- Mitigation of cybersecurity related risks are central to achieving public policy objectives in payment and settlement systems.
- Ongoing developments both enhance risks and at the same time also provide more tools.
- Payment Systems Oversight is the key tool for public authorities to ensure that the payment and settlement systems infrastructure continues to maintain the right security posture.
- Cyber security Risk profile of large value and systemically important payment and settlement systems while different from retail payment systems, they share several characteristics. The CPSS-IOSCO PFMIs – Principle 17 in particular provides guidance for overseers on operational reliability, in addition there are other specific principles on Governance and Risk Management that are also applicable.

Payment Systems Development Group
The World Bank

www.worldbank.org/paymentsystems

Securing Payments In GCC Net

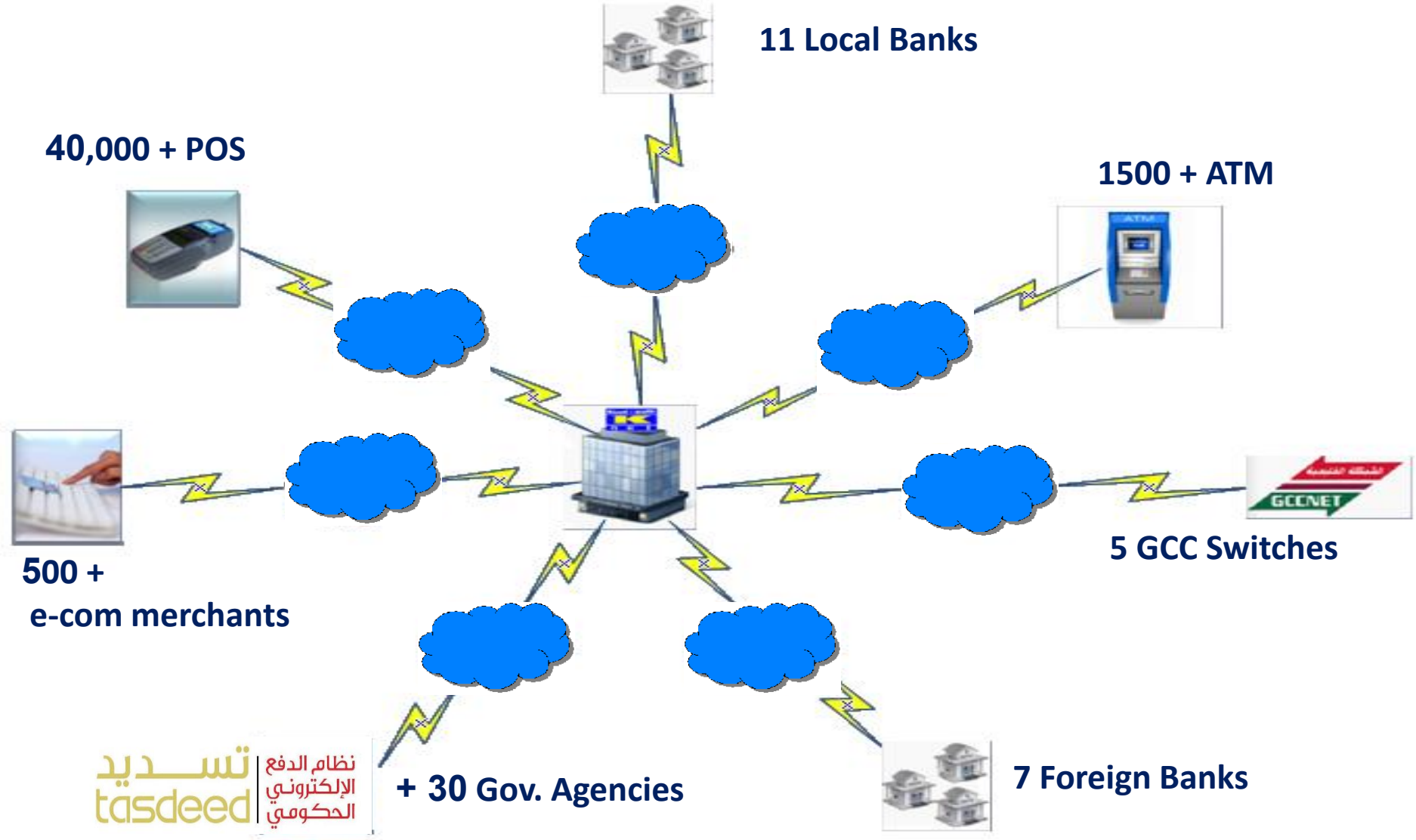
Abdulla Al-Ajmi
General Manager
The Shared Electronic Banking Services Company - Knet
Sunday, 16th November 2014

Agenda

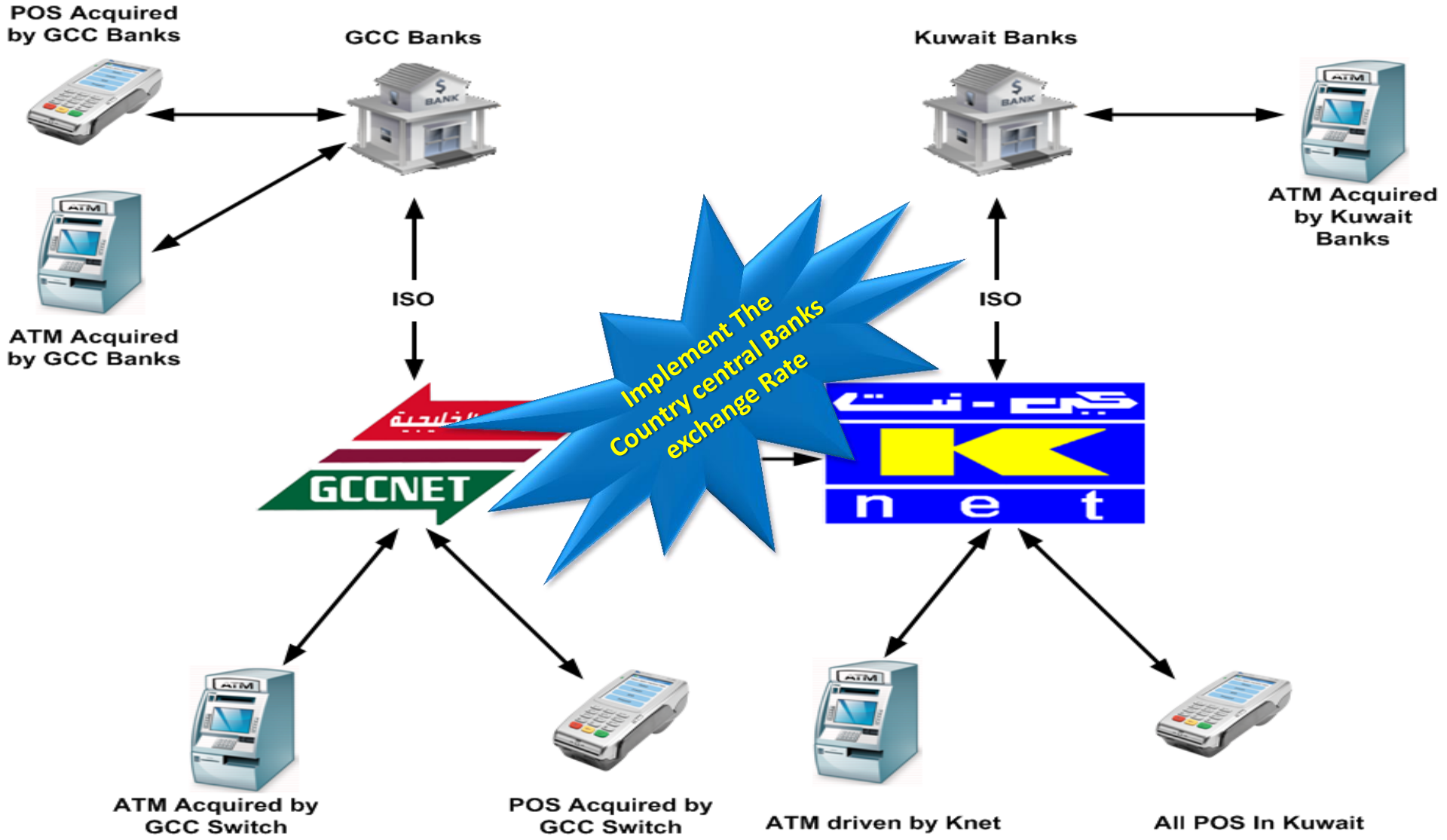
- Introduction
- About Knet
- GCCNet Overview
- GCCNet Regulations
- GCCNet Security
- GCCNet Future

Introduction

About Knet



GCCNet Overview



GCCNet Regulations

Data and Systems Security

Every Switch must fulfil the following requirements prior to ***"live"*** participation in GCCNet;

- Sufficient ***security controls and procedures*** should be implemented to ensure an acceptable level of integrity computer systems, processed information and data generated by those computer systems.

- Conform to the ***security requirements*** relating to key and PIN encryption, transaction processing and card specifications.

- Provide assurance of adherence to GCCNet ***regulations*** and ***standards***.

GCCNet Regulations

Data and Systems Security (Cont'd)

During the ***"live"*** participation in GCCNet, every participating Switch must;

- Encourage their member banks and participating merchants to adopt industry ***"Best Practice"*** standards in relation to the storage and handling of confidential cardholder, merchant and transaction data e.g. ***Payment Card Industry Data Security Standard - PCI-DSS)***.

- Perform regular monitoring and audits in relation to ***security and data integrity controls*** in order to ensure that an acceptable level of data protection and systems security is maintained.

GCCNet Security

Cardholder Verification Method (CVM)

- All GCCNET transactions are subject to on-line authorization by the issuer.
- EMV Cards with PIN are primarily supported.
- Magstripe as a fallback option is supported with a liability Shift
- Both On-line/Offline PIN Verification methods are supported.
- Card Not Present (CNP) transactions are not allowed.

GCCNet Security

Personal Identification Number (PIN)

- Cards issued with a valid Personal Identification Number (PIN) are only accepted.
- Variable length PINs are supported (up to 6 digits).
- The transmission of PINs in clear text format is not allowed.
- The Triple-DES encryption standard is mandated for EMV Transactions.
- PINs must be encrypted using transport keys that are unique to each Bank or Switch (zone encryption).
- PIN translation at the host must be embedded within the hardware. Software based encryption not permitted.

GCCNet Security

Network / Communications

- Participating Switches interconnected by private network links.
- No public communication channels (e.g. Internet) are allowed.
- Message Authentication Code (MAC) are optionally used to further enhance data transmission security of communication messages.

GCCNet Future

- Transition from a closed private interconnected Switches network to open (public) network to facilitate Ecommerce, Mobile commerce…etc. services.

- The successful transition would require enhancements to GCCNet regulations and security controls to protect transactions against the inherent risks of open (public) networks.

Thank you

Moving from Cyber Security to Cyber Resilience

Majed Al-Adwani
Head – IT Security Unit
Central Bank of Kuwait
Sunday, 16th November 2014

Agenda

- The Threat Landscape: Cyber Space, Latest Research on Cyber Threats
- Are Conventional Methods Enough?
- Cyber Resilience
- How others are doing?
- Conclusion

1 The Threat Landscape: Cyber Space, Latest Research on Cyber Threats

Cyber Space: Growth Predictions

Worldwide Internet Users

By end of 2014,
almost 3 billion
From 2.7 billion in 2013
source: ITU[1]

Population 7.1 billion

By 2017,
3.7 billion *source: ITU[1]*

Population 7.4 billion

By 2025,
4.7 billion *source:Microsoft[2]*

Population 7.9 billion

Technology Trends

- Mobile Computing (Smartphones,
- Tablets)
- Internet of Things / Cloud of Things
- Cloud Computing (Shadow IT)
- PCs
- Broadband networks

All this connectivity raises cyber security challenges to a new level

[1] *ITU – ICT Facts and Figures*
[2] *Microsoft Cyberspace 2025: Today's Decisions, Tomorrow's Terrain*

Latest Research: Data Compromise

According to the Verizon 2014 Data Breach report, the **financial sector** experienced the maximum number of confirmed data compromises.

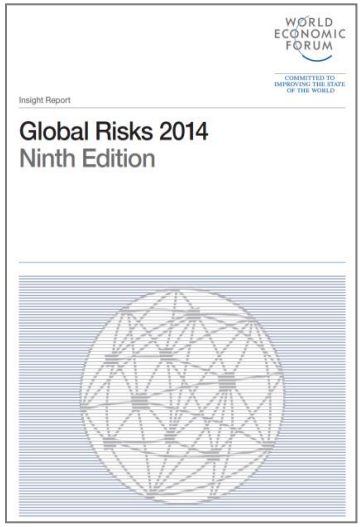
Industry	Total
Accommodation [72]	137
Administrative [56]	7
Construction [23]	2
Education [61]	15
Entertainment [71]	4
Finance [52]	465
Healthcare [62]	7
Information [51]	31
Management [55]	1
Manufacturing [31,32,33]	59
Mining [21]	10
Professional [54]	75
Public [92]	175
Real Estate [53]	4
Retail [44,45]	148
Trade [42]	3
Transportation [48,49]	10
Utilities [22]	80
Other [81]	8
Unknown	126
Total	**1367**

Type of Incident (Finance)	Freq.
Web App Attacks	27%
DoS	26%
Payment Card Skimmer	22%
Insider Misuse	7%
Misc. Error	5%

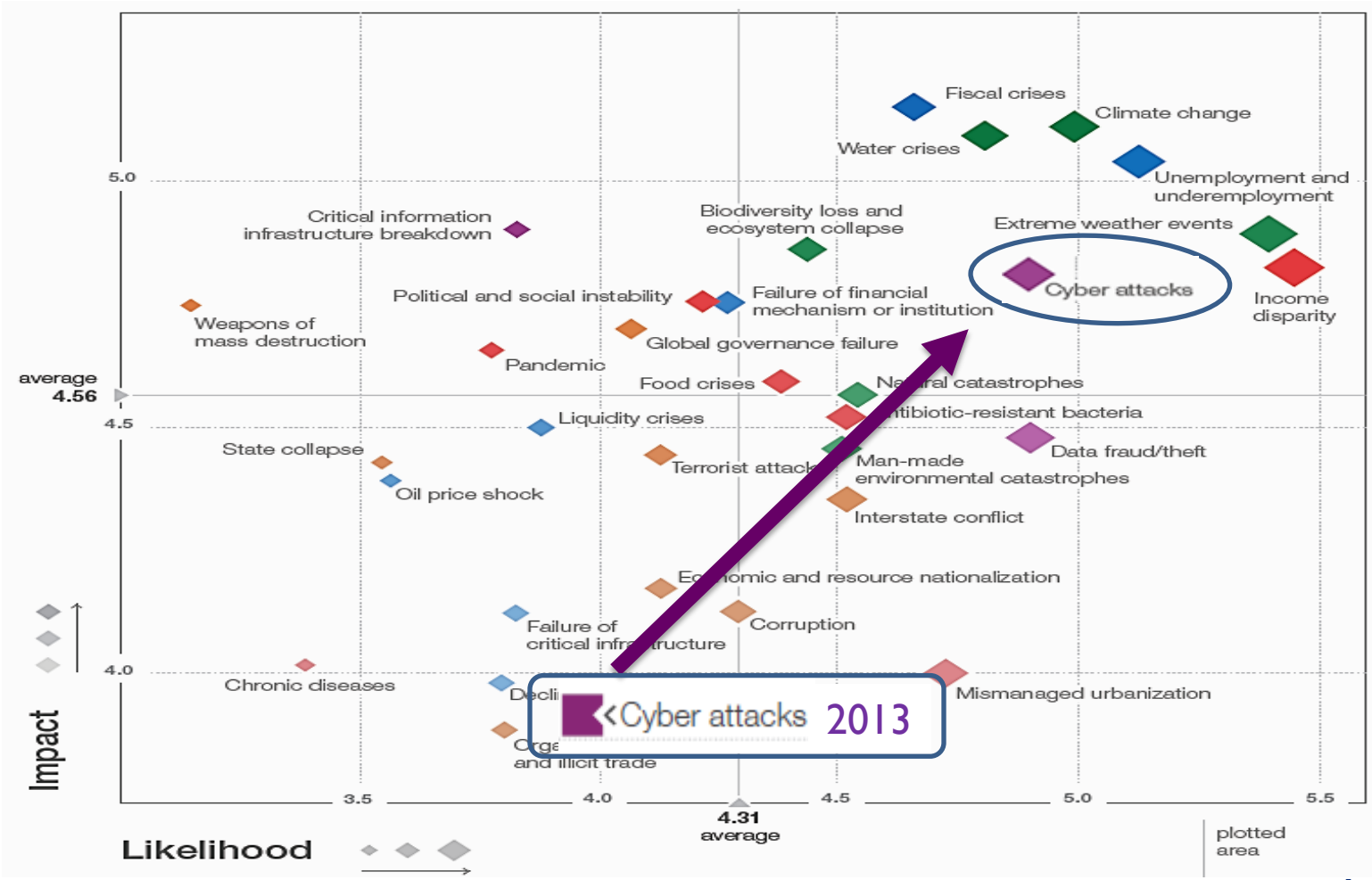
75% of incidents from the Financial sector related to Web App, DoS & Card Skimmer

Latest Research: Cyber Attacks are Rising

Cyber-Attacks are increasing in both in Likelihood and Impact



Economic Risks
Geopolitical Risks
Environmental Risks
Societal Risks
Technological Risks



Recent Cyber Attacks & Vulnerabilities

- Increases in Sophistication
- Low Risk / High Reward
- Evolving Motivations
- High Media Exposure

The Heartbleed Bug

25 September 2014 Last updated at 15:13 GMT

Shellshock: 'Deadly serious' new vulnerability found

By Dave Lee
Technology reporter, BBC News

abcNEWS HOME | VIDEO | U.S. | WORLD | POLITICS | ENTERTAINMENT | TECH

JPMorgan Says Data Breach Affected 76 Million Households

LOS ANGELES — Oct 2, 2014, 8:20 PM ET
By ALEX VEIGA AP Business Writer

Massive Cyber Attack

NEXT VIDEO

BBC News Sport Weather Capital Future Shop

NEWS TECHNOLOGY

Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Environment

3 September 2014 Last updated at 10:56 GMT

Share

Home Depot investigates possible credit card hack attack

It has been suggested that Home Depot might be the [illegible] hacked

REUTERS EDITION: U.S.

HOME | BUSINESS | MARKETS | WORLD | POLITICS | TECH | OPINION | BREAKINGVIEWS

MBIA says some client information may have been illegally accessed

NEW YORK | Tue Oct 7, 2014 1:08pm EDT

0 COMMENTS | Tweet 2 | Share 1 | Share this | 0 | Email | Print

ANALYSIS & OPINION

Revoking passports isn't the way to stop American jihadists from returning home

The Doors of Rabat

RELATED TOPICS

Stocks »
Bonds »
Markets »

Oct 7 (Reuters) - Bond insurer MBIA said on Tuesday it had been notified that some client information at its Cutwater Asset Management unit may have been illegally accessed.

The company said it was conducting a "thorough investigation" and would take all measures necessary to protect customer data and secure systems.

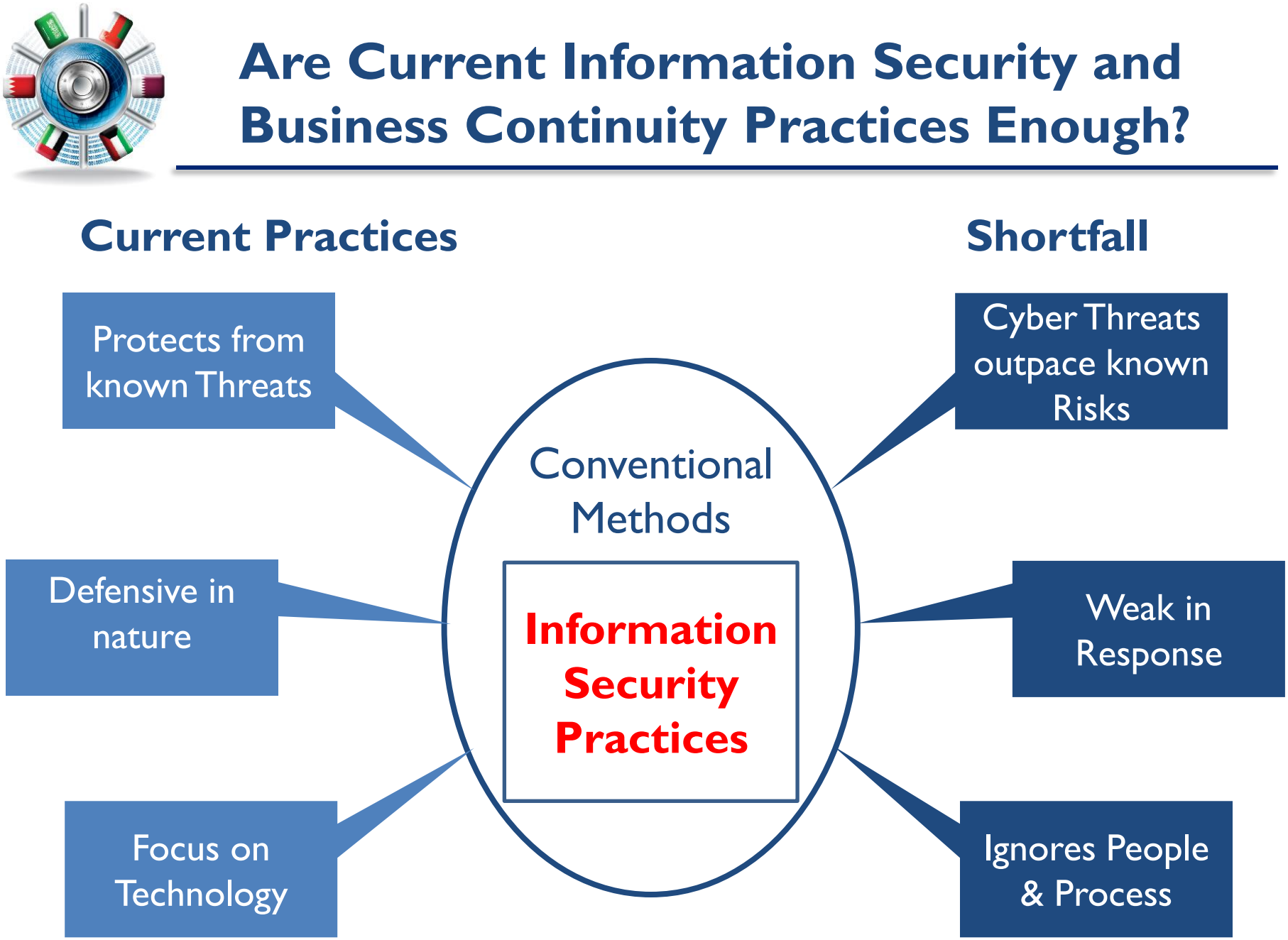
The breach was earlier reported by the KrebsOnSecurity website. For a link to the Krebs story: here

Cyber Threat / Attack Ecosystem

Actors	Vectors	Motives	Targets
Insiders / Competitors	Vulnerabilities in Hardware / Software	Financial Gain	Governments
Hacktivists / E-Fame	Spear Phishing	Competitive Advantage	Financial Services
State Sponsored	APT	Service Disruption	Energy Sector
Criminals	DoS / DDoS	Data Theft	Telecom
	Drive by Download		Retail
	Social Engineering		

2 Are Conventional Methods Enough?

Are Current Information Security and Business Continuity Practices Enough?



Are Current Information Security and Business Continuity Practices Enough?

Current Practices

Focus on physical threats

Exercise performed in closed group

Shortfall

Less Attention to Cyber Threats

Often ignores Dependent parties

Conventional Methods

Business Continuity Practices

Are Current Information Security and Business Continuity Practices Enough?

Current Practices

- Focused on CIA
- Based on Knows Threats
- Priority on IT Systems
- Compliance Centric

Conventional Methods

Testing and Review Practices

Shortfall

- Do not test for Resiliency
- Do not consider Sophisticated attacks
- Overlooks People & Process (Holistic Approach)
- Less Focus on Governance

A New Approach is Needed

Cyber Resilience is the ability of an organization to identify and respond to a cyber attack.
Reference: itgovernance

The focus of Cyber Resilience is Recovery

3 Cyber Resilience

Possible Approaches to a Cyber Resilience Program

Frameworks & Standards: Implementation

- World Economic Forum (2012, 2014)
- NIST - Cyber Security Framework (2014)
- ISO 27001(ISMS), ISO 22301(BCMS)
- ENISA - National Cyber Security Strategies - Practical Guide on Development and Execution (2012)

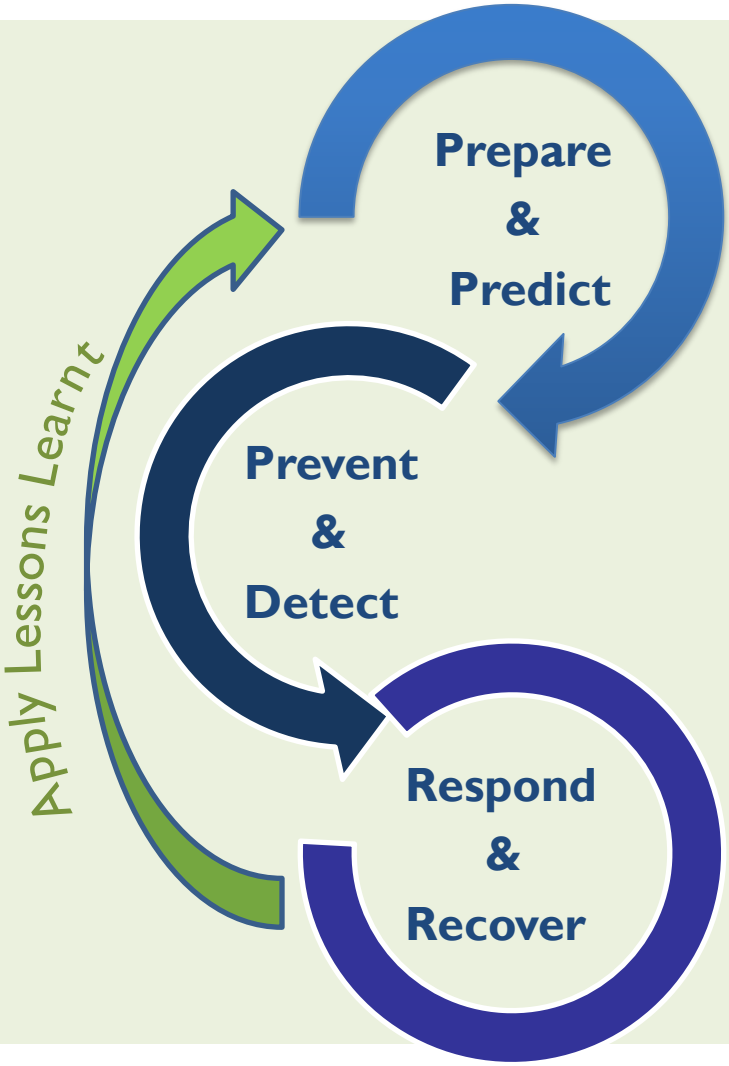
Frameworks & Guidelines: Testing

- CBEST – June 2014
- US CERT - Cyber Resilience Review (CRR)
- Others - Industry guidelines and best practices

CBEST - Framework for cyber resilience tests

- Information Gathering (access to Threat Intelligence, & Skilled analysts)
- Testing by Qualified Pen. Testers based on Advanced Threat Intelligence
- Information Sharing (Collaboration)

Commonalities in Frameworks



- Identify critical assets
- **Prioritize** controls based on business risks, **threat landscape**
- **Situation Awareness** (internal / external)
- Establish Risk Management Strategy & **Desired Maturity level**

- Training & Awareness
- Access Control / Defense layers
- **Do the basics well:** Baselining, Configuration & Patch Management

- **Gather Threat Intelligence,**
- Contain, Coordinate, Escalate, during incidents **(Test your IRP)**
- **Integrate Cyber Security Risks into enterprise RISK management process**

4

How others are doing?

How others are doing?

Bank of England - Waking Shark II, Desktop Cyber Exercise

- **Activity:** Participants from Investment Banks, FMI, Financial Authorities, Government agencies; To perform Desktop Review of cyber attacks (PC wipe, malware, DOS etc.).
- **Objective:** Test the **resiliency** of the financial sector to a cyber-attack; to understand how Org. would manage their response and Information Sharing.
- **Future Considerations:**
  - To establish central communication channel for information sharing and coordination
  - Include more focus on APT, Widen scope for cross border issues

Quantum Dawn 2 Cybersecurity Exercise hosted by SIFMA

5 Conclusion

Conclusion

- 100% protection is not achievable, the question become, what will you do when the inevitable happens?
- **"It's not about technology"** it's about the right authority, the right processes in place and to be ready on an organization level.
- **Cyber Resilience Exercises** are becoming essential in drilling organizing to effectively respond to attacks.
- Organizations **should** focus more on **Governance** rather than **Compliance** to reduce their Risk posture.

Thank You

Bitcoin, Electronic Currency, and Nontraditional Payment Vehicles

Benjamin Edelman

November 16, 2014

About me

- Associate Professor, Harvard Business School
  - Teaching: starting and running tech companies
  - Research: Internet architecture and business opportunities, especially vis-à-vis law and regulation
- Consulting: advertising fraud, privacy, compliance
  - Clients: Advertisers, ad networks, regulators, publishers, investors.
- I speak only for myself.

Topics for today

- Evaluating electronic payment services
- Existing systems
- New entrants
- Mobilization
- Future directions

Evaluating payment services

- Reliability
- Cost
- Speed
- Regulability
  - Anti-money laundering
  - Know your customer
  - …
- Correcting errors
- Preventing abuse
  - Scams
  - Merchandise not as described
  - …

Evaluating payment services

Reliability

Cost

Speed

Regulability

Correcting errors

Preventing abuse

“Bitcoin offers a sweeping vista of opportunity to reimagine how the financial system can and should work in the Internet era”

- Marc Andreessen, coauthor of Mosaic

“The people who rejected the Internet as a curiosity for scientists were on the wrong side of history, the people who rejected digital photography as really an artificial thing were on the wrong side of history, and the people who felt that non-gimmicky tennis racquets were made with wood were on the wrong side of history. … It seems to me that it’s a serious mistake to write this off as either ill-conceived or illegitimate.”

- Larry Summers, former US Secretary of the Treasury

Key Bitcoin Features

No one to ban improper or unlawful transactions.

- "Crypto-currency" providing both store of value and means of exchange.
- No central authority holds the currency or ledger.
- Decentralized "block chain" records.
- Conversion to/from Bitcoin by anyone so inclined.

Low transaction fees?

- How to prevent fake block chains from rogues?
  - Difficult math puzzles. Assume no one can do too many, so finding many answers implies consensus.

Slow. Must wait for chain to record.

"Private"? Anyone who learns your identity once can follow you forever. Or, "mixers" to conceal identity.

Why would a merchant accept Bitcoin?

- Marketing benefits. Free news coverage.
- No chargebacks.
- It's cheaper. Perhaps 1% cost, versus 2%+ for credit cards.

Why would a consumer pay with Bitcoin?

- Merchants that only accept Bitcoin
  - Consider merchants kicked out of card networks
- It's fun, new, and different.
  - How many consumers will this get? Will this last?
- It's cheaper.

Suppose I want to spend US$100 at a merchant that accepts Bitcoin.
My VISA card gives me 2.2% cash back.
If I pay by VISA, I pay $97.80 net.
If I pay with Bitcoin, it costs $100 + 1% exchange fee + 0.2% privacy fee.
If I already have $100 of Bitcoin, I could change that to US$99 and come out ahead.

Evaluating payment services

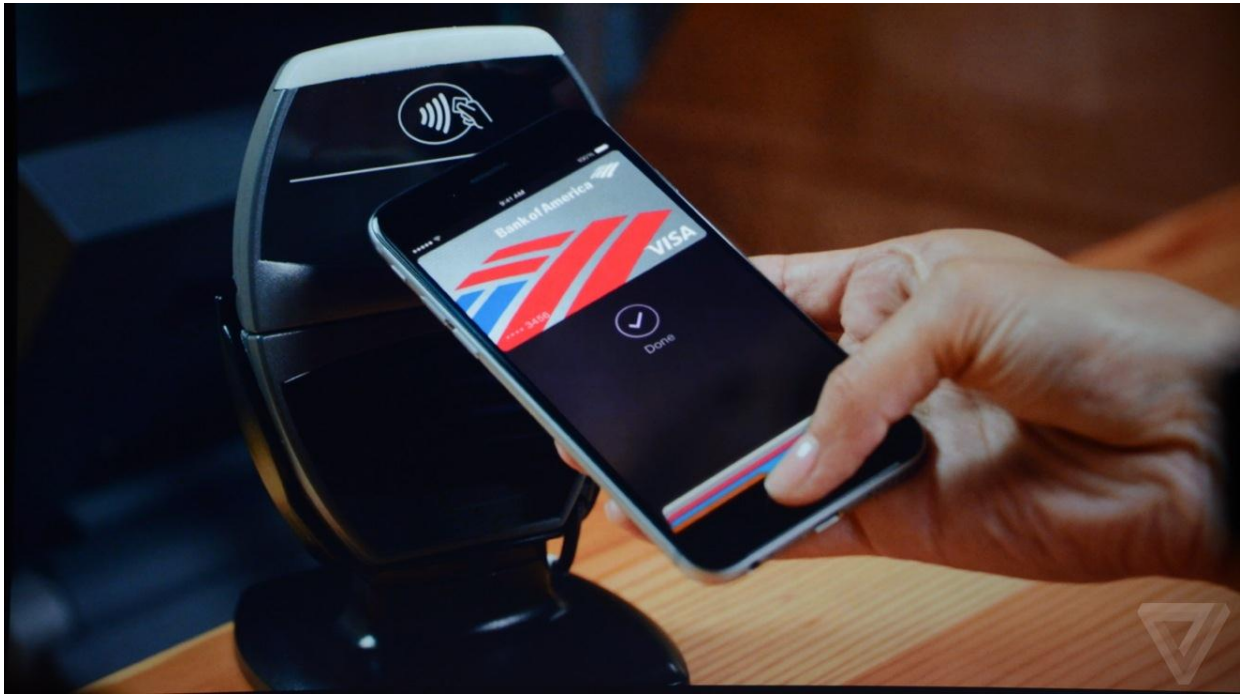
	Cash	Credit Card	Bitcoin
Reliability	○	○	○
Cost	○	○	○
Speed	○	○	
Regulability	○	●	○
Correcting errors		●	
Preventing abuse		●	

Lost your password (“private key”)?

Merchandise not as described?

No solutions provided within Bitcoiin.

Apple Pay



What does Apple Pay solve?

- “I forgot to bring my credit card.”
- “When I lose my card, I get a new number and must update recurring charges… so much work.”
  - Phone presents a revokable token.
- Speed? “Cool” factor?

BUT

- “Battery low.”
- Credit card costs unchanged.
- Not widely accepted. Costly to upgrade all POS.
- Do consumers care about security? Should they?

Launching a new payments service

- Mobilizing both consumers and merchants
- How to attract consumers?
  - Rebates/points
- How to attract merchants?
  - The consumers are already signed up.
- Implications
  - Smart consumers choose the payment service with the highest benefit.
  - Merchants' payment costs go up and up.

Looking forward

- Payments innovation is slow and costly.
  - Upgrading POS
  - Convincing consumers to use
- Payment innovators have a mixed to poor track record at cutting costs .
- Smart consumers figure out what's in their best interest.

Price Coherence and Excessive Intermediation*

Benjamin Edelman† and Julian Wright‡

October 2014

Abstract

Suppose an intermediary provides a benefit to buyers when they purchase from sellers using the intermediary's technology. We develop a model to show that the intermediary would want to restrict sellers from charging buyers more for transactions it intermediates. With this restriction an intermediary can profitably raise demand for its services by eliminating any extra price buyers face for purchasing through the intermediary. We show that this leads to inflated retail prices, excessive adoption of the intermediaries' services, over-investment in benefits to buyers, and a reduction in consumer surplus and sometimes welfare. Competition among intermediaries intensifies these problems by increasing the magnitude of their effects and broadening the circumstances in which they arise. We discuss applications to payment card systems, travel reservation systems, rebate services, and various other intermediaries.

European Cybersecurity Strategy and Related Directives: Legislative and Regulatory Approach

Rolf von Roessing
CISA, CISM, CISSP, CGEIT, FBCI
Central Bank of Kuwait
Sunday, 16th November 2014

ISACA Serving IT Governance Professionals

FORFA AG Holding

Agenda

- The European Approach as a top-down initiative
- Strategic Level: European Union, Member States and the Financial Sector
- Tactical Level: Combining Legislation & Regulation and Good Practice
- Operational Level: Frameworks and Tools
- Conclusions and Outlook

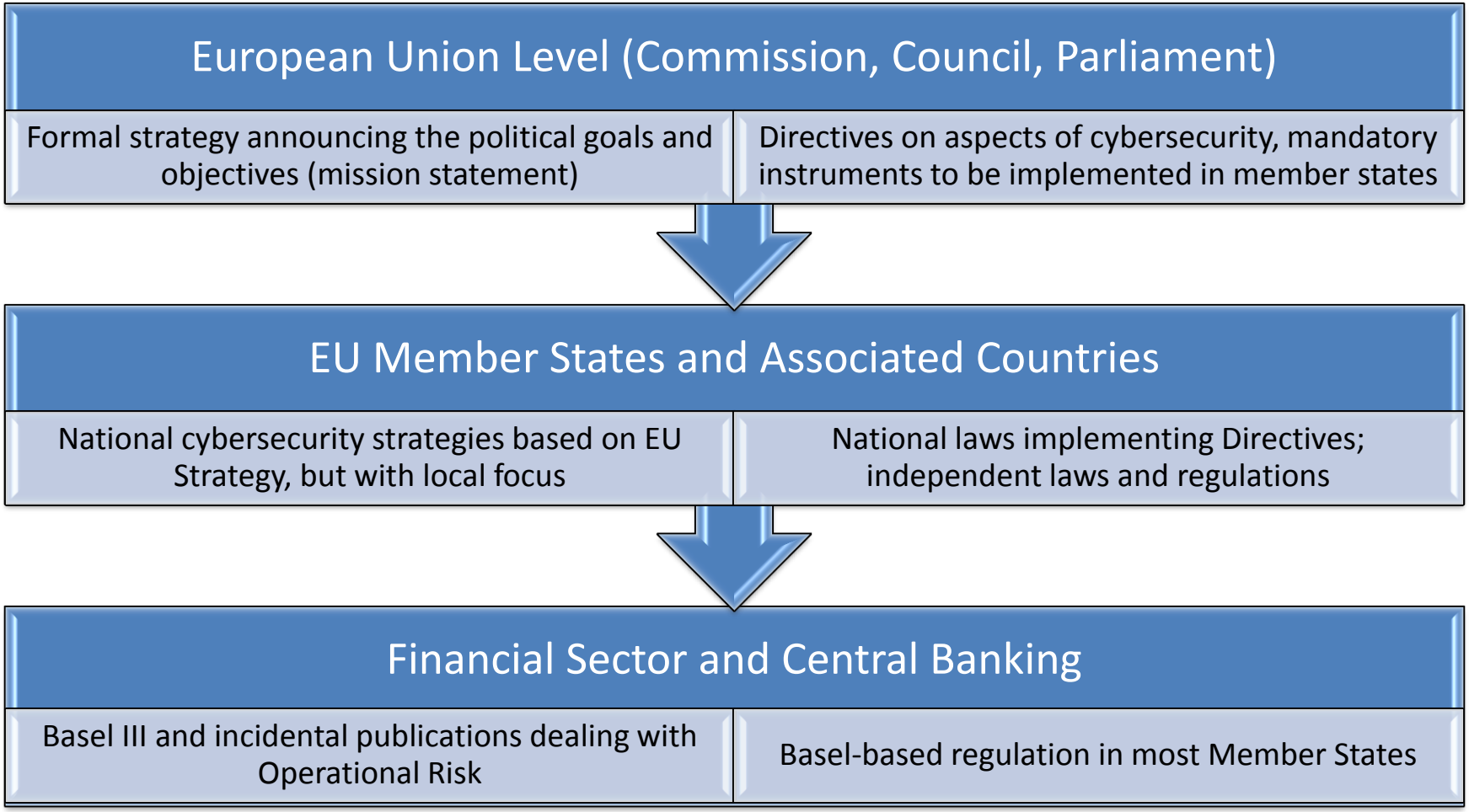
European Cybersecurity Strategy

THE EUROPEAN APPROACH AS A TOP-DOWN INITIATIVE

The European Approach as a Top-Down Initiative

- Rising tide: cybercrime and cyberwarfare are becoming more aggressive, and in some cases more successful
- Globally, nation states and their governments are proposing and implementing cybersec initiatives – with massive spending
- In the EU, the initial definition of a cybersec strategy is being followed by multiple tactical initiatives
- Laws and regulations are emerging, covering a multitude of technical, organisational and behavioural aspects
- ENISA, ISACA and several national institutions are increasing their effort to innovate and roll out practical solutions
- Industry is beginning to realise that cutting costs may not be the right answer to the threat

The European Approach as a Top-Down Initiative (2)



Background to the Approach

- EU started their security thinking in 2004 by founding the ENISA (European Network and Information Security Agency) which has since been the primary body to recommend strategies and measures
- Increasing cyber crime and cyberwarfare as well as the changing game in IT use (including finance) prompted the development of the cybersecurity strategy
- Interestingly, the EU utilises a two-pronged approach:
  - Mandatory: directives (e.g. privacy, telecomms) to invoke national legislatory mechanisms
  - Discretionary: recommendations, free (ENISA) advice and studies, aspirational documents
- The strategy is as much a mission statement as it is a foundation for national strategies. Much of it is – by necessity – political, signalling commitment and long term thinking

European Cybersecurity Strategy

STRATEGIC LEVEL: EUROPEAN UNION, MEMBER STATES AND THE FINANCIAL SECTOR

Union

- 28+ participating countries
- lowest common denominator in terms of political will and consensus
- It is remarkable that despite the diversity of opinion, the cybersecurity strategy has actually materialised
- Legislative powers of the EU supersede (!) national powers
- Any formal lawmaking shall be implemented at the national level rather than at Union level
- As a result, nations must implement the minimum (or more) of what Directives stipulate
- Cybersecurity, digital economy etc. are now represented by a dedicated commissioner

Member States

- Most member states have mirrored the EU Strategy, implementing their own versions with certain local priorities
- National lawmaking is aligned with EU Directives
- Best practice is shared through ENISA and other non-governmental organisations
- Some member states (e.g. Germany) operate their own national information security agencies
- The financial sector is heavily intertwined and linked to these processes
- Central banks and/or supervisory authorities may be empowered to drive cybersecurity in a regulatory and audit sense (e.g. the German draft Information Security Act)

Financial Sector

- Central and business banking is governed from two worlds:
  - Basel III and incidental materials, resulting in regulation
  - National legislation, often more restrictive in terms of curtailing banks' powers
- ECB and national central banks operate independently, including regulation
- Supervisory authorities provide additional safeguards and regulatory sanction
- In cybersecurity, the following picture is emerging:
  - Regulation and supervision tend to fall to the supervisory authorities rather than central banks proper (e.g. Germany, UK)
  - Cybersecurity is placed firmly in oprisk, but it appears to be taking on its own life as a specialised subject
  - In some cases (e.g. Germany), additional supervisory bodies may be created or empowered to support cybersecurity governance
  - Banks are classified as critical infrastructure and therefore at the crossroads of national security, civil defence, intelligence and law enforcement

European Cybersecurity Strategy

TACTICAL LEVEL: COMBINING LAWS & REGULATIONS AND GOOD PRACTICE

Combining Laws and Regulations

- European legislation usually shows restraint and remains broad and high-level
- Legal development is achieved by amending existing banking laws
- The regulatory side combines national laws and Basel III, sometimes using Basel materials verbatim (e.g. France)
- Regulation is generally more detailed, often with additional (informative) guidance
- In some cases, reference is made to existing formal standards issued by national agencies

Combining Laws & Regs with Good Practice

- Good practice in Europe often exists as:
  - Formal standards issued by national agencies (but non-binding)
  - Formal standards issued by ISO
  - Informal frameworks such as COBIT5
- ENISA as the official EU body issues a wide range of guiding documents, as well as surveys and market intelligence
- Good practice is integrated by:
  - the way in which supervisory authorities audit and review
  - benchmarking and accepted practice (includes banking sector)
  - gradual adoption or alignment of the above sources into more formal publications, usually through cross-references
- Central banks and supervisory authorities must tread a fine line between being overly orthodox (literal interpretation) and being too hands-off (laissez faire)
- To date, it has turned out that some degrees of freedom granted to financial institutions are advantageous: they produce more innovation and allow for quicker reaction to «disruptive technologies» etc.

European Cybersecurity Strategy

OPERATIONAL LEVEL: FRAMEWORKS AND TOOLS

Cybersecurity in Practice

- Banks tend to use a blend of tools and frameworks in cybersecurity:
  - Formal guidance as the skeleton
  - Inclusion of ISO, ISF, ENISA and other semi-formal guidance and recommendations
  - Inclusion of Basel incidental papers (e.g. Joint Forum publications)
  - Traditional use of COBIT5 as the common audit language
  - Almost traditional use of ISO 27001 as the overarching management system for information security

ISACA's European Initiatives

- S22 and subsidiary activities clearly address Europe as an important area
- ISACA formally and informally engages with external stakeholders through a number of Boards and Committees
- At the EU level, there are a number of joint research and development projects with ENISA
- At the Member State level, there a many joint initiatives with national authorities (e.g. UK, GER)
- In practice, many SMEs are permanent guests or observers in key committees at the national level, covering industry associations as well as other institutions
- The first set of targeted European publications is available for download

COBIT Related Publications in Cybersecurity

- COBIT5 for Information Security (2012)
- Transforming Cybersecurity Using COBIT5 (2013)
- Responding to Targeted Cyberattacks (2013)
- Securing Mobile Devices Using COBIT5 (2012)
- European Cybersecurity Implementation Series (2014)
- more to follow, see the Cybersecurity Nexus at www.isaca.org

European Cybersecurity Strategy

CONCLUSIONS AND OUTLOOK

Conclusions and Outlook

- The EU has managed to reach consensus with regard to strategy and political mission
- Most member states have been quick in following up with national strategies
- The regulatory (Basel) side is well aligned, central banking and supervisory reviews are functional
- More and more actors in the financial sector are looking at ENISA and practical guidance from other sources (e.g. COBIT) to enable hands-on implementation
- Given the unfortunate speed at which cybercrime and cyberwarfare are growing, a pragmatic approach is required
- The near future will show what spearheading national initiatives (e.g. laws) can achieve

About ISACA

With 95,000 constituents in 160 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the non-profit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfil their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

ISACA®
Serving IT Governance Professionals

Contact Details

Forfa AG provides independent advice on GRC, all aspects of security, and business resilience (including BCM and ITSCM).

Forfa AG Holding
Andhauser Str. 62
8572 Berg TG, Switzerland
Phone: +41 71 460 2181
mobile: +49 172 6712322
rvr@scmltd.com
skype: rvrscm

Alternatively, Rolf may be reached through ISACA HQ. Please feel free to ask any questions, provide comments or suggest improvements.

Making Leaders Successful Every Day

Tackling Fraud: The Next Frontier

Andras Cser, VP Principal Analyst

November 16, 2014


Mobile fraud management and
Behavior modeling fraud management
market growth.

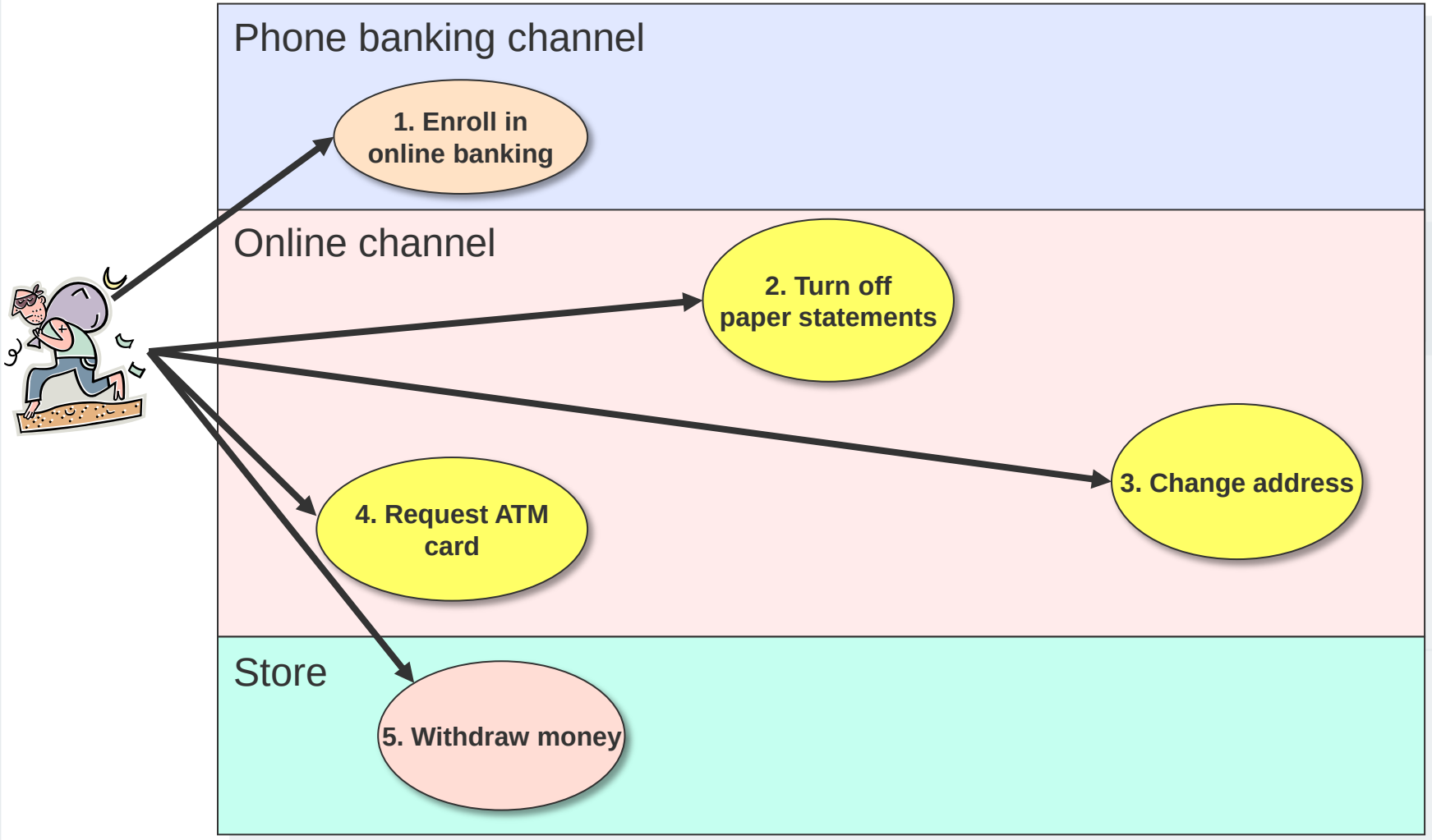
Agenda

- Trends and requirements in fraud management
- Fraud Management high-level architecture and taxonomy
- Behavioral analytics in fraud management
- Mobile fraud management
- Forrester’s recommendations and predictions

Organizational Challenges Around Fraud Management

- LOBs use different types of fraud management solutions.
- Lack of internal information sharing:
  - Risk scores, model parameters, rule templates
  - Entity whitelists and blacklists
- Internal / M&A religious wars around:
  - Products
  - Real-time versus batch-based
  - Statistical versus rules-based
- Poorly documented and tracked patterns for fraud
- Data integration ownership

It’s All Cross Channel



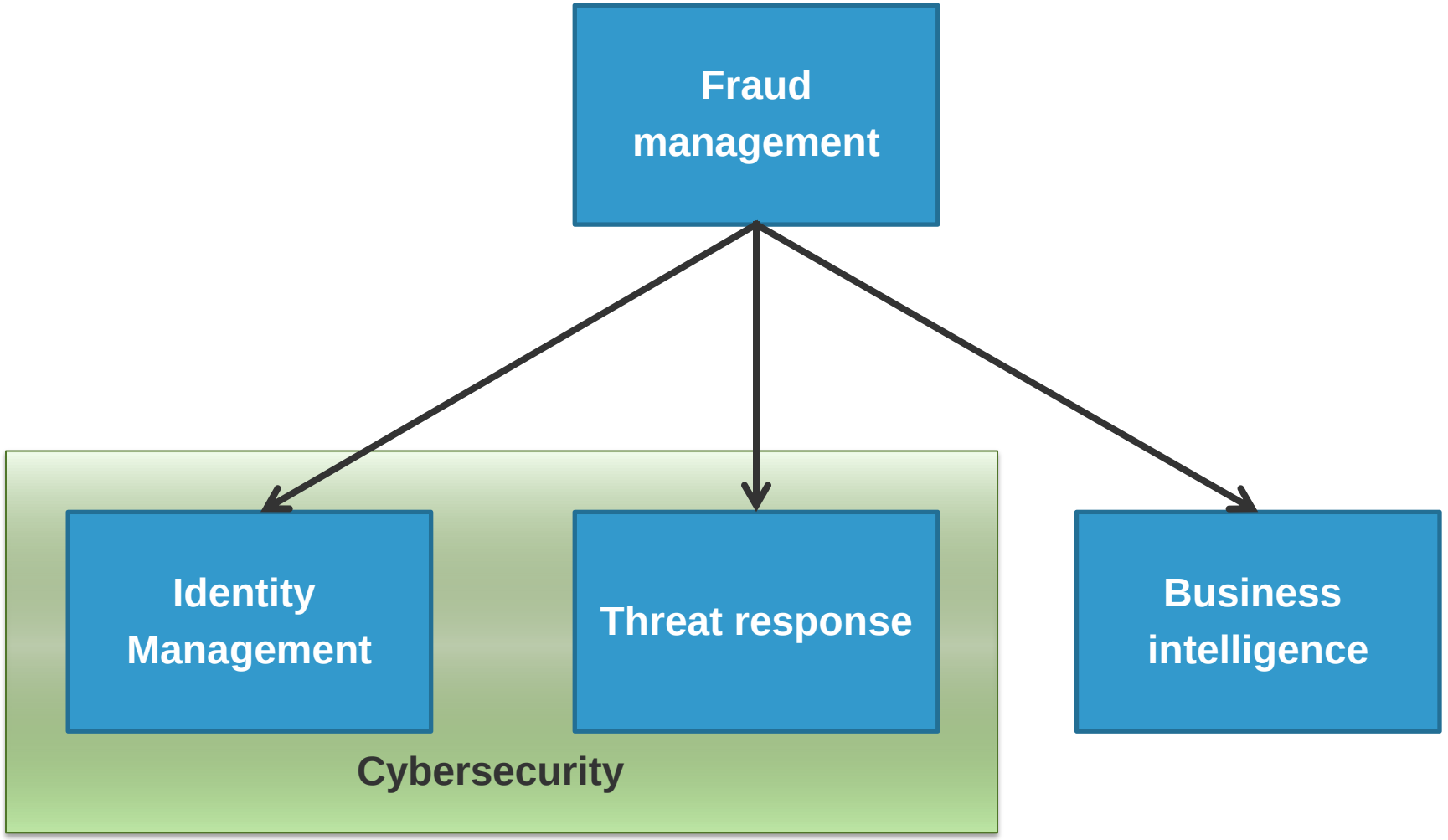
It's A Delicate Balance And A Hard Problem To Solve

Operational Efficiency

Fraud Management Efficiency

Customer Satisfaction

Why Do It?: “By-products” Of Better Fraud Management



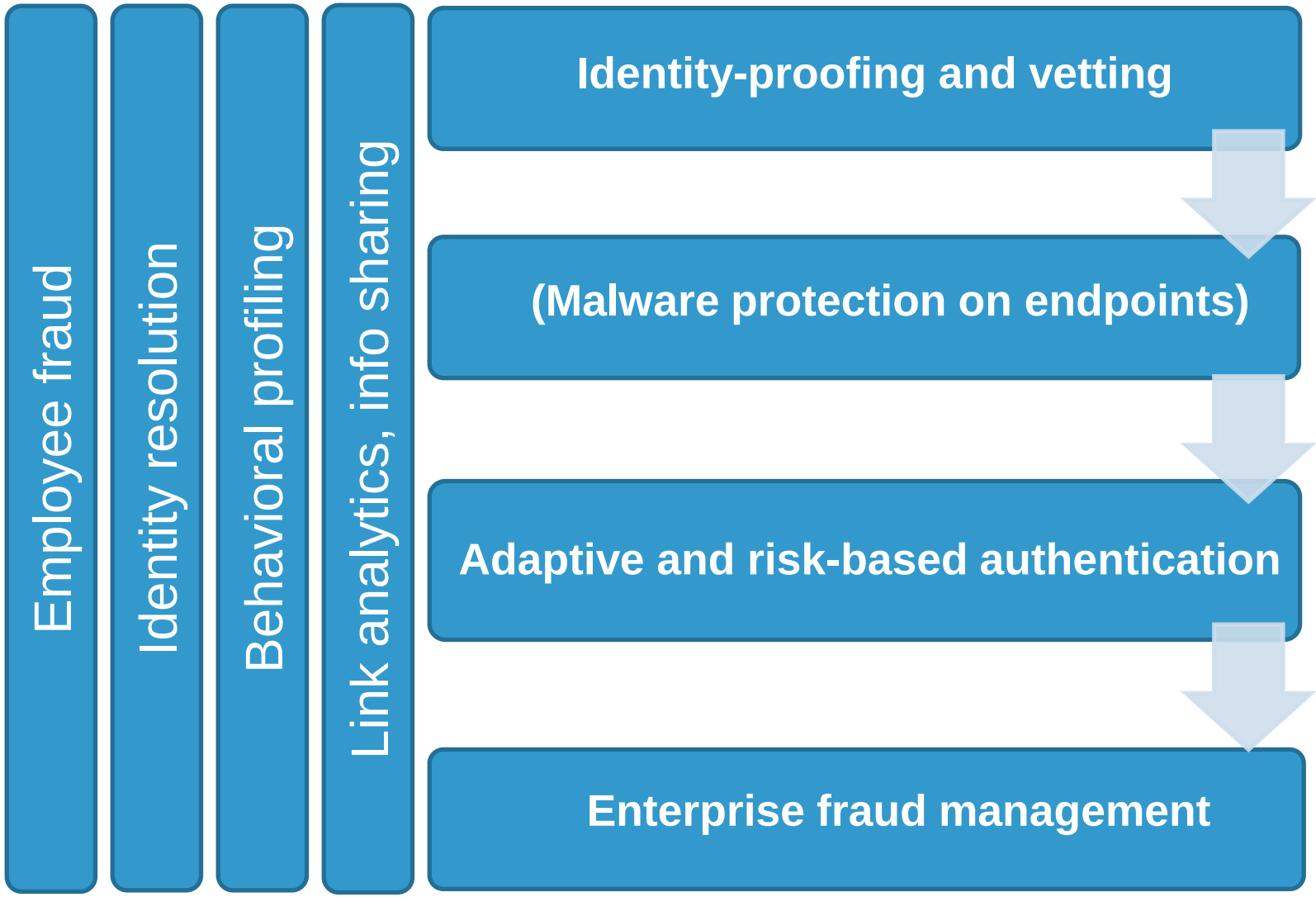
Fraud Management Market Trends

- Increased **sophistication** (3 way fraud schemes, MITB/MIM attacks) requires predictive analysis capabilities
- New **interlinked** areas of fraud (retail, airlines, gaming)
- **Organized** crime with customer service, warranties for CC numbers
- **Mobile** device uptake for perpetration
- Need for vendor **collaboration for sharing** fraud data
- **Check fraud** on the rise
- Online **account opening** fraud
- **ACH and wire** fraud
- **Cross channel** fraud expansion

Agenda

- Trends and requirements in fraud management
- Fraud Management high-level architecture and taxonomy
- Behavioral analytics in fraud management
- Mobile fraud management
- Forrester's recommendations and predictions

Fraud Management Architecture



Channel/ Task	Web/mobile web 	Mobile device 	Voice 	In person 
Identity proofing	Mature: KBA	Immature: None	Mature: KBA	Immature: ID cards
Device fingerprinting	Mature: fonts, installed SW	Medium: SDKs	Immature: obsolete	N/A: Immature
Authentication	Medium: Pa55w0rds!, OTP	Immature: Pa55w0rds!	Mature: SSN, DOB, ZIP, obsolete	Immature: ID cards, obsolete
Step up authentication	Medium: RBA, OTP	Immature: RBA, OTP, not out of band	Immature: SSN, DOB, ZIP, dangerous	Immature: ID cards, obsolete
Transaction monitoring	Mature	Immature: lacking context	Immature: lacking context	Immature: employee fraud

Agenda

- Trends and requirements in fraud management
- Fraud Management high-level architecture and taxonomy
- Behavioral analytics in fraud management
- Mobile fraud management
- Forrester's recommendations and predictions

Big Data

Volume

Velocity

Variety

Breadth of shared and consortium information

Agenda

- Trends and requirements in fraud management
- Fraud Management high-level architecture and taxonomy
- Behavioral analytics in fraud management
- Mobile fraud management
- Forrester's recommendations and predictions

Mobile Fraud Management

- What does mobile mean? SMS?, eWallets?, NFC?, QR?
- It's data integration for EFM systems using
  - Geolocation
  - Device usage patterns
  - Mobile device fingerprinting
- Apple Pay uses secure element used for storing tokenized CC numbers, unlock with TouchID fingerprint (not strong authN)
- Rich context not used today
- Samsung Galaxy S5/Alpha and Apple iPhone 5s/6/6+ TouchID reader is open to developers
- Will MNOs be involved? They should, but they won't

Agenda

- Trends and requirements in fraud management
- Fraud Management high-level architecture and taxonomy
- Behavioral analytics in fraud management
- Mobile fraud management
- Forrester's recommendations and predictions

Forrester's Recommendations

- Encapsulate AML/KYC/Compliance and Cyber Security in Fraud Management
- Infuse Behavioral analytics
  - Network
  - Authentication
  - Back end transactions
- Expect Big Data to impact analytical models, in-memory processing
- Mobile device identification
- Link analysis visualization
- Reporting and auditing and balanced fraud dashboards

Forrester's Predictions

- Machine learning will auto-tune models
- Magstripe+EMV+Contactless payment terminals adoption in the US will push eWallets
- Mobile payments going contactless
  - Apple Pay
  - HCE (Android KitKat)
- EMV Chip will be eclipsed worldwide by contactless
  - EMV Chip is old
  - No US adoption of EMV Chip
- More than PIN numbers in authentication
  - Voiceprint biometrics
  - Fingerprint biometrics

Forrester's Predictions (cont'd)

- Fraud management vendors will provide SDKs for mobile devices for on-device transaction context reading
- Fraud management vendors will want to get increasingly into payment-time / card authorization-time authentication using risk based authentication and biometrics
- Payment networks will adopt fraud management increasingly
- NFC / contactless payments are the future
  - Ease of use
  - Better security
  - Authentication


Bon Appétit! ☺
CAVIAR

Thank you

Andras Cser

+1 617.613.6365

acser@forrester.com

forrester.com