Strengthening your fraud and cyber-crime protection controls

March 2017

Audience question:

What is your role within your institution?

a) Payment operations / cash management / treasury services

b) Compliance

c) IT / Technology

d) Security / information security

e) Other

Speakers

Name	**David Ferbrache**
Position	*Technical Director Cyber Security, KPMG UK*
Relevant experience	David has over 25 years experience of all aspects of cyber defence dealing with the most sophisticated and disruptive cyber attacks, and the is the lead for Cyber Defence Services in the UK — Previously Head of Cyber and Space for the Ministry of Defence in the UK. Defending MOD against high end cyber threats, leading cyber policy for MOD and international relations on cyber issues, sponsor for the Defence Cyber Security Programme. MOD lead on Central Government cyber contingency planning and exercises — Extensive experience of threat scenario development and cyber risk assessment, including previous end-end security assessments for UBS, and for over a dozen financial institutions in the UK and Switzerland — Board and executive committee engagement on cyber security issues, including design and delivery of senior cyber wargaming and exercising of diverse cyber attack scenarios

Name	**Bedria Bedri (Bia)**
Position	*Partner, Cyber Security, KPMG UK*
Relevant experience	Bia is an experienced consultant with 20 years industry knowledge, leading large-scale complex transformation and change programmes to enable clients to effectively manage emerging cyber threats, risk and regulatory expectations whilst delivering business objectives, innovation and growth. — As a Partner, Bia's focus has been developing client relationships in the market with a very strong network of organisations at senior levels who trust Bia as an advisor and delivery lead. — Bia's clients include leading global banks, where consistent high quality, leadership and partnership with clients has been key to a successful track record in delivering clients' multi-million pound programmes, managing large teams of 50+ in multiple geographies including client teams and third party suppliers. — Bia has excellent communication skills and is well traveled with advisory experience gained in the UK, EMA, ASPAC, and the Americas. — Bia publishes in the UK and global media as a thought leader in cyber security space and has links into business and academia such as Royal Holloway, University of London.

Speakers

Name	**Dr. Tony Wicks**
Position	*Head of AML and Fraud Prevention Initiatives*
Relevant experience	For over 20 years, Tony has worked with leading financial institutions to provide technology solutions for regulation, compliance and fraud detection. Tony is currently working as part of the SWIFT Customer Security Programme, heading up Your Counterparts focus area. Working in Financial Crime Compliance at SWIFT, Tony is creating utility based solutions to help institutions meet their financial crime compliance obligations. These solutions help institutions maintain AML and sanctions compliance, manage regulatory risk, prevent fraud, and ensure effectiveness and increase efficiency. Tony holds a PhD in Signal Processing from the University of Warwick.

Audience question:

What do you think are the greatest areas of weakness to cyber-threats? (pick three)

a) Human factors

b) Email compromise

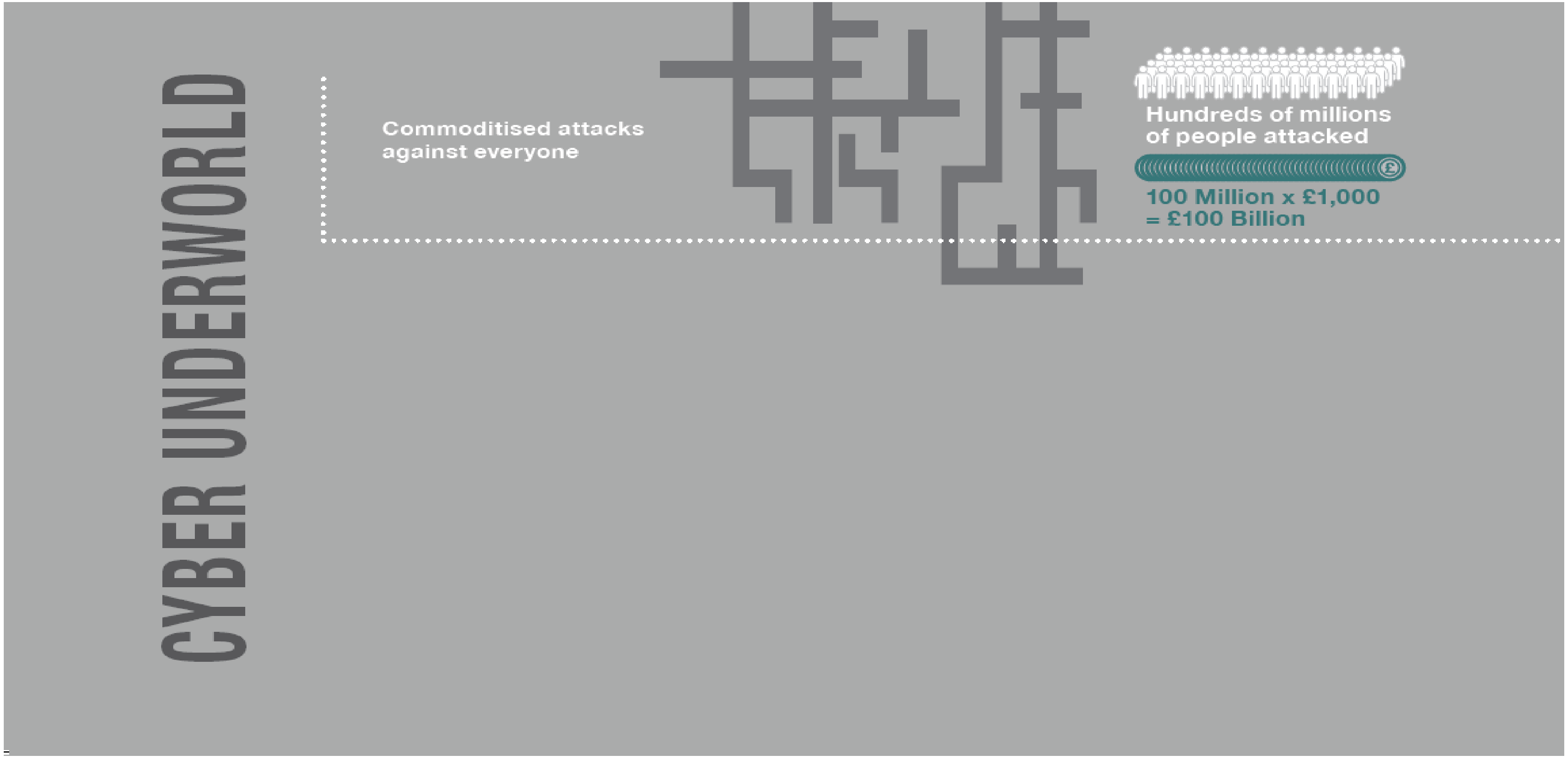
c) Infra-structure and connectivity

d) Computing environment

e) Physical security controls

Cyber Security Risks to SWIFT Members

Ruthless and Rational Entrepreneurs



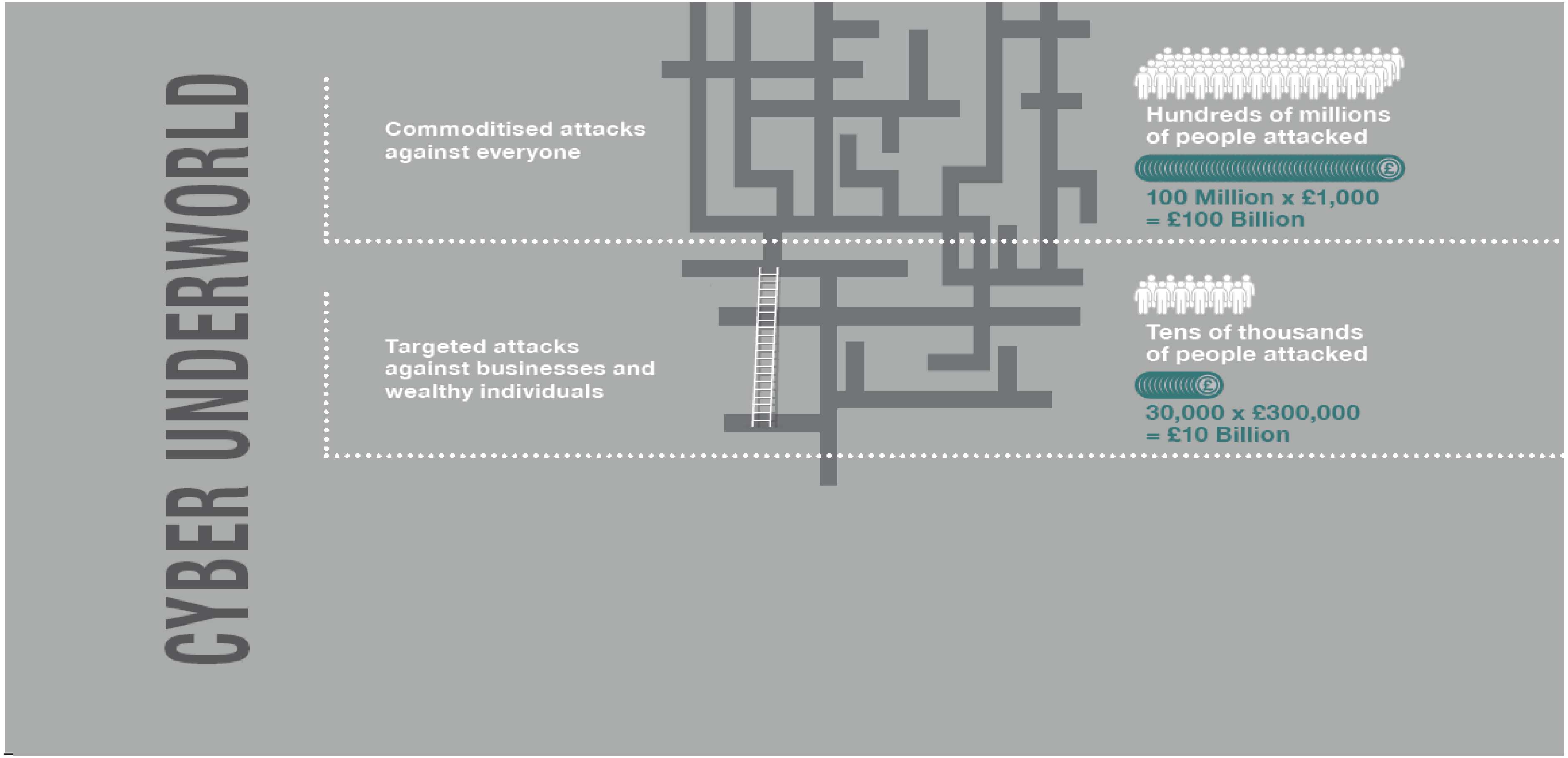
CYBER UNDERWORLD

Commoditised attacks against everyone

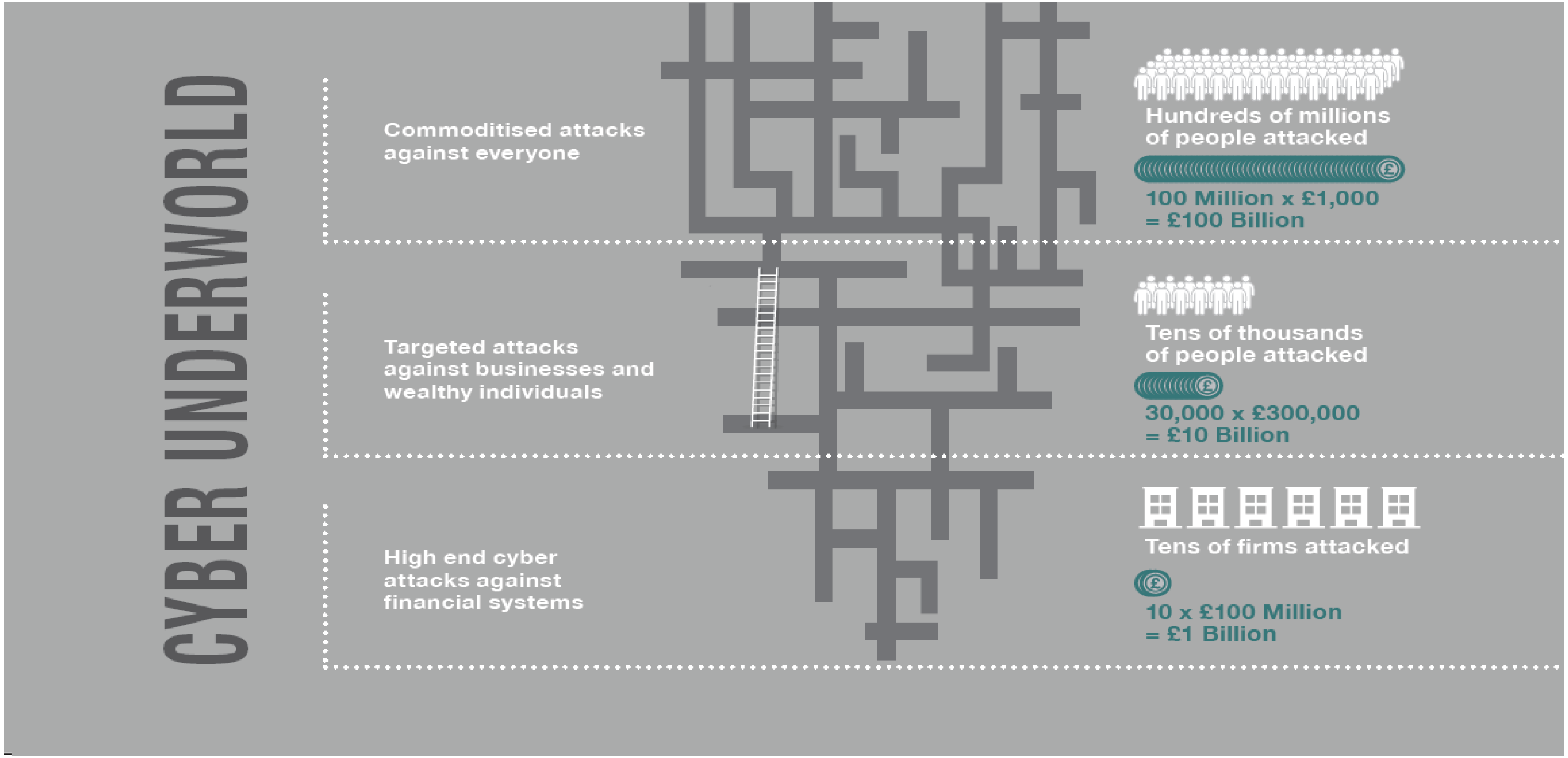
Hundreds of millions of people attacked

100 Million x £1,000
= £100 Billion

Ruthless and Rational Entrepreneurs


CYBER UNDERWORLD
Commoditised attacks against everyone
Hundreds of millions of people attacked
100 Million x £1,000 = £100 Billion
Targeted attacks against businesses and wealthy individuals
Tens of thousands of people attacked
30,000 x £300,000 = £10 Billion

Ruthless and Rational Entrepreneurs



CYBER UNDERWORLD

Commoditised attacks against everyone

Hundreds of millions of people attacked

100 Million x £1,000
= £100 Billion

Targeted attacks against businesses and wealthy individuals

Tens of thousands of people attacked

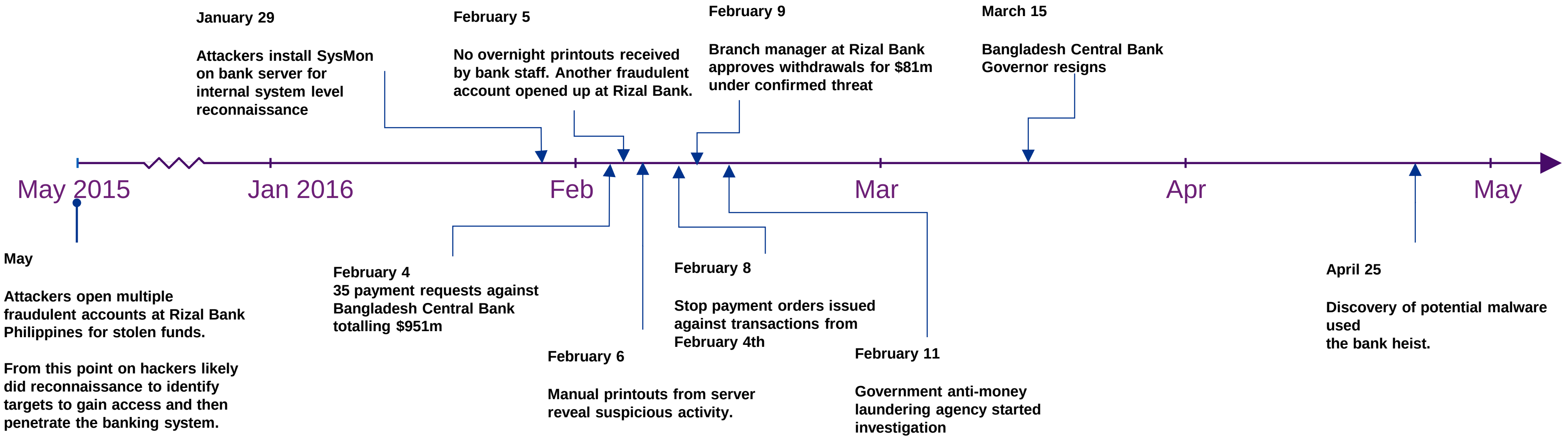
30,000 x £300,000
= £10 Billion

High end cyber attacks against financial systems

Tens of firms attacked

10 x £100 Million
= £1 Billion

Funds Transfer Attacks



May

Attackers open multiple fraudulent accounts at Rizal Bank Philippines for stolen funds.

From this point on hackers likely did reconnaissance to identify targets to gain access and then penetrate the banking system.

January 29

Attackers install SysMon on bank server for internal system level reconnaissance

February 4
35 payment requests against Bangladesh Central Bank totalling $951m

February 5

No overnight printouts received by bank staff. Another fraudulent account opened up at Rizal Bank.

February 6

Manual printouts from server reveal suspicious activity.

February 8

Stop payment orders issued against transactions from February 4th

February 9

Branch manager at Rizal Bank approves withdrawals for $81m under confirmed threat

February 11

Government anti-money laundering agency started investigation

March 15

Bangladesh Central Bank Governor resigns

April 25

Discovery of potential malware used
the bank heist.

February 2016 - Bank of Bangladesh

June 2016 – Ukrainian Bank attacked

October 2016 – Multiple countries

Possible links to Carbanak – Russia

Audience question:

What measures are most effective in dealing with insider frauds and cyber threats?

a) Staff training and awareness

b) Employee vetting

c) Enhanced IT security / logging and control

d) Penetration testing

e) Fraud detection tools

Security Good Practice – Basic Hygiene

Protecting the Environment	Protecting the Business	Detection, Response & Recovery
Policy & Standards (defined and consistently applied)	**Education & Awareness** (awareness of threats, risks, policies, remote/home working, incident reporting)	**Security Monitoring** (continuous policy monitoring, critical events, threat intel)
Network Security & Architecture (internal, external, perimeter, segmentation, content / malware scan)	**Business Access Management** (business roles, JML and periodic Certification)	**Log & Intelligence Analysis** (unusual events or anomalies indicating suspicious trends or attacks)
Infrastructure Maintenance (unsupported s/w, patching, configuration)	**Organisational Culture** (employees are the first line of defence, malware, phishing)	**Response** (planning, analysis, containment, mitigation)
Access Management (roles, SoD, joiner, mover, leaver, privileged)		**Recovery** (planning, capability, communication)
Physical Access (social engineering, 3rd party, unauthorised devices, removable media		**Continuous Improvement** (ongoing improvement)

People | **Processes** | **Technology**

Information & Cyber Security Frameworks

ISO 27001 Information Security	NIST Cyber Security Framework	CESG 10 Steps to Cyber Security	Cyber Essentials Certification Scheme	ISO 27032 Cyber Space	PCI-DSS / Swift / other

KPMG

KPMG

Bia Bedri
Partner, Cyber Security

Tel: +44 (0) 207 311 5278
bedria.bedri@kpmg.co.uk

David Ferbrache
Technical Director, Cyber Security

Tel: +44 (0)7545 124116
david.ferbrache@kpmg.co.uk

kpmg.com/uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

For full details of our professional regulation please refer to 'Regulatory Information' at www.kpmg.com/uk

Audience question:

What measures do you already apply in your business to address cyber-threats? (tick all that apply)

a) Two-factor authentication

b) Maker checker (four-eyes) review

c) Anti-virus

d) Payments reconciliation

e) Fraud detection

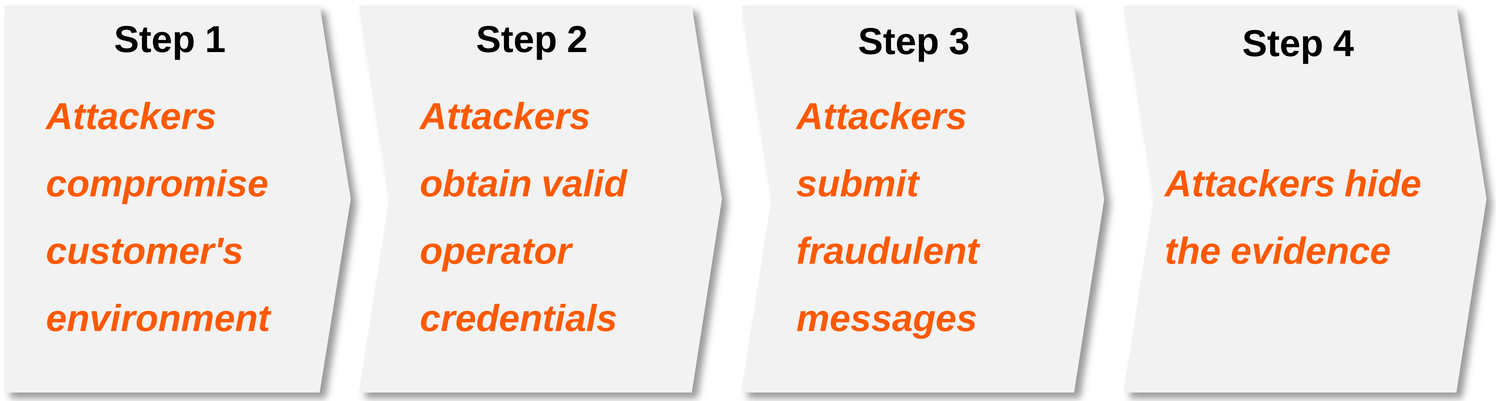
SWIFT Customer Security Programme

Your Counterparts | Prevent and Detect

Tony Wicks

Customer Security Programme | Modus Operandi

- Common starting point has been a security breach in a customer's local environment
- In all cases, the SWIFT's network and core messaging services have not been compromised
- Attackers are well-organised and sophisticated



Step 1

Attackers compromise customer's environment

Step 2

Attackers obtain valid operator credentials

Step 3

Attackers submit fraudulent messages

Step 4

Attackers hide the evidence

Audience question:

Are you planning to re-evaluate your security controls?

a) Within the next 3 months

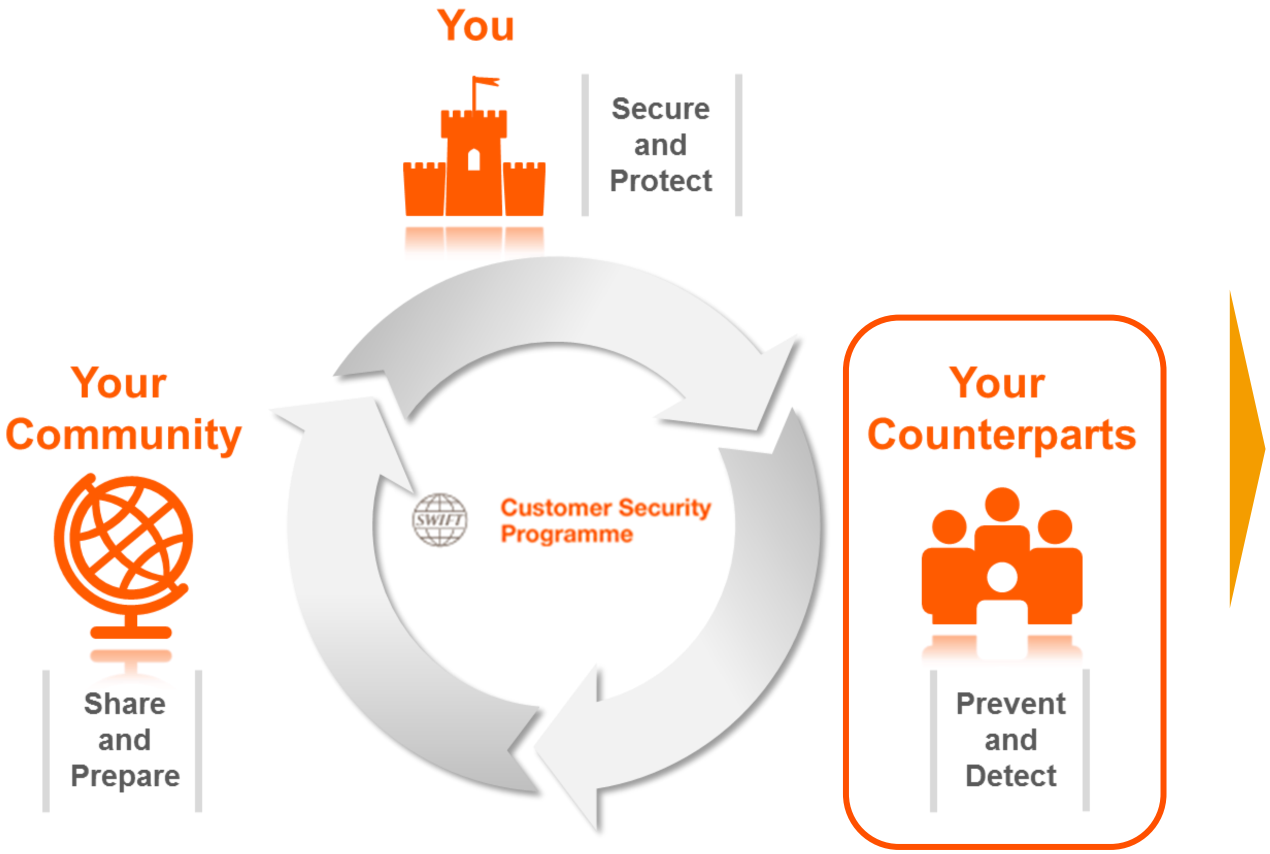
b) 3 – 6 months

c) Within a year

d) Within the next 3 years

e) We do not plan to do any re-evaluation

SWIFT Customer Security Programme (CSP) | Framework



Customer Security Programme

While all SWIFT customers are individually responsible for the security of their own environments, a concerted, industry-wide effort is required to strengthen end-point security

On May 27th 2016 SWIFT announced its Customer Security Programme (CSP) that supports customers in reinforcing the security of their SWIFT-related infrastructure

CSP focuses on mutually reinforcing strategic initiatives, and related enablers

CSP | Your Counterparts

Your Counterparts | Prevent and Detect

1. ‘Clean-up’ your RMA relationships

2. Engage with us on market practice

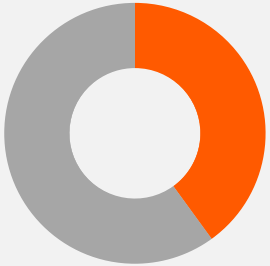
3. Put in place fraud detection measures

CSP | Relationship Management Application (RMA)

RMA and RMA plus

Poor management of RMAs creates potential security risks

Wolfsberg guidance means banks are under greater regulatory pressure to control RMAs



Only 40% of RMA relationships are actively used

Unilateral RMA revocation is now easy and is confirmed within 15 minutes

***"RMA and RMA Plus: managing your correspondent connections"* info-paper provides details on best practice**

CSP | Market Practice

Getting the basics right is the first defence against cyber-crime

What should you do?

1. Encourage the use of confirmations for all payments (MT900 / MT910)

2. Check that confirmations and statements (MT940 / MT950) are as expected

3. Avoid using free format messages to change payment instructions

4. Know how to respond in the event of fraud - use the “FRAD code” when sending cancellation messages

5. Report any incidents to SWIFT Support

Information paper

Mitigating fraud risk through strengthened payment operations

https://www.swift.com/myswift/customer-security-programme-csp_/document-centre

CSP | Daily Validation Reports

A simple, secure way to validate your SWIFT transaction activity and understand your payment risks

Validates
Back-office

with

Detects
Incident response

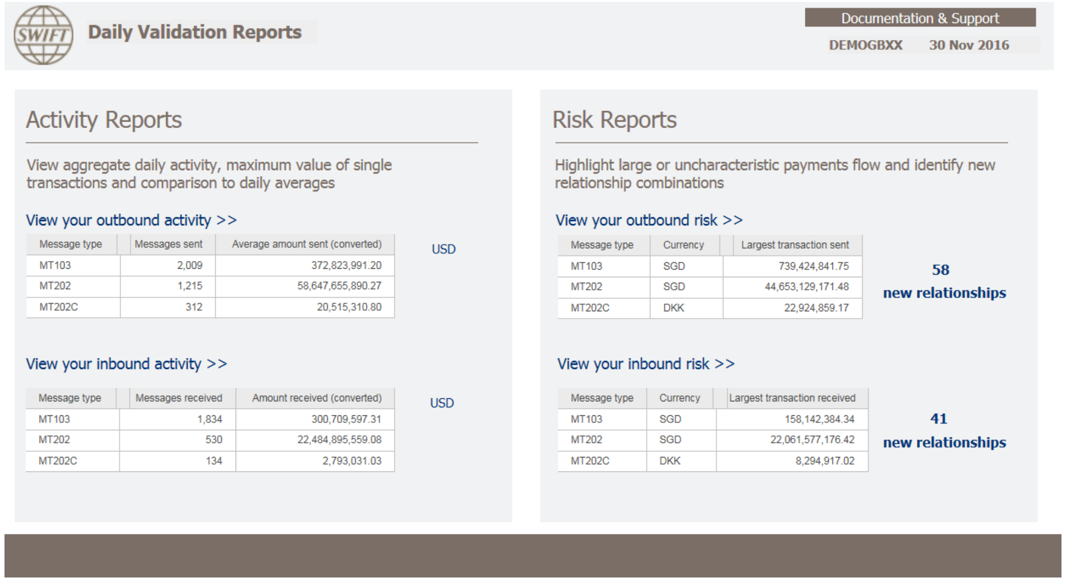
with

Secures
Data protection

CSP | Daily Validation Reports

Activity Reporting – reports aggregate daily activity by message type, currency, country and counterparties with daily volume and value totals, maximum value of single transactions and comparisons to daily volume and value averages

Risk Reporting - highlights large or unusual message flows based on ordered lists for largest single transactions and largest aggregate transactions for counterparties, and a report on new combinations of counterparties to identify new relationships



Daily Validation Reports

Documentation & Support

DEMOGBXX 30 Nov 2016

Activity Reports

View aggregate daily activity, maximum value of single transactions and comparison to daily averages

View your outbound activity >>

Message type	Messages sent	Average amount sent (converted)
MT103	2,009	372,823,991.20
MT202	1,215	58,647,655,890.27
MT202C	312	20,515,310.80

USD

View your inbound activity >>

Message type	Messages received	Amount received (converted)
MT103	1,834	300,709,597.31
MT202	530	22,484,895,559.08
MT202C	134	2,793,031.03

USD

Risk Reports

Highlight large or uncharacteristic payments flow and identify new relationship combinations

View your outbound risk >>

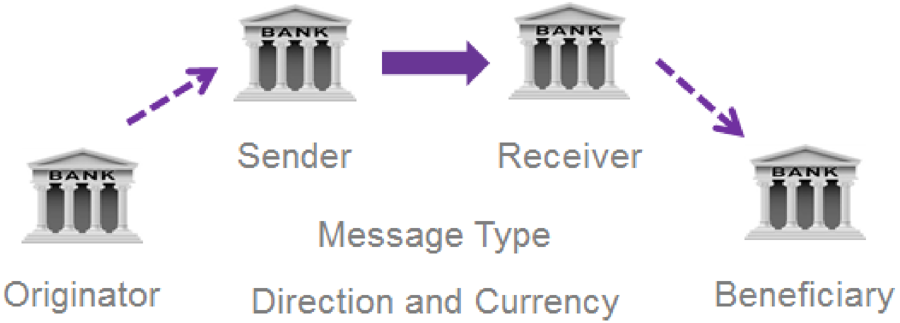
Message type	Currency	Largest transaction sent
MT103	SGD	739,424,841.75
MT202	SGD	44,653,129,171.48
MT202C	DKK	22,924,859.17

58
new relationships

View your inbound risk >>

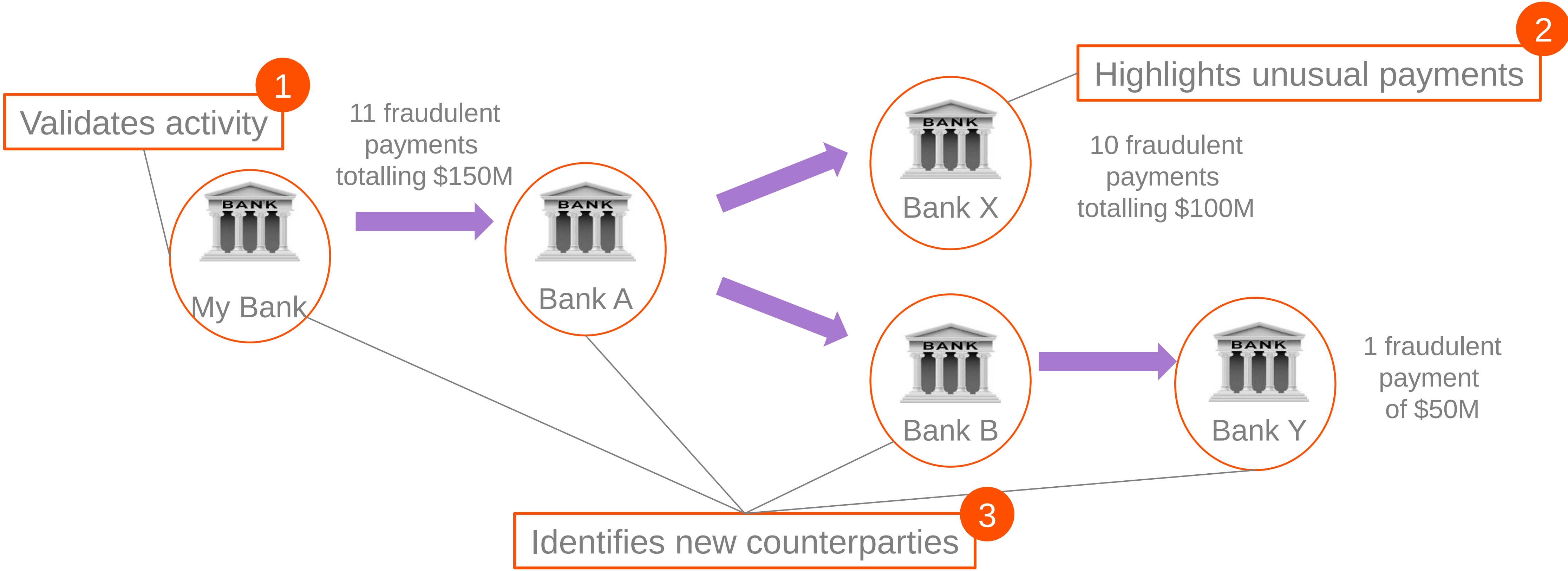
Message type	Currency	Largest transaction received
MT103	SGD	158,142,384.34
MT202	SGD	22,061,577,176.42
MT202C	DKK	8,294,917.02

41
new relationships



New Counterparties Reporting - highlights any new combinations of direct and indirect counterparties. Makes it easy to identify new payment relationships that may be indicative of risk, and helps you quickly understand the values and volumes of the transactions involved

CSP | Daily Validation Reports | Addressing the threat


1
Validates activity
11 fraudulent payments totalling $150M
2
Highlights unusual payments
BANK
Bank X
10 fraudulent payments totalling $100M
BANK
My Bank
BANK
Bank A
BANK
Bank B
BANK
Bank Y
1 fraudulent payment of $50M
3
Identifies new counterparties

Q&A

SWIFT

www.swift.com