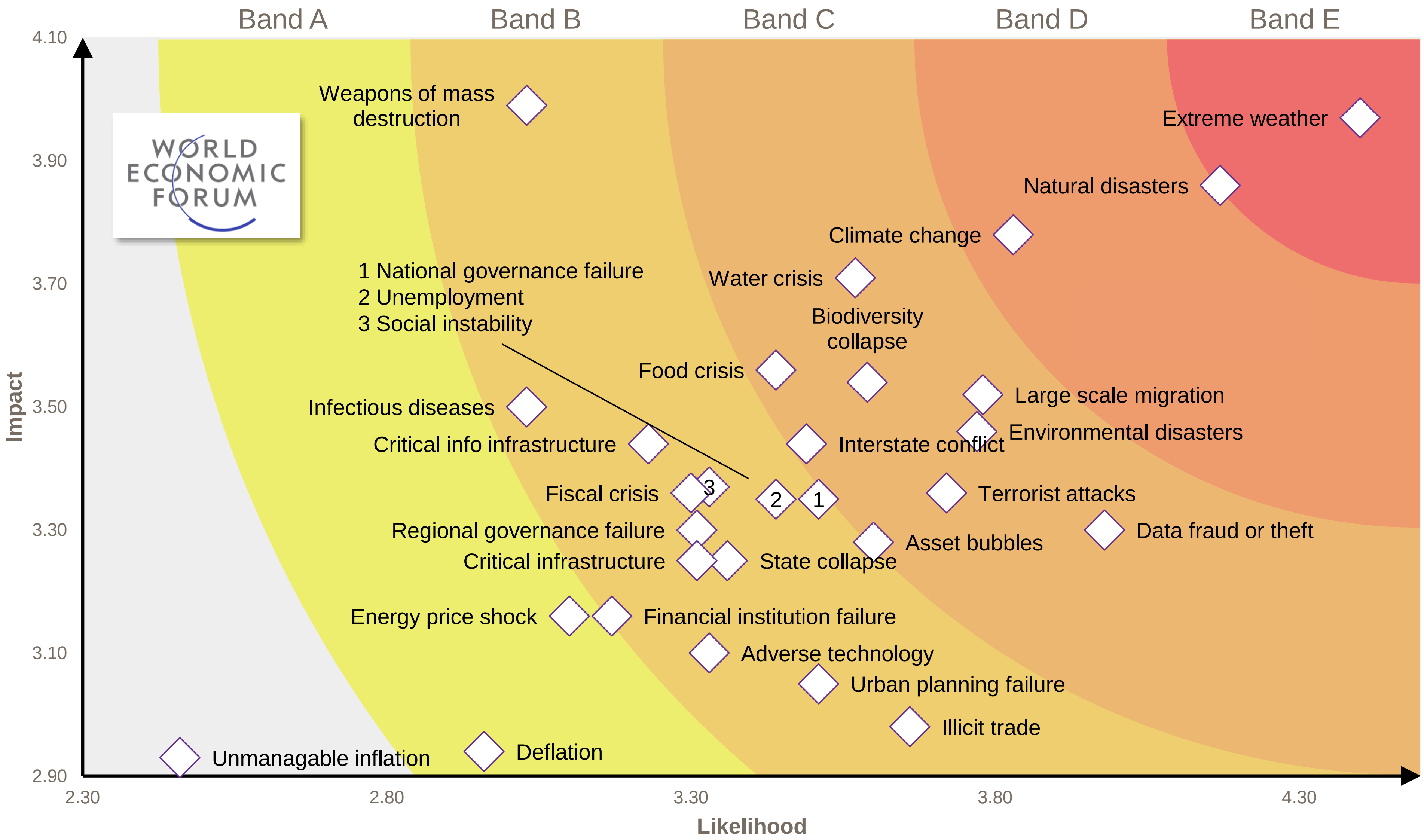
Customer Security Programme ‘Evolving threat landscape’

Frank Versmessen, Global Security, SWIFT

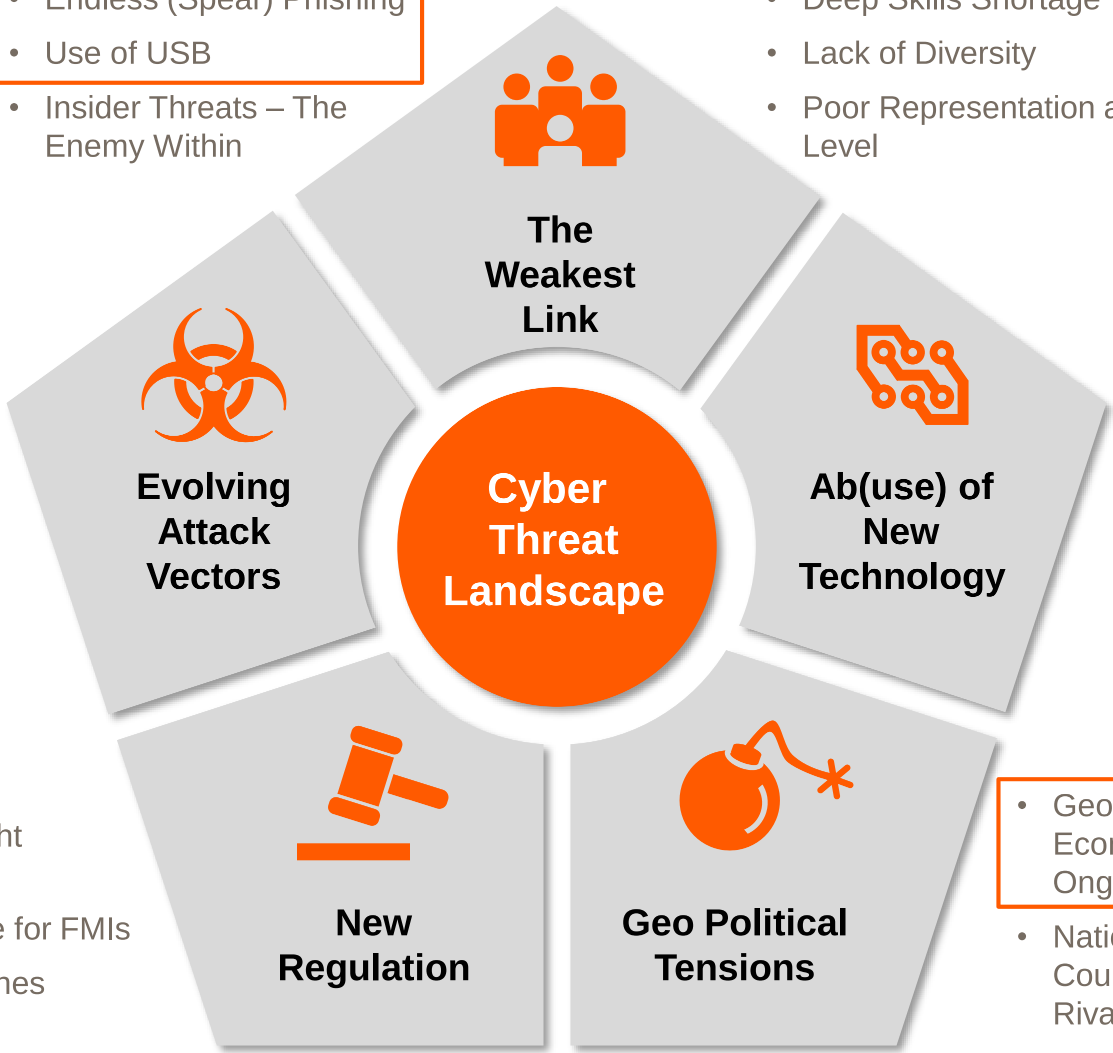
October 2019

The Big Picture for the World Economic Forum



Source: 2018 WEF survey spanning 684 respondents which assessed [likelihood] and [impact] of each risk on a scale of 1 to 5 [very unlikely / minimal impact] to [very likely / catastrophic]

Cyber threat landscape is shifting and the attack surface is always changing



Cyber Threat Landscape

The Weakest Link

- Endless (Spear) Phishing
- Use of USB
- Insider Threats – The Enemy Within

- Deep Skills Shortage
- Lack of Diversity
- Poor Representation at Board Level

Evolving Attack Vectors

- Intense DDoS Attacks
- Evolving Zero-Day APTs
- Rise in Ransomware
- Advanced 'Undetectable' Malware
- Larger Data Breaches
- (Possible) Targeting of Critical Infrastructure

Ab(use) of New Technology

- Reliance on a Few Technologies / Few Suppliers
- Reliance on the Cloud
- Internet of Things
- Overhead of Constant Patching
- Real Time Payments
- APIs and Open Banking
- 'Arms-Race' with AI / ML

New Regulation

- ECB Cyber Resilience Oversight Expectations for FMIs
- CPMI-IOSCO Cyber Resilience for FMIs
- GDPR with Fines for PII Breaches

Geo Political Tensions

- Geo-Political Tensions, Macro-Economic Trade Instability and Ongoing Conflicts
- Nation States use Cyberattacks to Counter Aggression from Geopolitical Rivals

There are major differences in the various threat actors

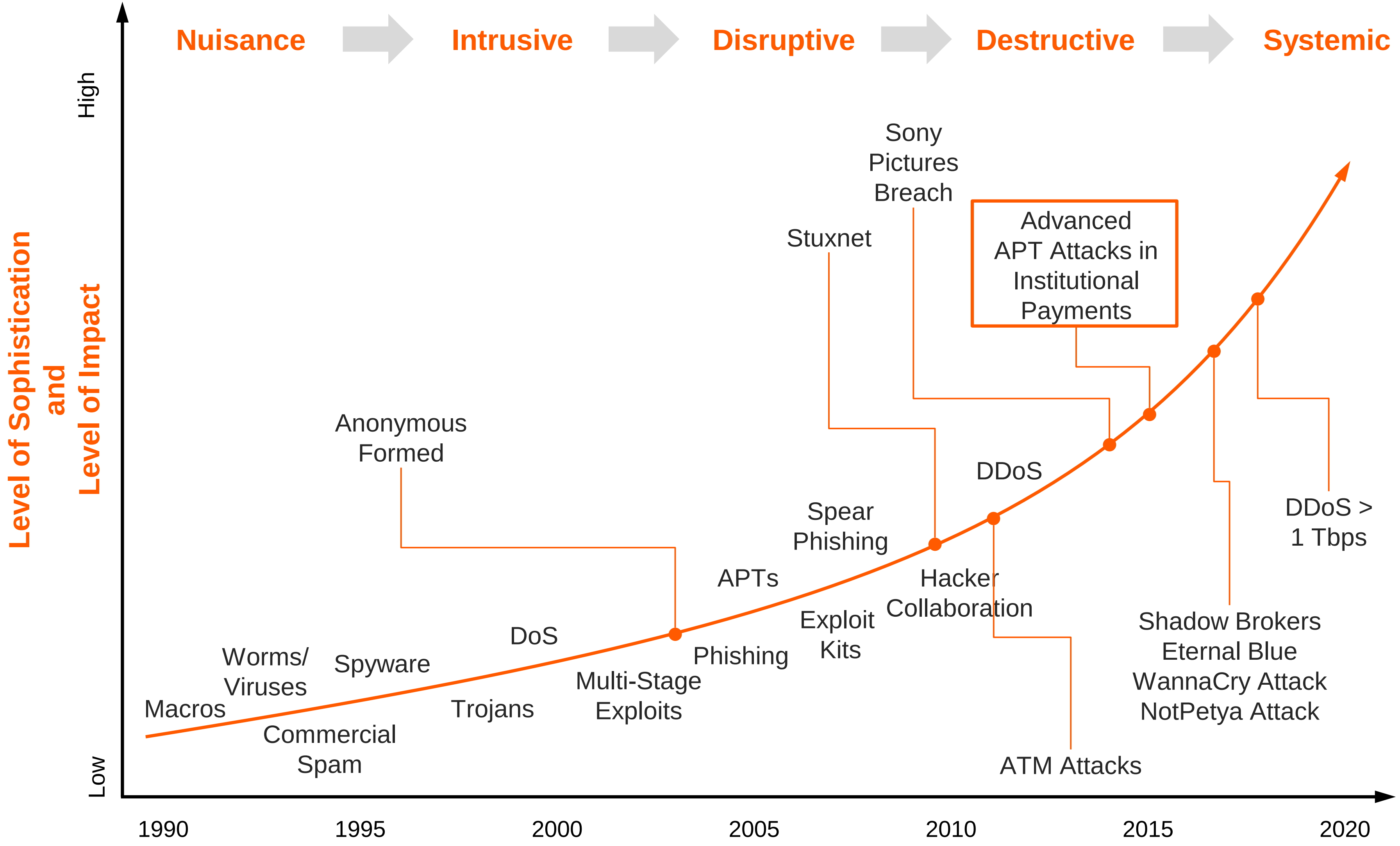
	Funding Levels	Disruption Levels	Motivation
Nation States	High	High	• Political unrest • Economic disturbance • Espionage • Intellectual property • Financial gain
Organised Crime	Medium	Medium	• Financial gain • Intellectual property
Hactivists	Medium	Medium – High	• Reputation damage • Operational disruption • Social / political ideology
Malicious Insiders	N/A	Medium – High	• Revenge • Operational disruption • Intellectual property • Financial gain
Unwitting Insiders	N/A	Medium – High	N/A - accidental impact / disruption

Sources:
Verizon 2017 Data Breach Investigations Report
IBM X-Force Threat Intelligence Index 2017
ENISA Threat Landscape Report 2017

There are major differences in threat actor motivations

Attack Types	Description	Systemic Reach	Ease of Execution	Impact
Disruption / Ransom	Systemic market disruption / destruction / ransom on key market players and resultant market liquidity issues from an APT and/or DDoS attack	Wide - Endemic	Difficult	Very High
Asset Theft	Asset theft from manipulated records / information for a specific organisation from a coordinated APT attack	Contained - Local	Medium	Medium
Information Theft	Information theft of sensitive intellectual property that could give competitive advantage from a coordinated APT attack	Local	Easy – Medium	Low
Market Manipulation	Through manipulation of pricing / news feeds from a coordinated APT attack. HFT algorithms would adjust stock price automatically	Wide - Endemic	Easy – Medium	High

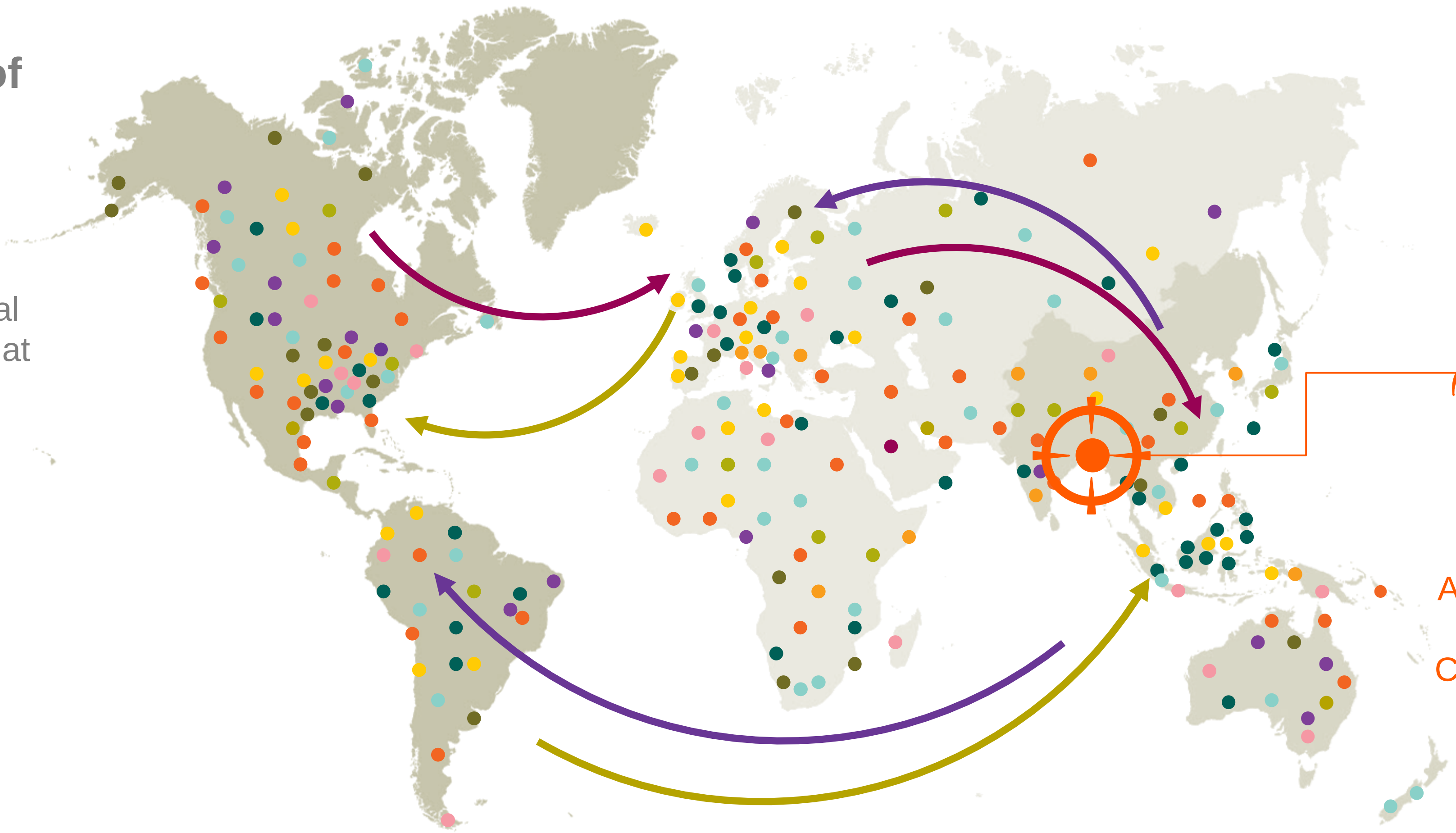
Level of impact and the level of sophistication of cyber attacks are both rising



SWIFT

Global provider of secure financial messaging services

Industry owned, financial services cooperative, that does not seek to maximise profit



Ground Zero for APT Attacks on SWIFT Customers

Connecting **12,000+** institutions

200+ Countries and territories

7+ billion FIN messages in 2017

Proven network **99.999%** **FIN availability**

Strong PKI security **encryption**

ISO 20022 Unique role developing standards

Profile of all Customer Incidents

Advanced Persistent Threat (APT) | Modus Operandi

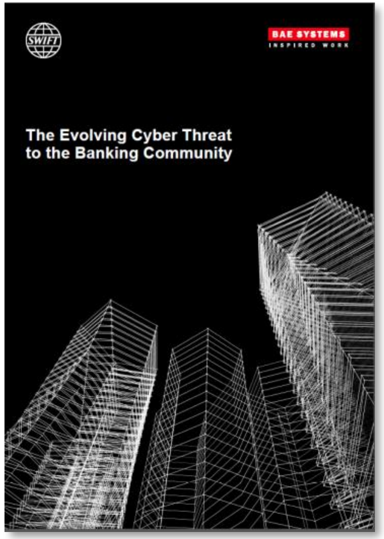
- Attackers are **well-organised and sophisticated**
- There is (still) **no evidence** that SWIFT's network, core messaging services or OPCs have been compromised
- All **IOC details** are published on the SWIFT ISAC portal

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


BAE SYSTEMS INSPIRED WORK

The Evolving Cyber Threat to the Banking Community

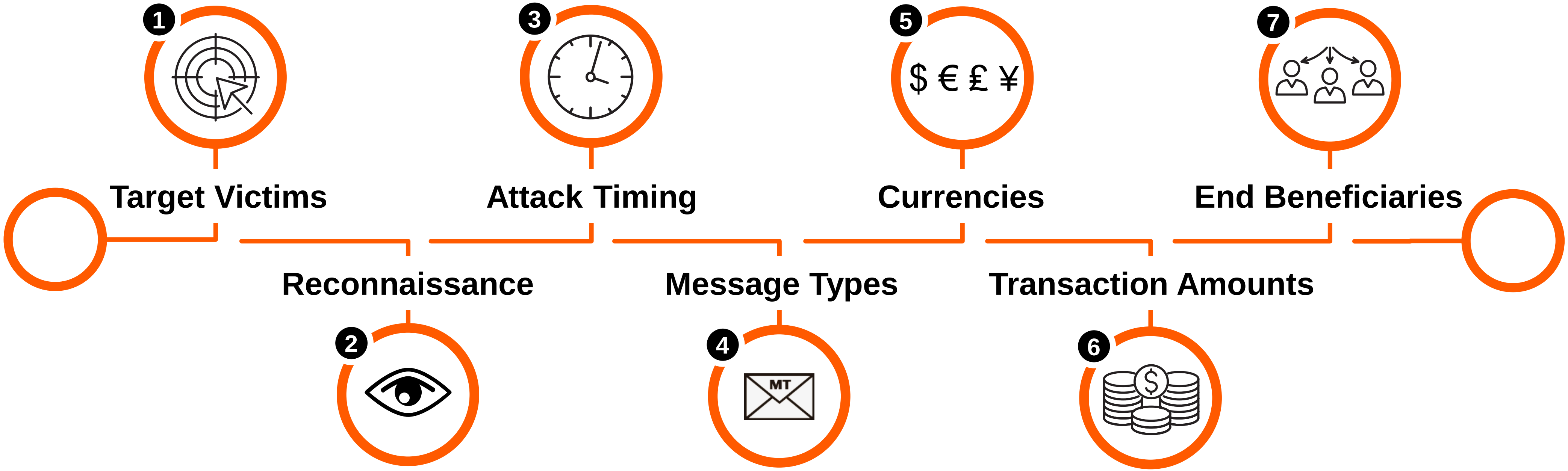
- **Malware** injected by e-mail phishing, USB device, rogue URL or insider
- Long **reconnaissance** period monitoring banks' back office processes

- Keylogging / screenshot malware looking for **valid account ID and password** credentials

- Attacker impersonate the operator / approver and submits **fraudulent payment instructions**
- May happen outside the normal bank working hours / over public holiday

Gain time by:
- Deleting or manipulating records / log used in reconciliation
- Wiping Master Boot Record

As attacks on SWIFT customers continue, a risk profile emerges of the threat



1 Target Victims

Profile of target customers:

- (Very) High on Basel AML Country Corruption Risk Index
- Central Africa, Central Asia, South East Asia, Latin America
- Banks with small traffic volumes

2 Reconnaissance

- Attacker patience - can wait for weeks / months before injecting fraudulent messages
- Reconnaissance time used to gather user credentials and learn operational behaviour

3 Attack Timing

- Outside business hours
- During local public holidays
- During business hours to blend in with legitimate traffic
- Fraudulent messages can be minutes or hours apart

4 Message Types

- Cross-border payments
- Mainly MT-103 FIN messages
- Typically messages are sent from victim bank to end beneficiary bank via one or more correspondent Nostro bank(s)

5 Currencies

Currency of fraudulent transactions:

- 70% USD
- 21% EUR
- 9% GBP, HKD, AUD, JPY …

6 Transaction Amounts

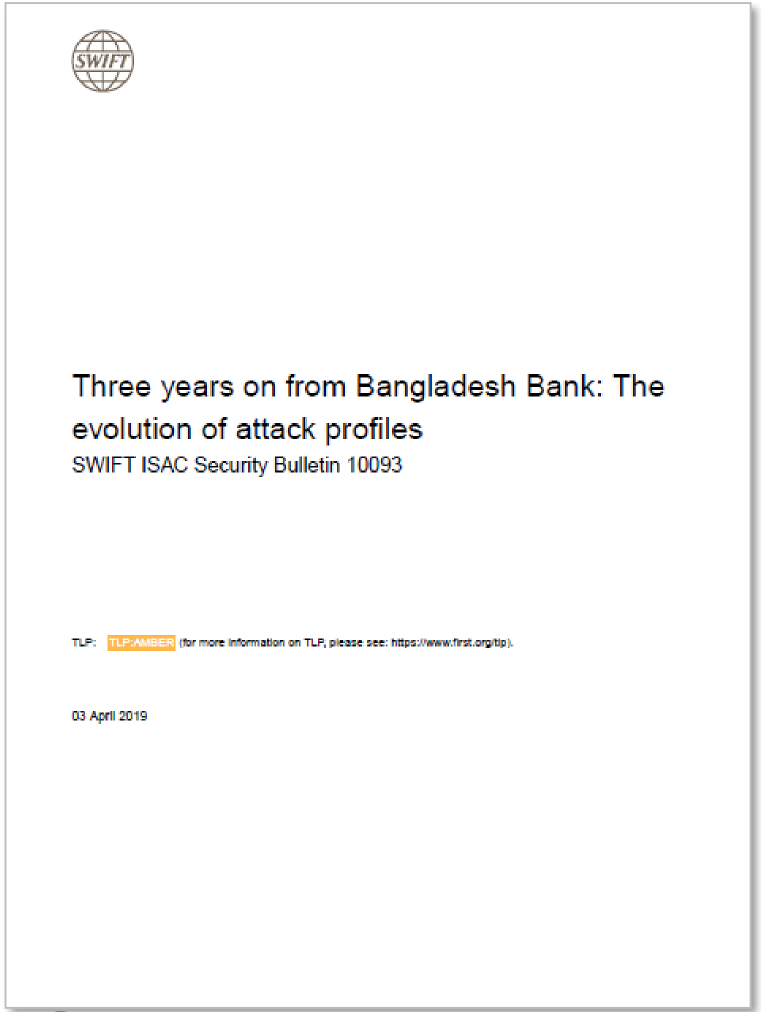
- Before 2018, typically MUSD ten or MUSD tens
- From 2018 , typically MUSD 0.25 - 2
- Typical per transaction amounts were much larger than ‘average’ amounts sent over them in the prior 24 months

7 End Beneficiaries

End beneficiary destination of fraudulent transactions:

- 83% Asia Pacific
- 10% Europe
- 4% North America
- 3% Middle East

As attacks on SWIFT customers continue, a risk profile emerges of the threat



Three years on from Bangladesh Bank: The evolution of attack profiles

SWIFT ISAC Security Bulletin 10093

TLP: TLP:AMBER (for more information on TLP, please see: https://www.first.org/tlp).

03 April 2019

SWIFT ISAC Report
April 2019

Three years on from Bangladesh

Tackling the adversaries

Detailed Bulletin 10093:

Bulletin published on SWIFT ISAC on 3 Apr 19

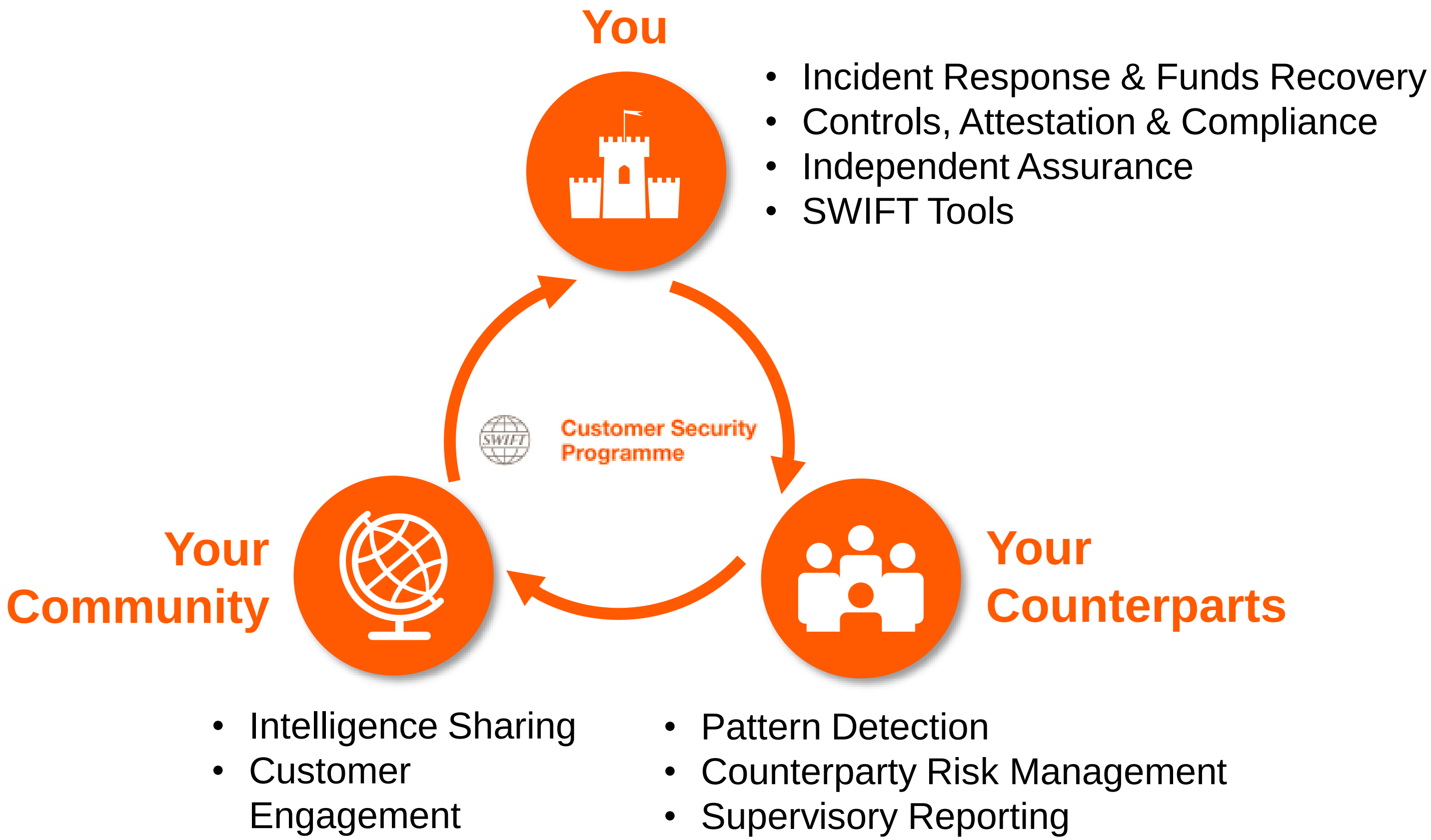
Summary White Paper:

White Paper published to community on 10 Apr 19

Customer Security Programme | the basics

Launched in 2016 in response to the attack on Bangladesh Bank, CSP is a multi-year, multi-facetted initiative

CSP aims to transform the institutional financial services ecosystem by raising the bar of cybersecurity hygiene, reducing the risk of cyberattacks and minimising the impact of fraudulent transactions



You

- Incident Response & Funds Recovery
- Controls, Attestation & Compliance
- Independent Assurance
- SWIFT Tools

Your Community

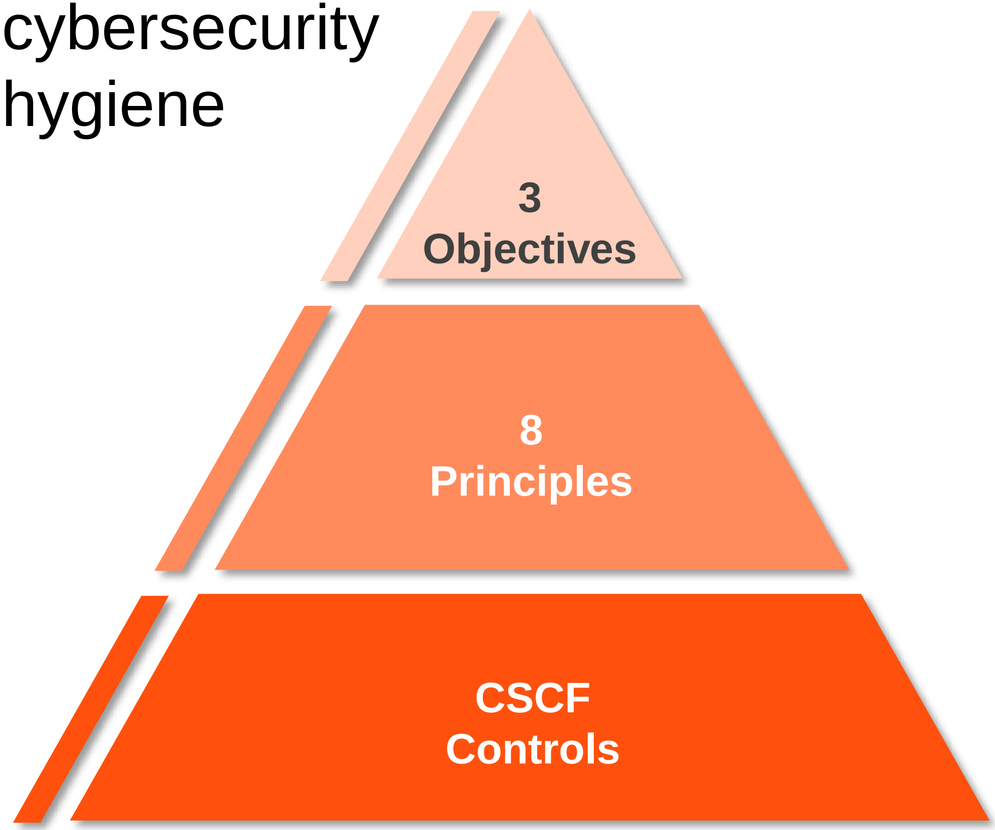
- Intelligence Sharing
- Customer Engagement

Your Counterparts

- Pattern Detection
- Counterparty Risk Management
- Supervisory Reporting

Where we are now | controls

Improve cybersecurity hygiene



3 Objectives

8 Principles

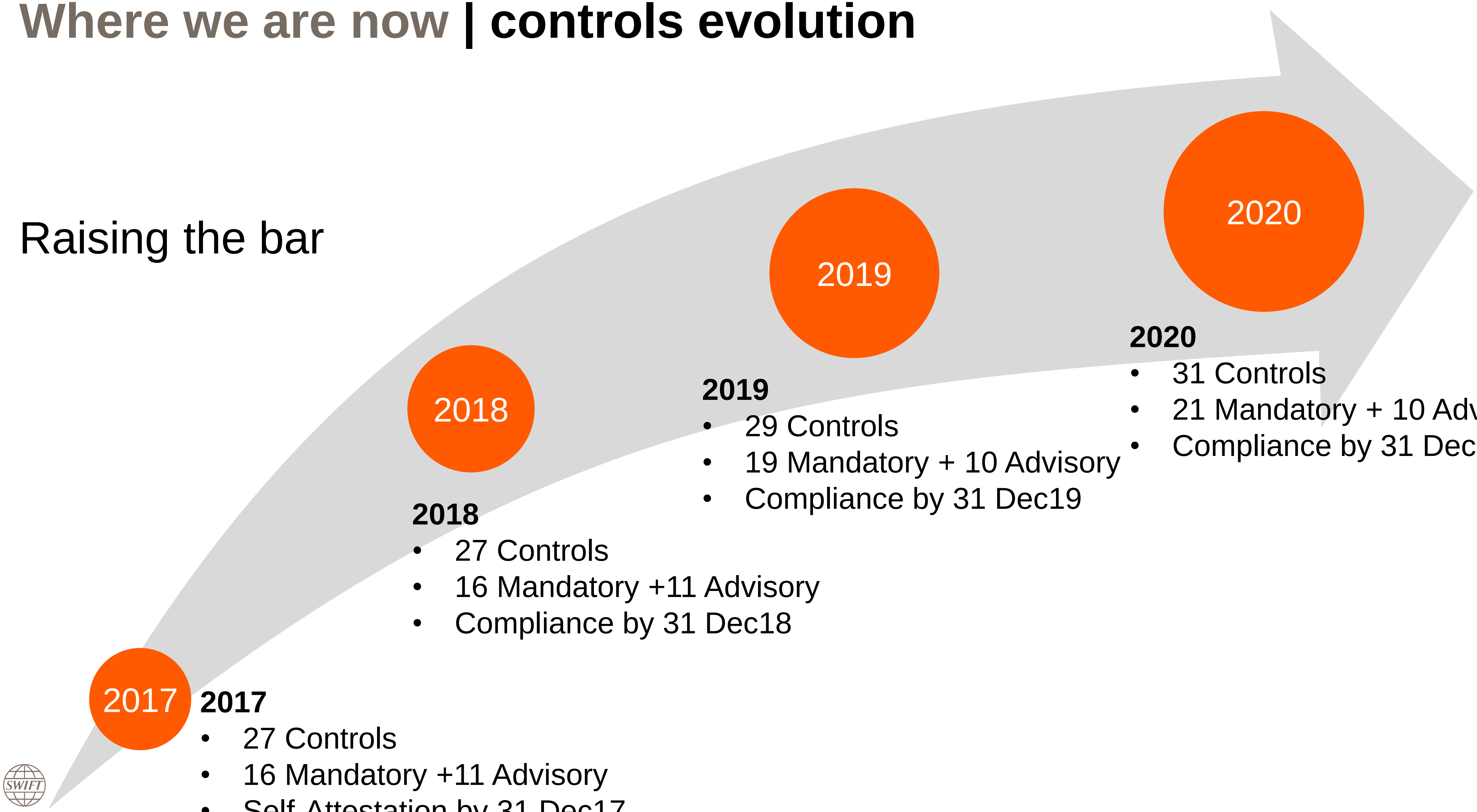
CSCF Controls

CSP Security Controls

Secure Your Environment	1.	Restrict Internet access
	2.	Segregate critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

Where we are now | controls evolution

Raising the bar



2017

- 27 Controls
- 16 Mandatory +11 Advisory
- Self-Attestation by 31 Dec17

2018

- 27 Controls
- 16 Mandatory +11 Advisory
- Compliance by 31 Dec18

2019

- 29 Controls
- 19 Mandatory + 10 Advisory
- Compliance by 31 Dec19

2020

- 31 Controls
- 21 Mandatory + 10 Advisory
- Compliance by 31 Dec20

Where we are now | assurance

Assessment Type	Selection Criteria	Assessor	Timeline			
			2017	2018	2019	2020 and beyond
❶ **User-Initiated Assessment**	Voluntary - Customer Initiated	Internal or external	■	■	■	■
❷ **Community-Standard Assessment**	Mandated - All Users	Internal or external				■
❸ **SWIFT-Mandated Assessment**	Mandated - Sampled Customers Driven by QA Analysis	External only		■	■	■

Where we are now | intelligence sharing

Security Notifications

12,000
# unique users

6500
# unique BICs

SWIFT ISAC Access (rolling year)

19k
# accesses

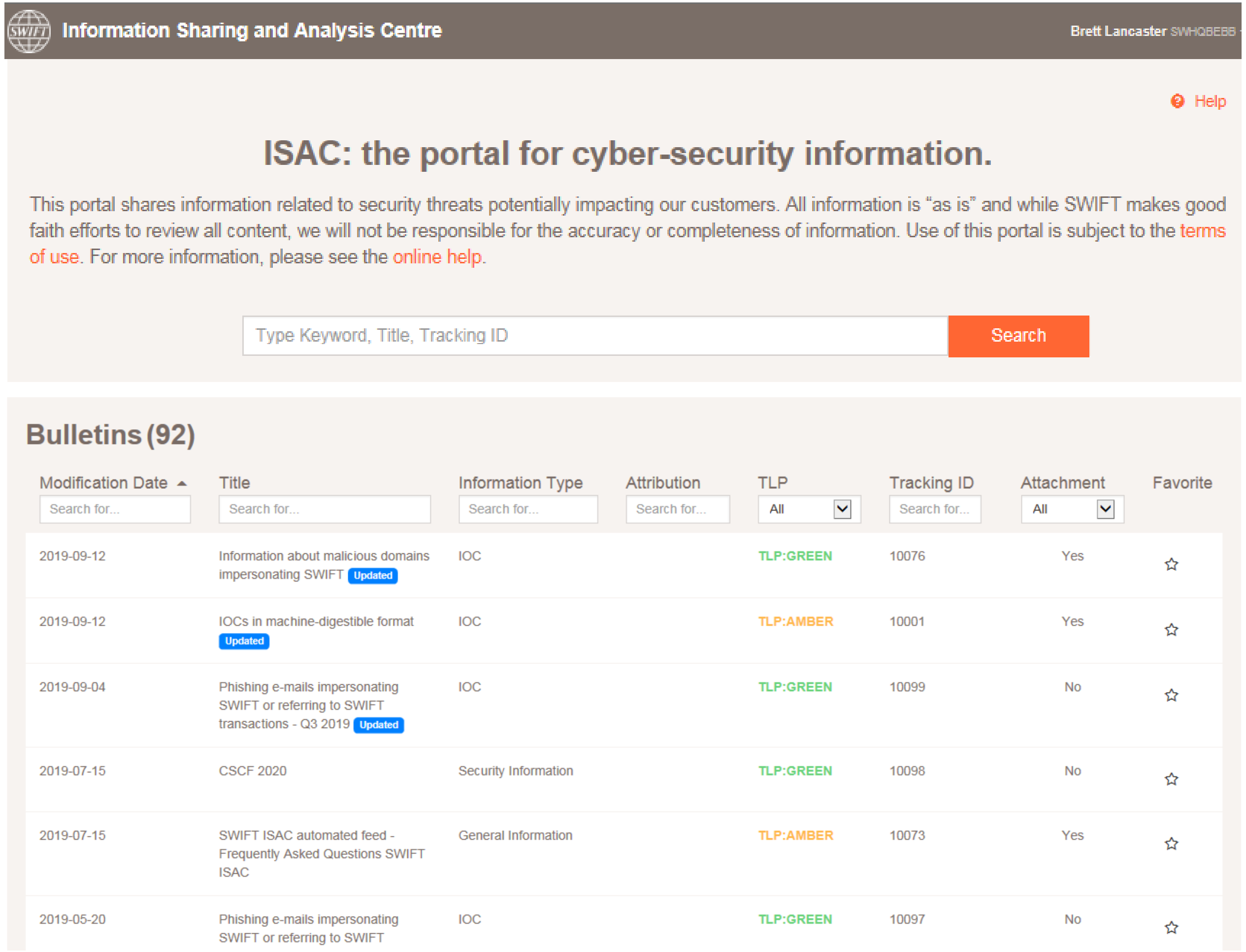
5400
# unique users

27%
of BIC population

200
# countries

Available as STIX/TAXII feed

SWIFT ISAC: Filenames; Filehashes; IP addresses; Domains; Ports; Processes; YARA Rules; MO …



Information Sharing and Analysis Centre

Brett Lancaster SWHQBEBB

Help

ISAC: the portal for cyber-security information.

This portal shares information related to security threats potentially impacting our customers. All information is "as is" and while SWIFT makes good faith efforts to review all content, we will not be responsible for the accuracy or completeness of information. Use of this portal is subject to the terms of use. For more information, please see the online help.

Type Keyword, Title, Tracking ID | Search

Bulletins (92)

Modification Date ▲	Title	Information Type	Attribution	TLP	Tracking ID	Attachment	Favorite
Search for...	Search for...	Search for...	Search for...	All	Search for...	All	
2019-09-12	Information about malicious domains impersonating SWIFT Updated	IOC		TLP:GREEN	10076	Yes	☆
2019-09-12	IOCs in machine-digestible format Updated	IOC		TLP:AMBER	10001	Yes	☆
2019-09-04	Phishing e-mails impersonating SWIFT or referring to SWIFT transactions - Q3 2019 Updated	IOC		TLP:GREEN	10099	No	☆
2019-07-15	CSCF 2020	Security Information		TLP:GREEN	10098	No	☆
2019-07-15	SWIFT ISAC automated feed - Frequently Asked Questions SWIFT ISAC	General Information		TLP:AMBER	10073	Yes	☆
2019-05-20	Phishing e-mails impersonating SWIFT or referring to SWIFT	IOC		TLP:GREEN	10097	No	☆

Where we are now | intelligence sharing

OLIVER WYMAN

COUNTERPARTY CYBER RISK MANAGEMENT FRAMEWORK

DECEMBER 2017

ISSA

Cyber Security Risk Management in Securities Services

Final Draft – October 2018

SWIFT INSTITUTE

SWIFT INSTITUTE WORKING PAPER NO. 2018-002

SMALL BUT AGILE:
PROTECTING SMALLER FINANCIAL ORGANIZATIONS AGAINST CYBER THREATS

TOOLKIT

TIM MAURER

KATHRYN TAYLOR

PUBLICATION DATE: TBC 2019

The views and opinions expressed in this paper are those of the authors. SWIFT and the SWIFT Institute have not made any editorial review of this paper, therefore the views and opinions do not necessarily reflect those of either SWIFT or the SWIFT Institute.

SWIFT ISAC Report
April 2019

Three years on from Bangladesh
Tackling the adversaries

Summary of attacks in which attackers deploy malware to obtain operator access

SWIFT ISAC Security Bulletin 10060

TLP: TLP:AMBER (for more information on TLP, please see: https://w

26 February 2019

BAE SYSTEMS
INSPIRED WORK

The Evolving Cyber Threat to the Banking Community

BAE SYSTEMS

The Evolving Advanced Cyber Threat to Financial Markets

Information paper

From security baseline to best practice

Securing India's critical channel infrastructure

Guideline

Assessing Cybersecurity Counterparty Risk

A Getting Started Guide

Where we are now | CISO engagement

Ireland BF
Dublin
30 Apr

Sibos
London
23 Sep

FSIE
London

Benelux
Forum
Brussels

SOFE BF
Amsterdam
27 Nov

DE/AT CISO RT
Frankfurt
5 Feb

ECRB Intel
Share
Frankfurt

ECRB Crisis
Mgt
Frankfurt

Nordics BF
Copenhagen
28 Mar

Poland BF
Warsaw
29 May

FSARC - GMI
New York

MX CISO RT
Mexico City
20 Jun

PA CISO RT
Panama City
22 May

LARC BF
Panama City
21 May

CL CISO RT
Santiago
26 Mar

AR CISO RT
Buenos Aires
21 Mar

CN CISO RT
Beijing
28 Nov

HK CISO RT
Hong Kong
10 May

IN CISO RT
Mumbai
8 May

India BF
Mumbai
9 May

SG CISO RT
Singapore
9 Jul

x12 CISO RT Events
x11 SWIFT BF/RC Events
x47 Industry Mtg Events
x19 External Conference Events

GH/NG CISO
RT
Accra

ARC BF
Accra
18 Jun

CPMI-IOSCO
Intel Share
Basel

IT CISO RT
Milan
11 Feb

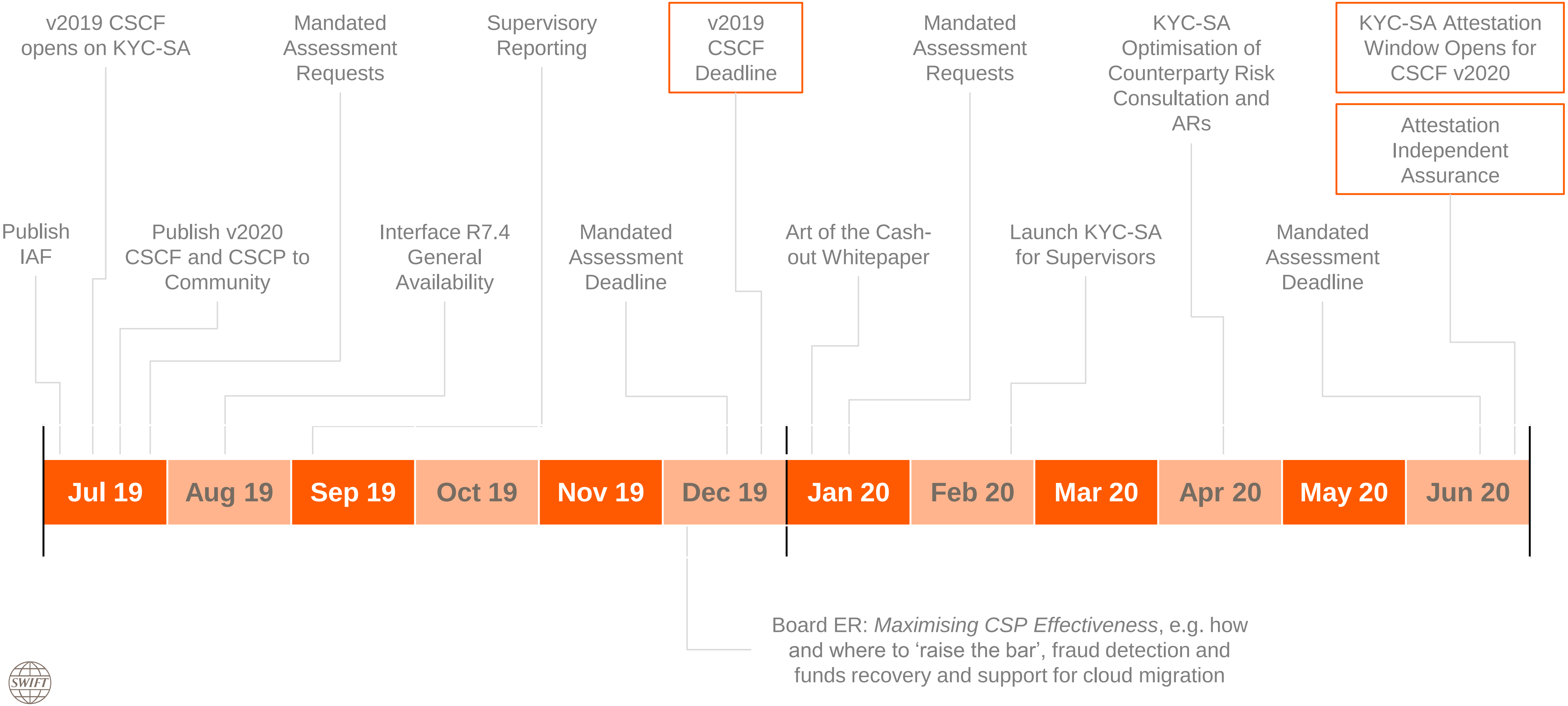
Romania BF
Bucharest
24 Oct

JSE + Brokers
Johannesburg

Turkey BF
Istanbul
5 Nov

TR CISO RT
Istanbul
7 Nov

Where we are now | current roadmap



v2019 CSCF opens on KYC-SA

Mandated Assessment Requests

Supervisory Reporting

v2019 CSCF Deadline

Mandated Assessment Requests

KYC-SA Optimisation of Counterparty Risk Consultation and ARs

KYC-SA Attestation Window Opens for CSCF v2020

Attestation Independent Assurance

Publish IAF

Publish v2020 CSCF and CSCP to Community

Interface R7.4 General Availability

Mandated Assessment Deadline

Art of the Cash-out Whitepaper

Launch KYC-SA for Supervisors

Mandated Assessment Deadline

Jul 19 | Aug 19 | Sep 19 | Oct 19 | Nov 19 | Dec 19 | Jan 20 | Feb 20 | Mar 20 | Apr 20 | May 20 | Jun 20

Board ER: *Maximising CSP Effectiveness*, e.g. how and where to ‘raise the bar’, fraud detection and funds recovery and support for cloud migration

Call to action

1. Stay up to date with SWIFT software releases
2. Sign up for Security Notifications and use of the SWIFT ISAC information sharing portal or STIX/TAXII feeds
3. Consume and utilise attestation data for counterparty risk management
4. Consider SWIFT’s anti-fraud tools (Payment Controls, Daily Validation Reports, RMA clean-ups, etc.)
5. Always inform SWIFT immediately if you suspect a cyber-attack on your SWIFT-related infrastructure
6. Ensure that you fully comply with all the mandatory security controls and attest by end December

Questions