Customer Security Programme Priorities

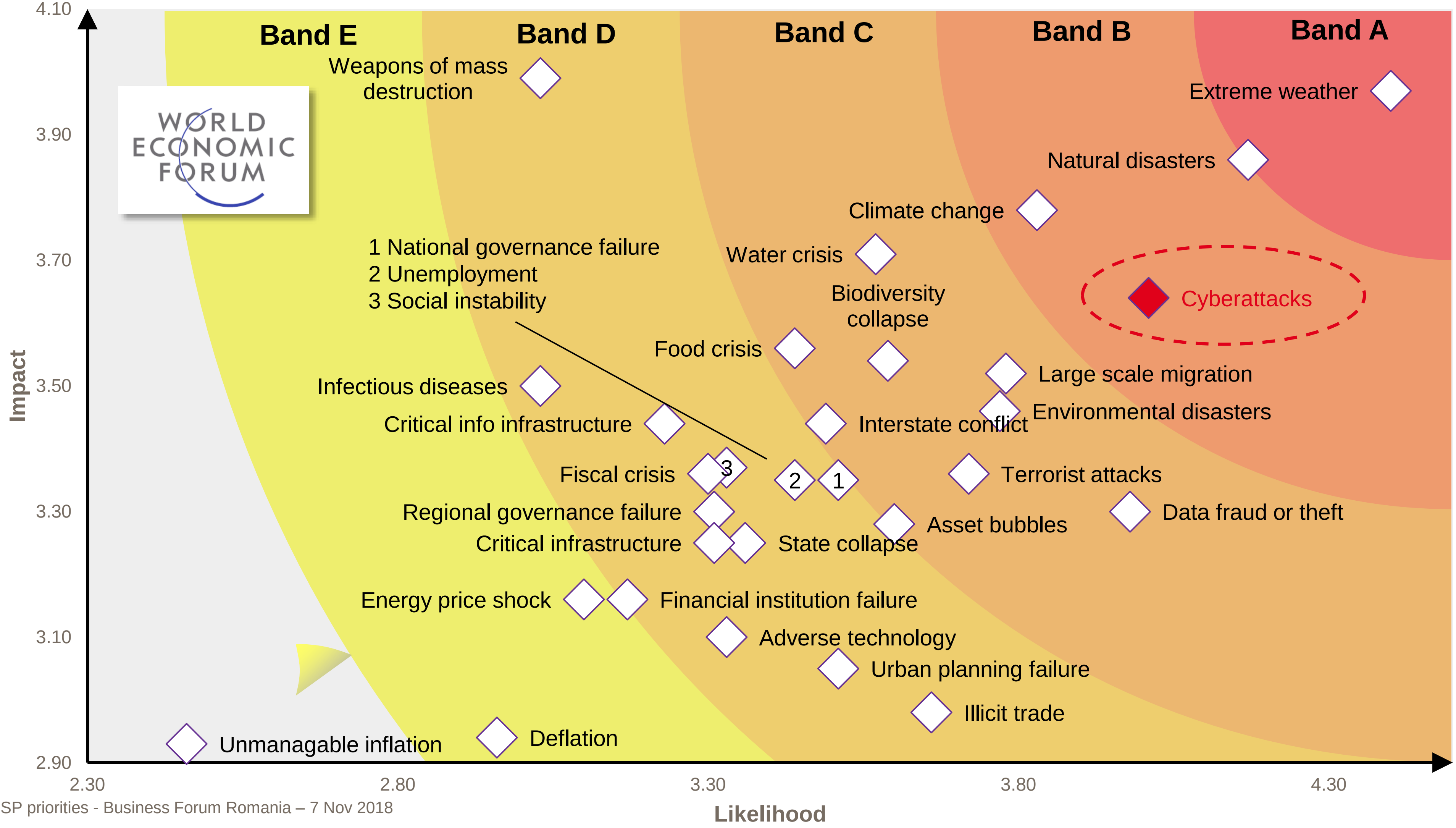
Business Forum Romania 2018

Bucharest, 7 November 2018

Judit Baracs, Senior Account Director, Country Manager Romania

Overall Evolution of the Threat Landscape

World Economic Forum ranks ‘cyberattacks’ as a top global risk

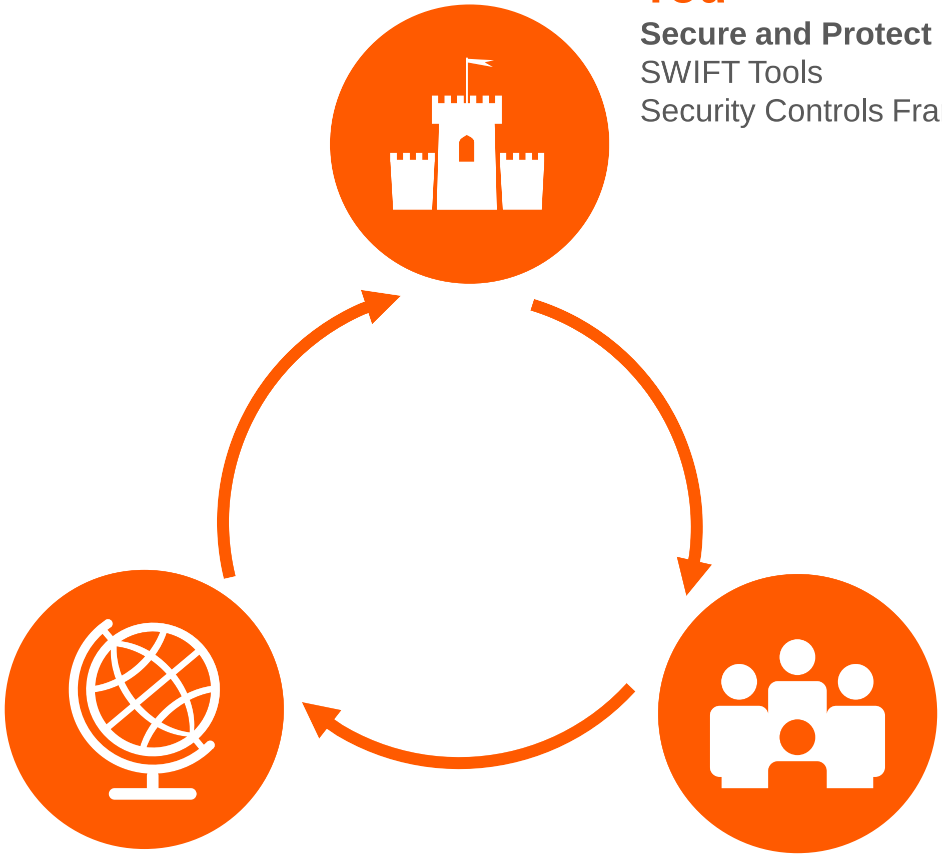


Source: 2018 WEF survey spanning 684 respondents which assessed [likelihood] and [impact] of each risk on a scale of 1 to 5 [very unlikely / minimal impact] to [very likely / catastrophic]

CSP | SWIFT's Response

Customer Security Programme (CSP)

Launched in May 2016, the CSP supports all customer segments in reinforcing the security of their local SWIFT-related infrastructure



You

Secure and Protect
SWIFT Tools
Security Controls Framework

Your Counterparts

Prevent and Detect
Transaction Pattern Detection –
RMA, DVR and 'In Flight' Sender Payment Controls

Your Community

Share and Prepare
Intelligence Sharing
SWIFT ISAC Portal

CSP | 2018 Priorities

**Compliance,
Re-Attestation,
Consultation,
Prepare for 2019**

You

- Change Management process Customer Security Controls Framework (CSCF)
- Release of CSCF v2019 (version 2)
- Updated Customer Security Attestation Policy
- Interface Hardening – Release 7.3

Your Counterparts

- Security Attestation Application v3 – Consult
- Quality Assurance framework.
- Payment Controls Service, Daily validation Report, RMA cleanup & RMA+

Your Community

- SWIFT–ISAC
- Directory of Cyber Security Providers
- Industry engagement

CSP | Modus Operandi

- Attackers are **well-organised and sophisticated**
- There is **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

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

Step 2

Attackers obtain valid operator credentials

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

Step 3

Attackers submit fraudulent messages

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

Step 4

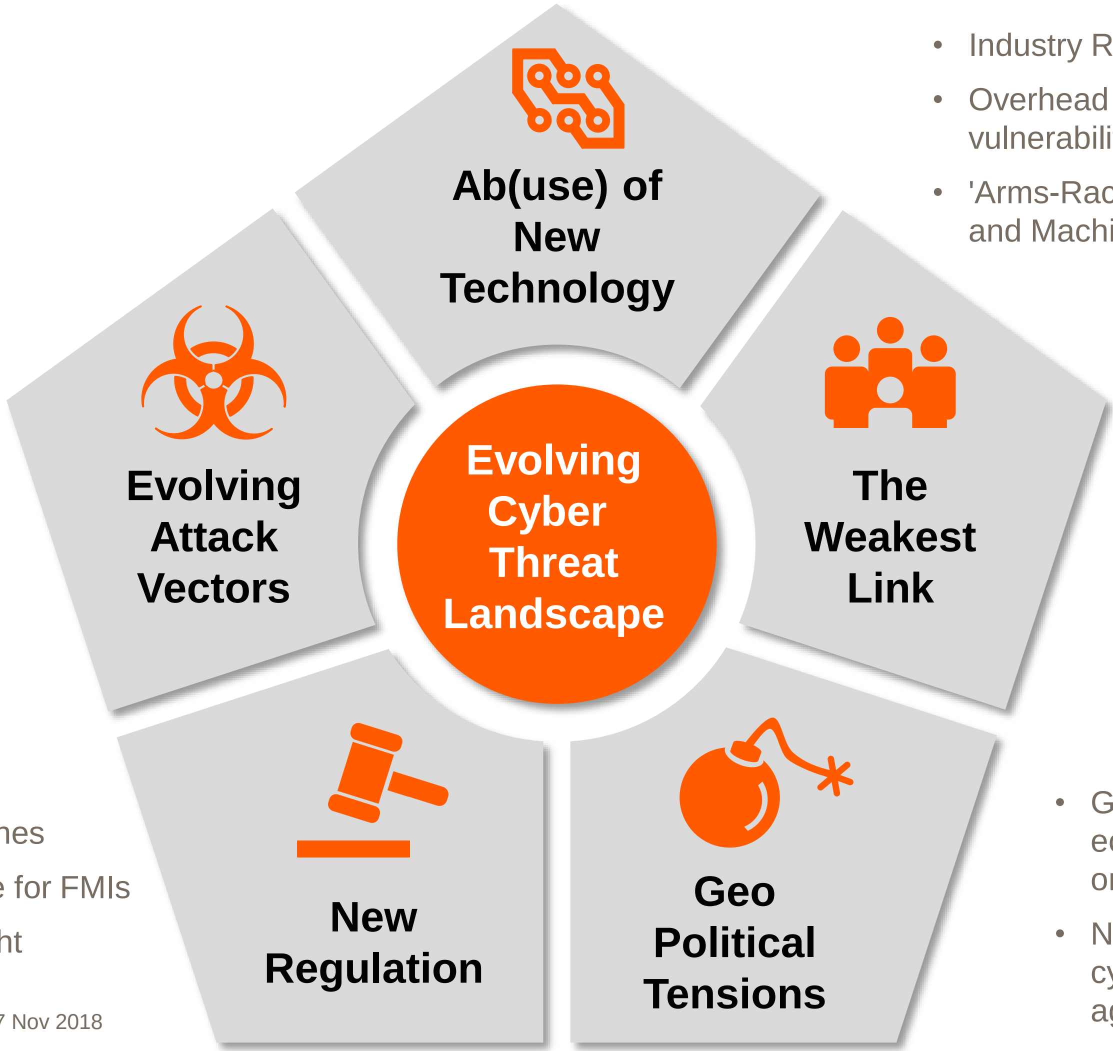
Attackers hide the evidence

Gain time by:

- Deleting or manipulating records / log used in reconciliation
- Wiping Master Boot Record

Evolution of the Threat Landscape

The cyber threat landscape is always shifting and the attack surface is always changing



Evolving Cyber Threat Landscape

Ab(use) of New Technology

- Industry Reliance on the Cloud
- Overhead of constantly patching critical software vulnerabilities
- 'Arms-Race' as New Technologies Mature – AI and Machine Learning

Evolving Attack Vectors

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

The Weakest Link

- Endless (Spear) Phishing
- Rise in Insider Threats – The Enemy Within
- Deep Skills Shortage

New Regulation

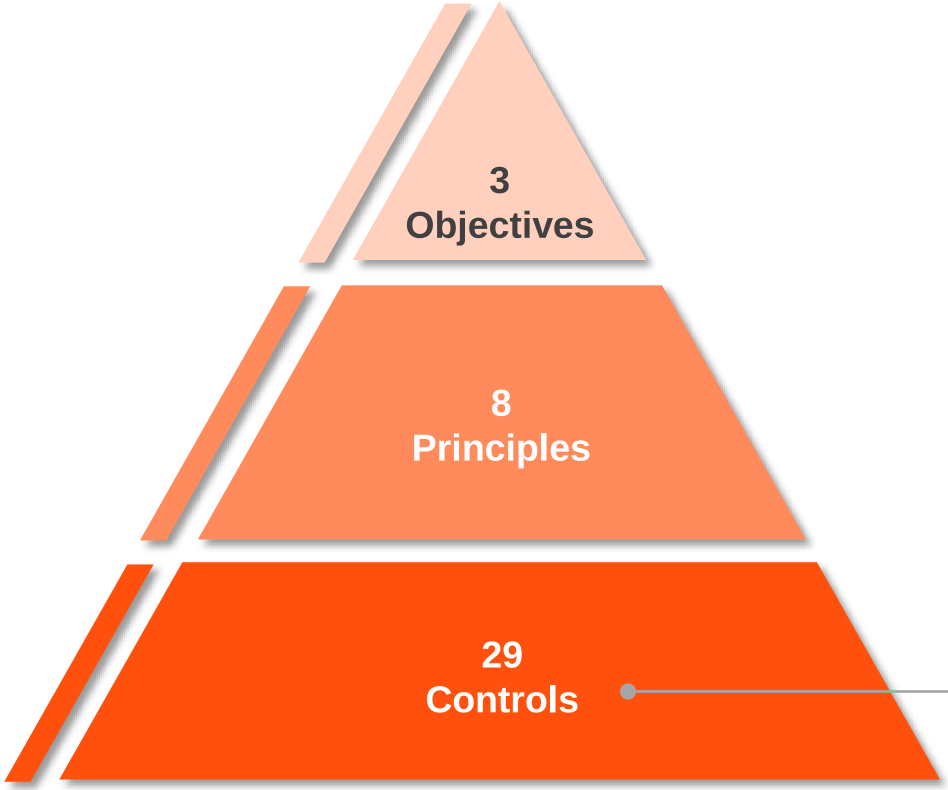
- GDPR with Fines for PII Breaches
- CPMI-IOSCO Cyber Resilience for FMIs
- ECB Cyber Resilience Oversight Expectations for FMIs

Geo Political Tensions

- Geo-political tensions, macro-economic trade instability and ongoing conflicts
- Nation states have used cyberattacks as a way to counter aggression from geopolitical rivals

CSP | Customer Security Controls Framework v2019

Security Controls



CSP Security Controls Framework

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

- 19 controls are mandatory – 3 advisory promoted:
  - 2.6 Secure Operator sessions
  - 2.7 Yearly vulnerability scanning
  - 5.4 Physical and Logical Password Storage
- 10 controls are advisory - 2 new advisory controls:
  - 1.3A Virtualization Platform Protection
  - 2.10A Application Hardening
- Full compliance against mandatory controls by end 2019

CSP | Call to action for SWIFT customers

1 Stay up to date with SWIFT software releases

2 Sign up for Security Notifications and use of the SWIFT ISAC information sharing portal. Includes STIX/TAXII from Mar 18

3 Consider your institution's counterparty risk frameworks to consume and utilise counterparty attestation data

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 16 mandatory security controls and attest by 31 December 2018

SWIFT

www.swift.com

SWIFT donates 3,000 EUR for SOS Children’s Villages Bucharest

SWIFT donates 3,000 EUR for SOS Children’s Villages Bucharest

How the donation will be used:

In Bucharest, the future of disadvantaged Roma and street children is uncertain.

SOS Children’s Villages gives access to basic needs such as health, education and nutrition to as many children as possible.

SWIFT’s support will help finance a “**Playmobile Bus**”, a mobile centre which stops where many disadvantaged children live.

Children are encouraged to play imaginative and educational games, including craft, dancing and theatrical activities.

The aim is to give children a chance to be children and to increase the confidence in themselves and in others around them.