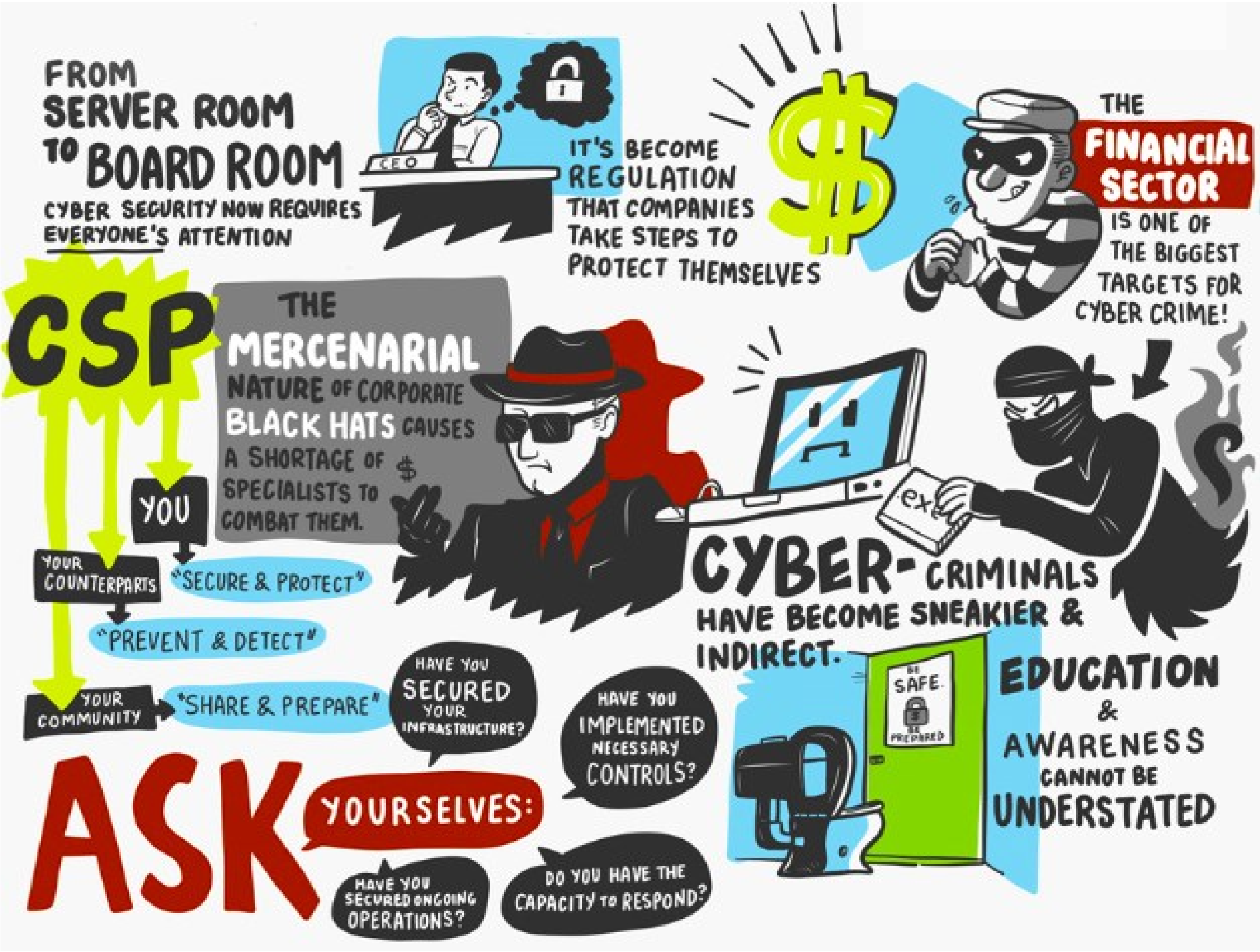
SWIFT

Cyber Resilience ACG Cross Training Seminar

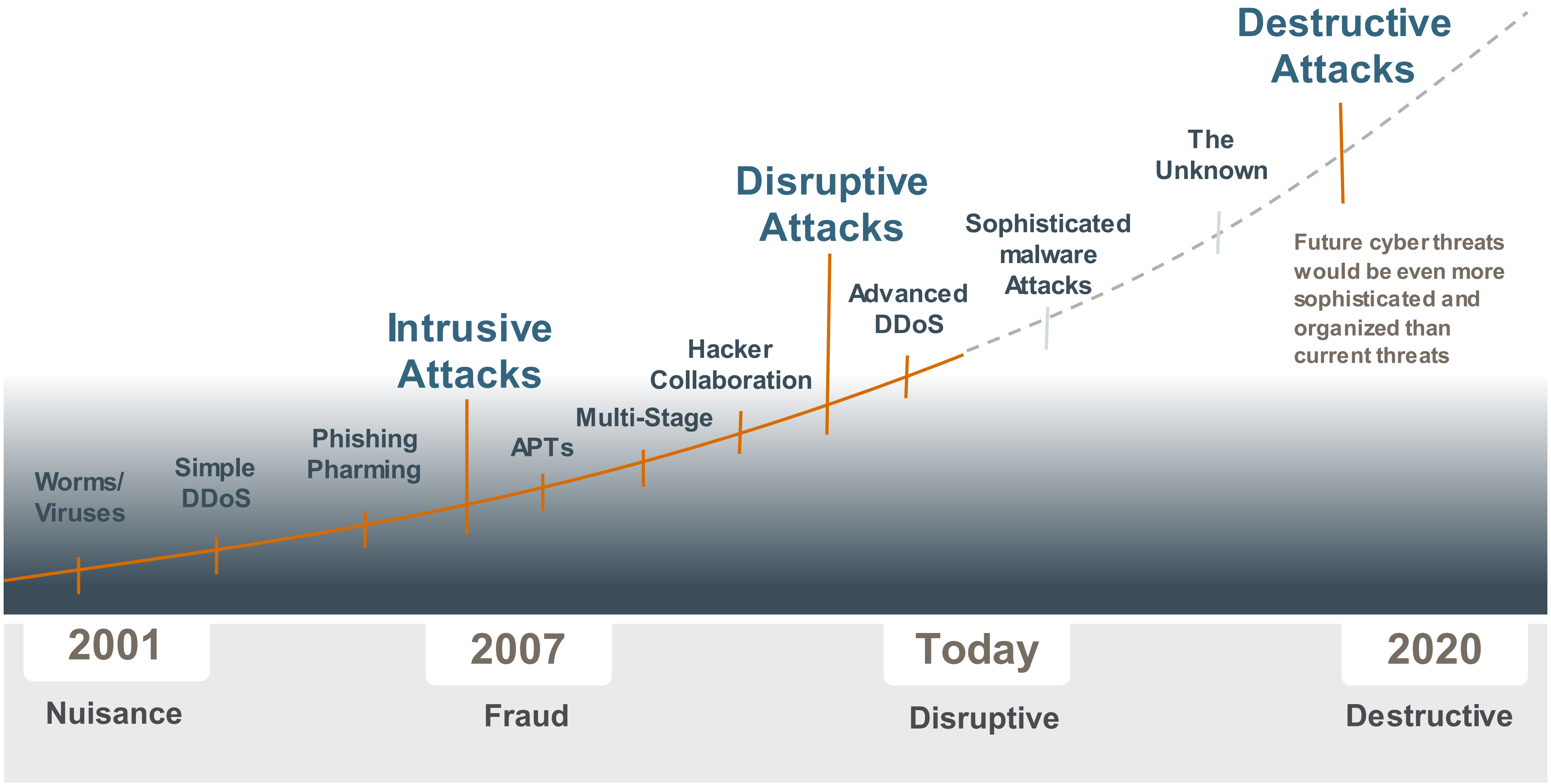
May 2018

TLP rating **AMBER**
Confidential to participants and restricted distribution

Cyber threats continue to be persistent and sophisticated

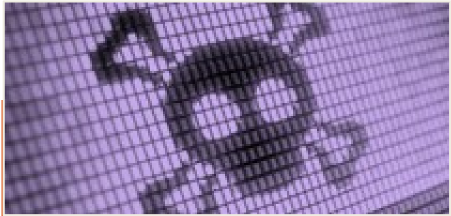

FROM SERVER ROOM TO BOARD ROOM
CYBER SECURITY NOW REQUIRES EVERYONE'S ATTENTION
CEO
IT'S BECOME REGULATION THAT COMPANIES TAKE STEPS TO PROTECT THEMSELVES
$
THE FINANCIAL SECTOR IS ONE OF THE BIGGEST TARGETS FOR CYBER CRIME!
CSP
THE MERCENARIAL NATURE OF CORPORATE BLACK HATS CAUSES A SHORTAGE OF $ SPECIALISTS TO COMBAT THEM.
YOU
"SECURE & PROTECT"
YOUR COUNTERPARTS
"PREVENT & DETECT"
YOUR COMMUNITY
"SHARE & PREPARE"
exe
CYBER-CRIMINALS HAVE BECOME SNEAKIER & INDIRECT.
BE SAFE BE PREPARED
EDUCATION & AWARENESS CANNOT BE UNDERSTATED
ASK YOURSELVES:
HAVE YOU SECURED YOUR INFRASTRUCTURE?
HAVE YOU IMPLEMENTED NECESSARY CONTROLS?
HAVE YOU SECURED ONGOING OPERATIONS?
DO YOU HAVE THE CAPACITY TO RESPOND?

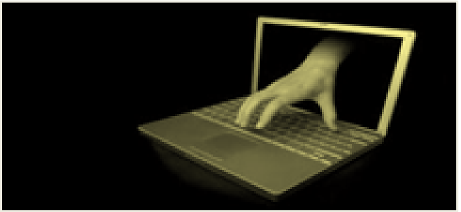
Cyber threats are evolving in frequency and sophistication



Future cyber threats would be even more sophisticated and organized than current threats

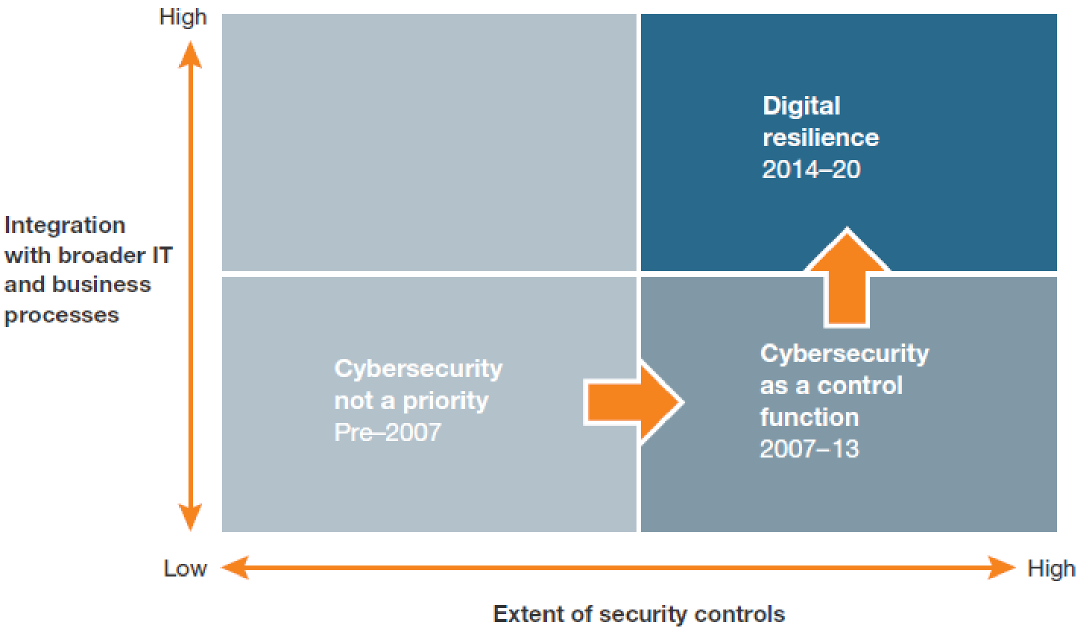
There are several threat actors that are a source of cyber risk

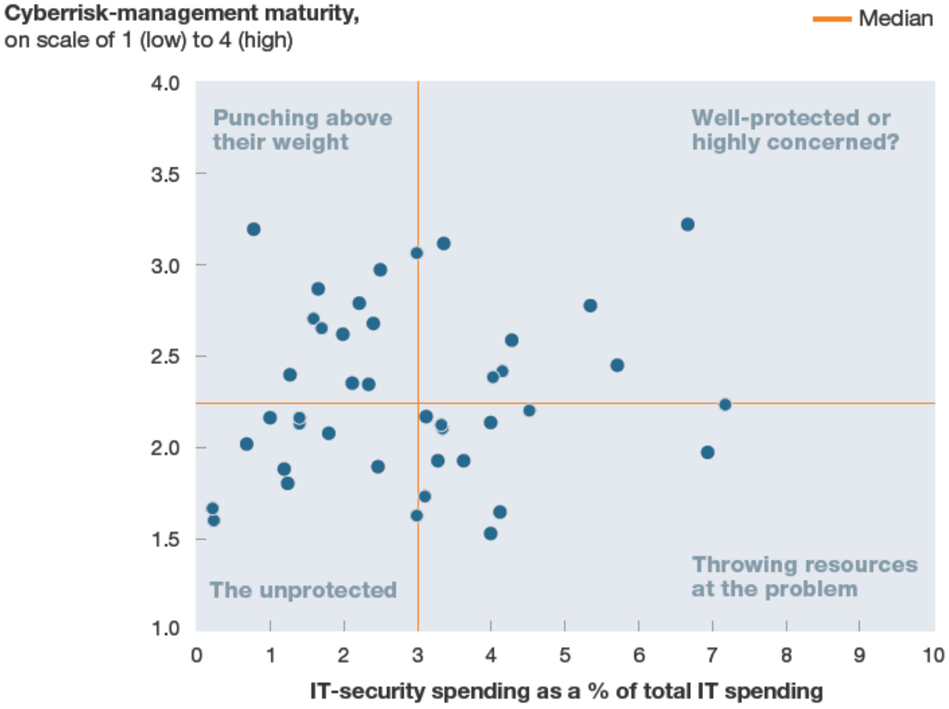




Nation State	Cyber Criminals	Hacktivists	Insider Threat
Targeted attack with a lot of pre-planning; well funded or backed by Nation States. Motivation factors include political unrest and economic disturbance.	Primary threatens the financial sector networks; Team and network size varies based upon the operation size.	Political, Religious, Ethical, or Retaliatory motive. Not motivated by money or financial gain. Bring attention to political or social cause.	Legitimate Access to applications or network. Exploit known vulnerabilities or pass on internal application/network information to outsider.
Objectives: Intellectual Property theft; competitive nation state advantage. Espionage or sabotage.	**Objectives:** financial gain; steal intellectual property;	**Objectives:** Disrupt operations; disclosure of sensitive information. Promote social ideology.	**Objectives:** Data theft; Destruction; Revenge. Fraud and Financial gain.
Type of Attacks: Advanced Persistent Threat (APT); spearphishing; identify system flaws and gain control of the system.	**Type of Attacks:** Identity theft; fraud; extortion; Malware injection	**Type of Attacks:** DDoS; exfiltration of sensitive information using hacking techniques or spearphising. Disrupt services and sabotage targets.	**Type of Attacks:** access systems using legit access; data exfiltration to personal devices. Social engineering to manipulate co-worker.

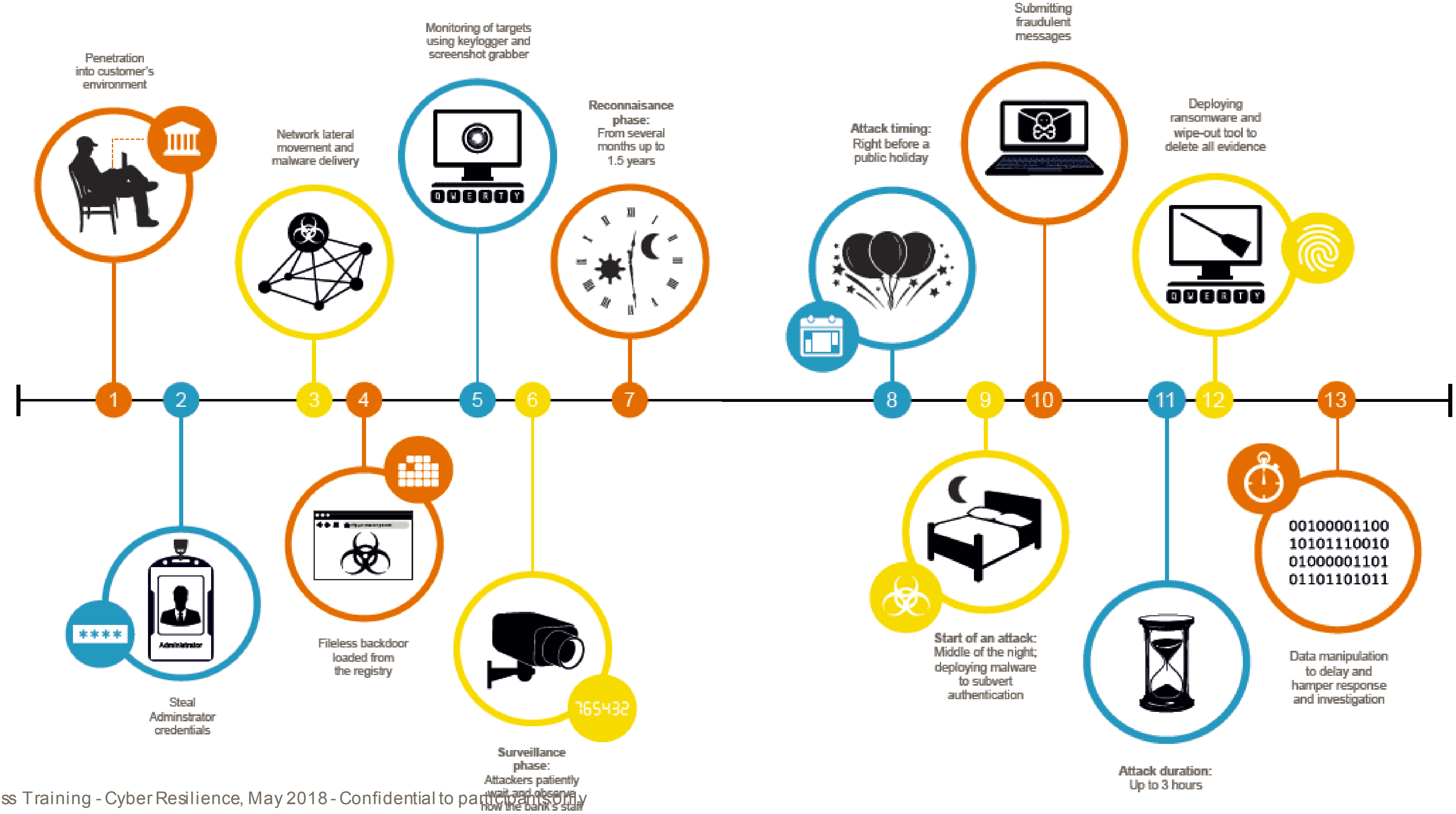
Cyber response must evolve from control to resilience


High
Integration with broader IT and business processes
Low
Digital resilience 2014–20
Cybersecurity not a priority Pre–2007
Cybersecurity as a control function 2007–13
High
Extent of security controls



Source: Bailey, Kaplan & Reznek, *Beyond Cybersecurity: Protecting Your Digital Business*, April 2015

SWIFT published a detailed case study in November 2017, customers must remain vigilant and ensure sound mitigating controls are in place



1 Penetration into customer's environment

2 Steal Adminstrator credentials

3 Network lateral movement and malware delivery

4 Fileless backdoor loaded from the registry

5 Monitoring of targets using keylogger and screenshot grabber

6 **Surveillance phase:** Attackers patiently wait and observe how the bank's staff

7 **Reconnaisance phase:** From several months up to 1.5 years

8 **Attack timing:** Right before a public holiday

9 **Start of an attack:** Middle of the night; deploying malware to subvert authentication

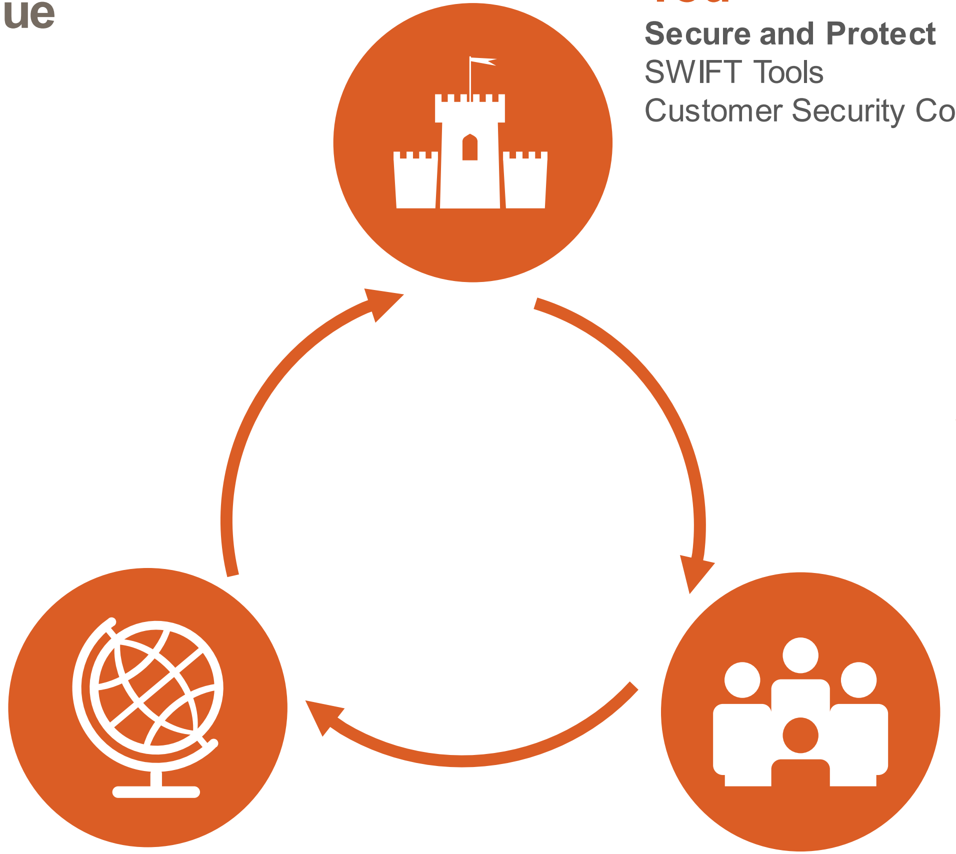
10 Submitting fraudulent messages

11 **Attack duration:** Up to 3 hours

12 Deploying ransomware and wipe-out tool to delete all evidence

13 Data manipulation to delay and hamper response and investigation

The Customer Security Programme (CSP) will continue to support our customers in responding to cyber threats, based on these three pillars



You

Secure and Protect
SWIFT Tools
Customer Security Controls Framework

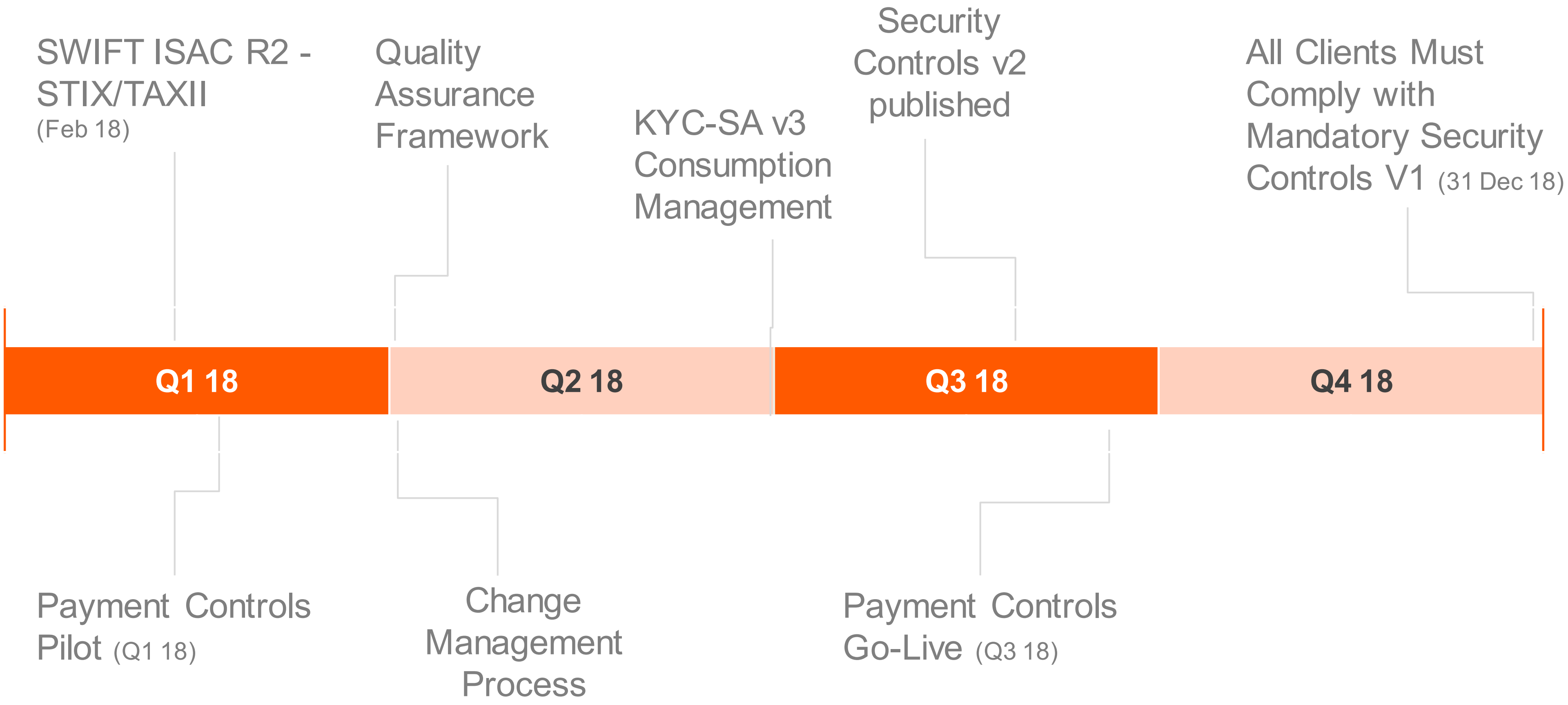
Your Counterparts

Prevent and Detect
Transaction Pattern Detection –
RMA, DVR and Payment Controls

Your Community

Share and Prepare
Intelligence Sharing
SWIFT ISAC Portal

In 2018, key milestones around cyber intelligence sharing, evolution of the control framework and new anti-fraud tools are planned



SWIFT ISAC R2 - STIX/TAXII (Feb 18)

Quality Assurance Framework

KYC-SA v3 Consumption Management

Security Controls v2 published

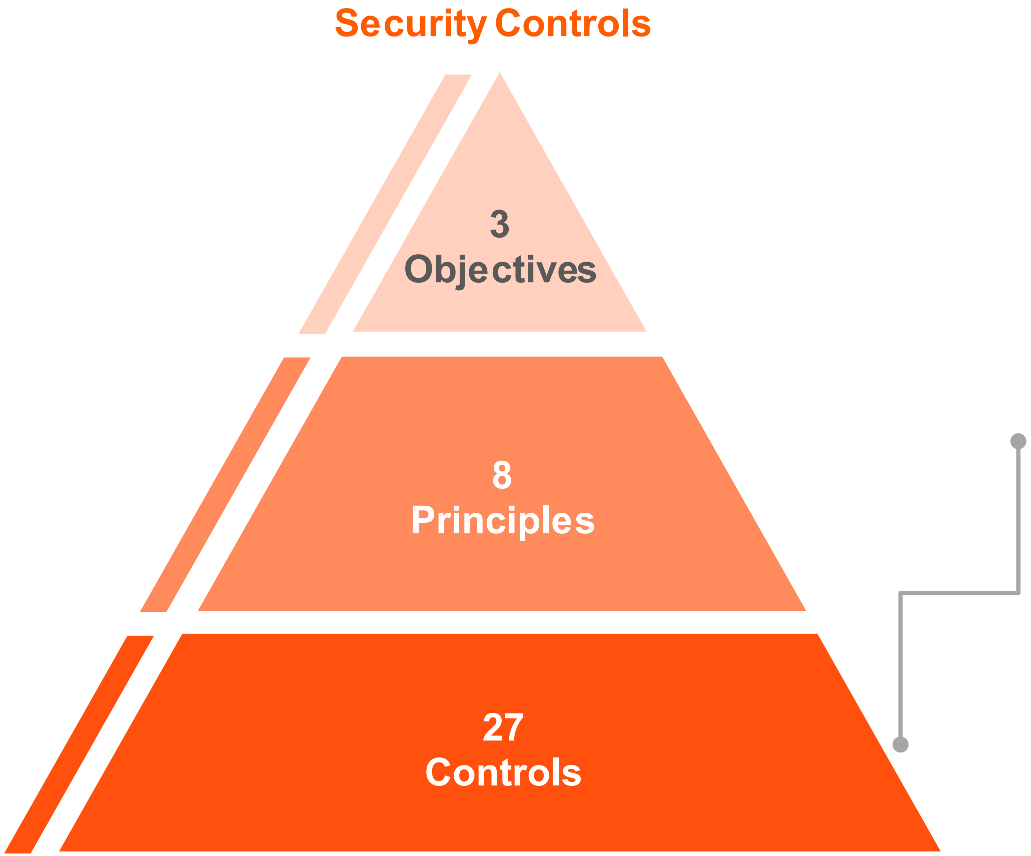
All Clients Must Comply with Mandatory Security Controls V1 (31 Dec 18)

Payment Controls Pilot (Q1 18)

Change Management Process

Payment Controls Go-Live (Q3 18)

SWIFT Customer Security Controls Framework
27 Controls



The 8 security principles are put into practice with 27 controls. **16 mandatory, 11 advisory.**

- in line with existing information security industry standards, and product-agnostic.
- expected to evolve over time in light of the changing cyber-threat landscape

Mandatory security controls

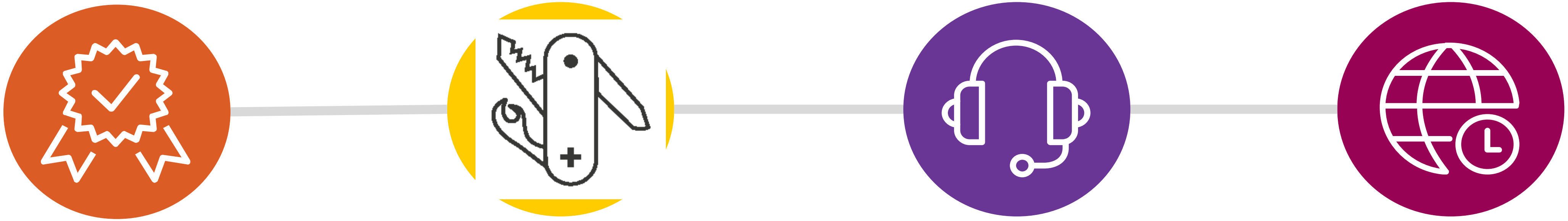
- establish a security baseline for the entire community
- all users must self-attest against their implementation on their local SWIFT-related infrastructure.
- set a realistic goal for near-term, tangible security gain and risk reduction.

Advisory controls

- based on good practice that SWIFT recommends customers implement on their local SWIFT-related infrastructure.

Cyber resilience must be considered from multiple perspectives – technology, processes and people

Are you prepared to respond to these persistent and sophisticated cyber threats?



Have you secured your infrastructure?

Have you implemented necessary controls?

Do you have the capacity to respond?

Have you secured your ongoing operations?

Questions

www.swift.com