Cyber Threats and Resiliency: Customer Security Programme

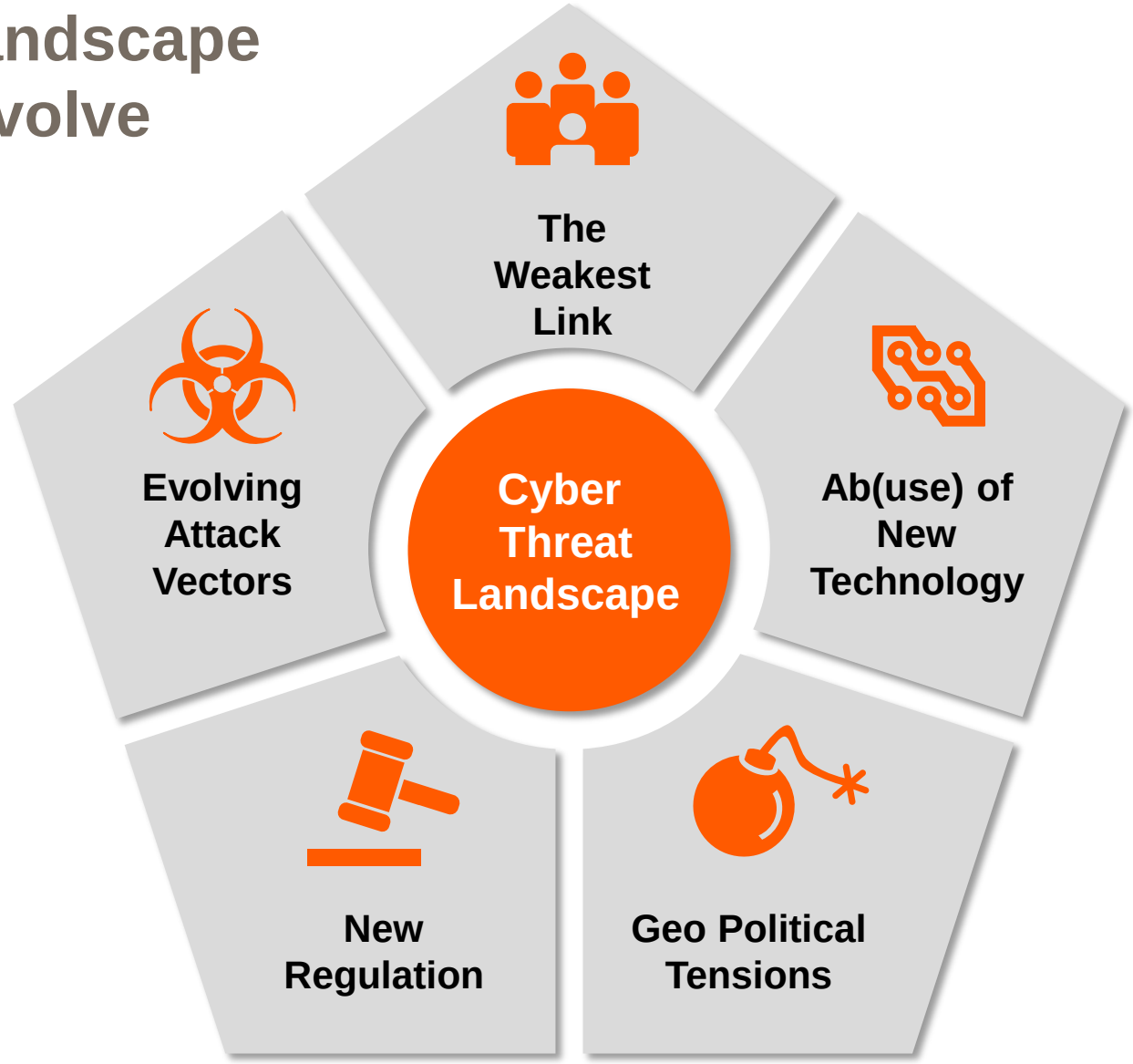
Mark Buysse

Abu Dhabi, Arab Regional Fintech Meeting

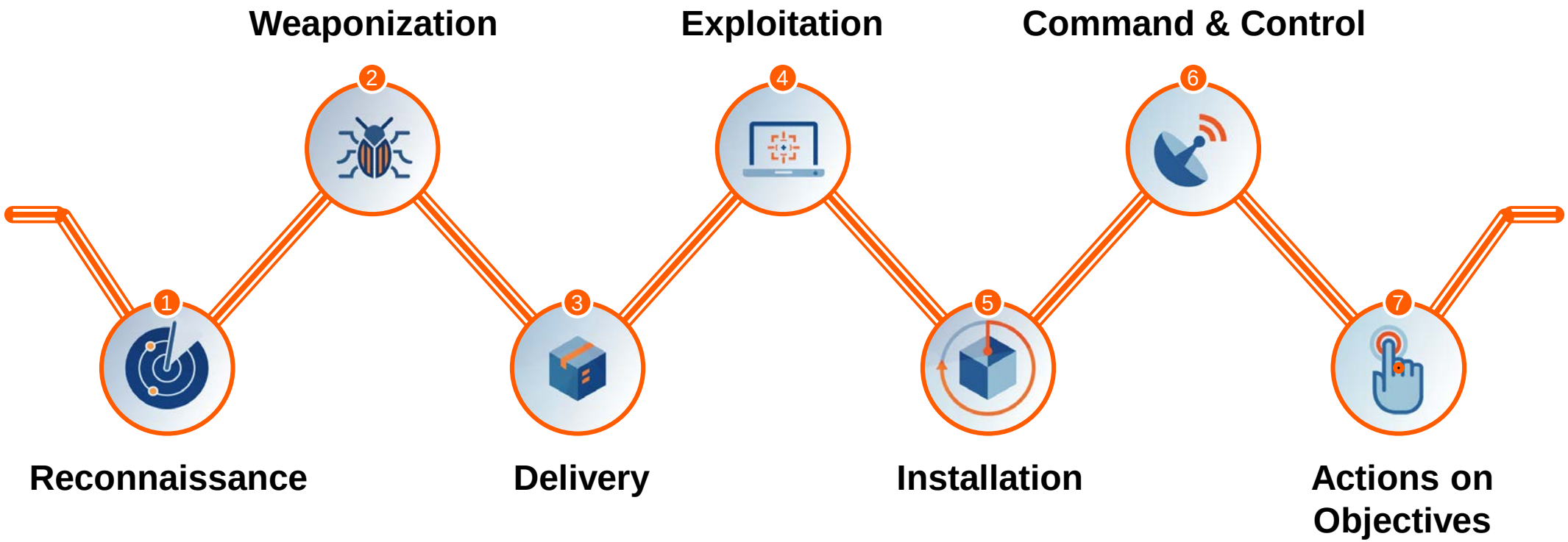
Cyberattacks on SWIFT customers continues

For 2019, the rate of new, confirmed customer cases is similar to 2018

Cyber threat landscape continues to evolve



These APT attacks follow the ‘cyber kill chain’



1 month to 2 years	In customers’ environment
0 to 2 weeks	In customers’ messaging interface
0 to 6 hours	Sending fraudulent messages

THE CYBER KILL CHAIN® LOCKHEED MARTIN

Many of the attacks are attributed to Lazarus

Lazarus | Bluenoroff | APT38

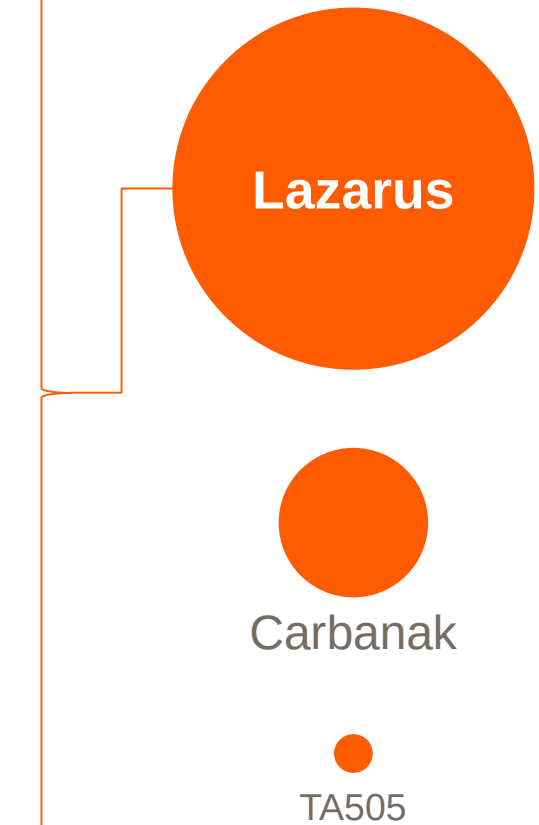
Chollima - Mythical Winged Horse

Experts identify as nation-state sponsored, well funded and patient with sophisticated APT TTPs and malware

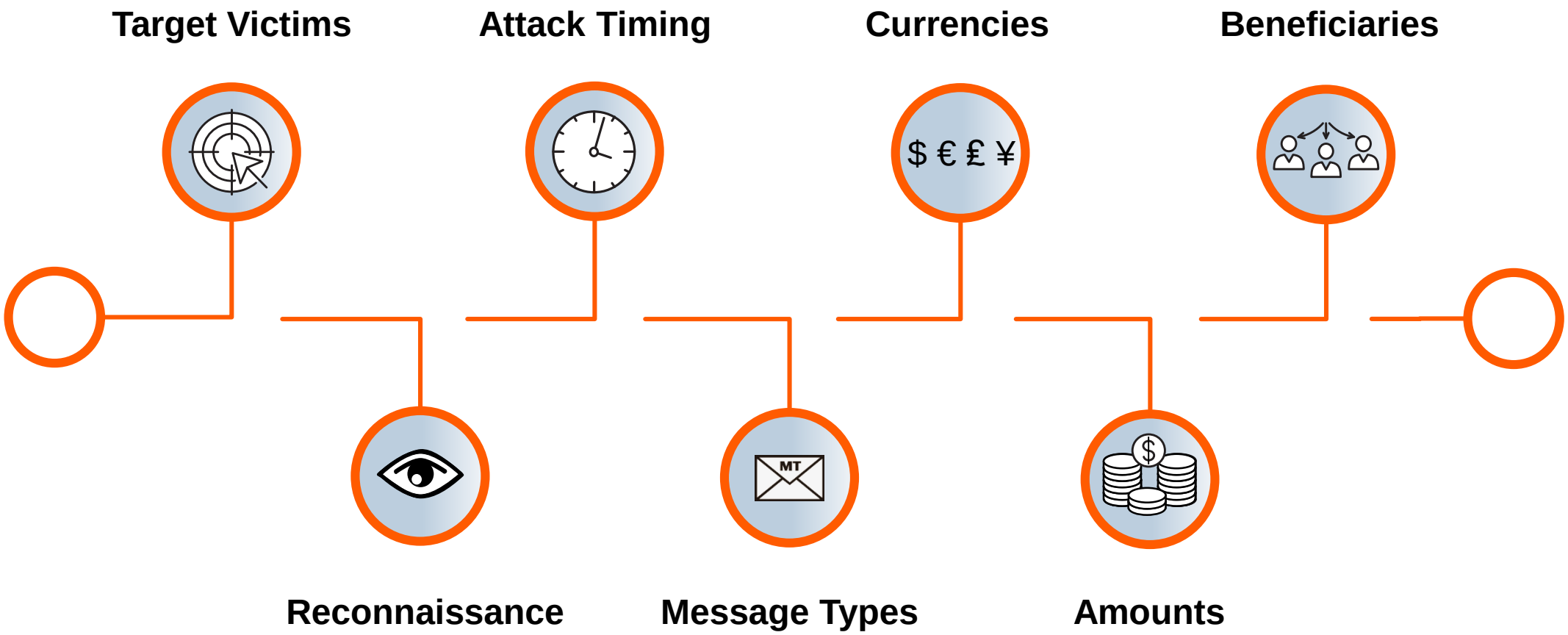
Constantly adapting and evolving – modifies malware to try to circumvent additional security measures such as alerting, file-based detection and 2FA

Believed to work with other criminal groups e.g. ATM cash-outs

Tools and malware sets have evolved over time



Common risk factors have emerged



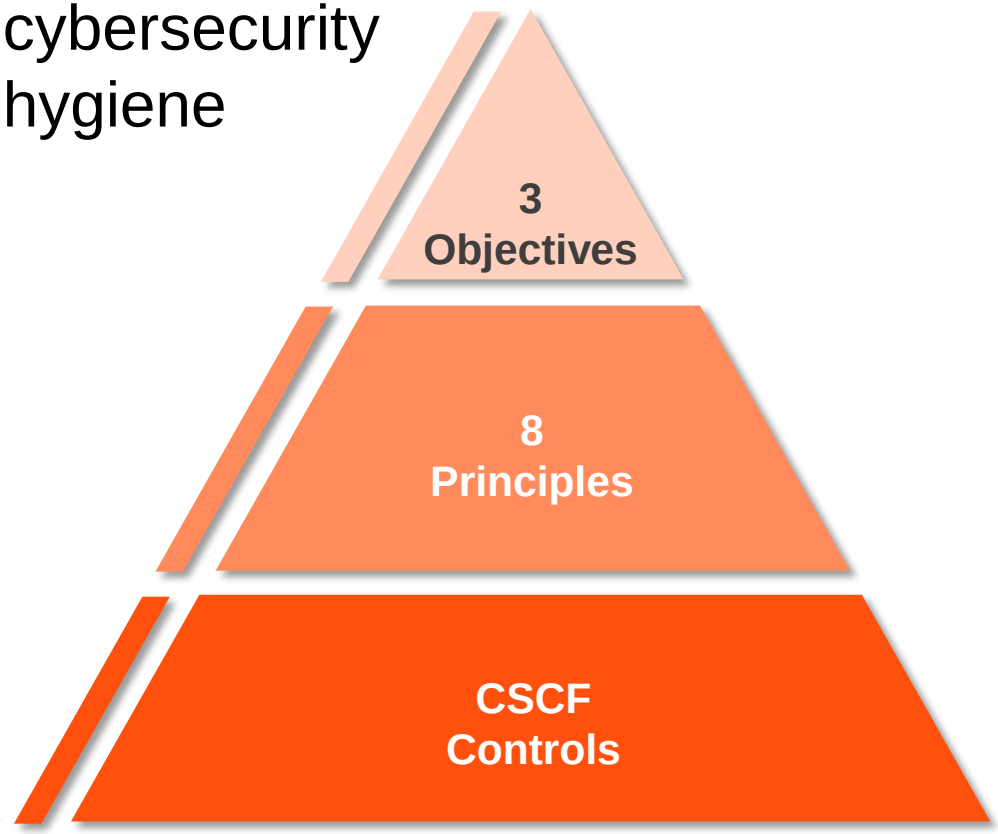
Customer Security Programme

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

Where we are now | controls

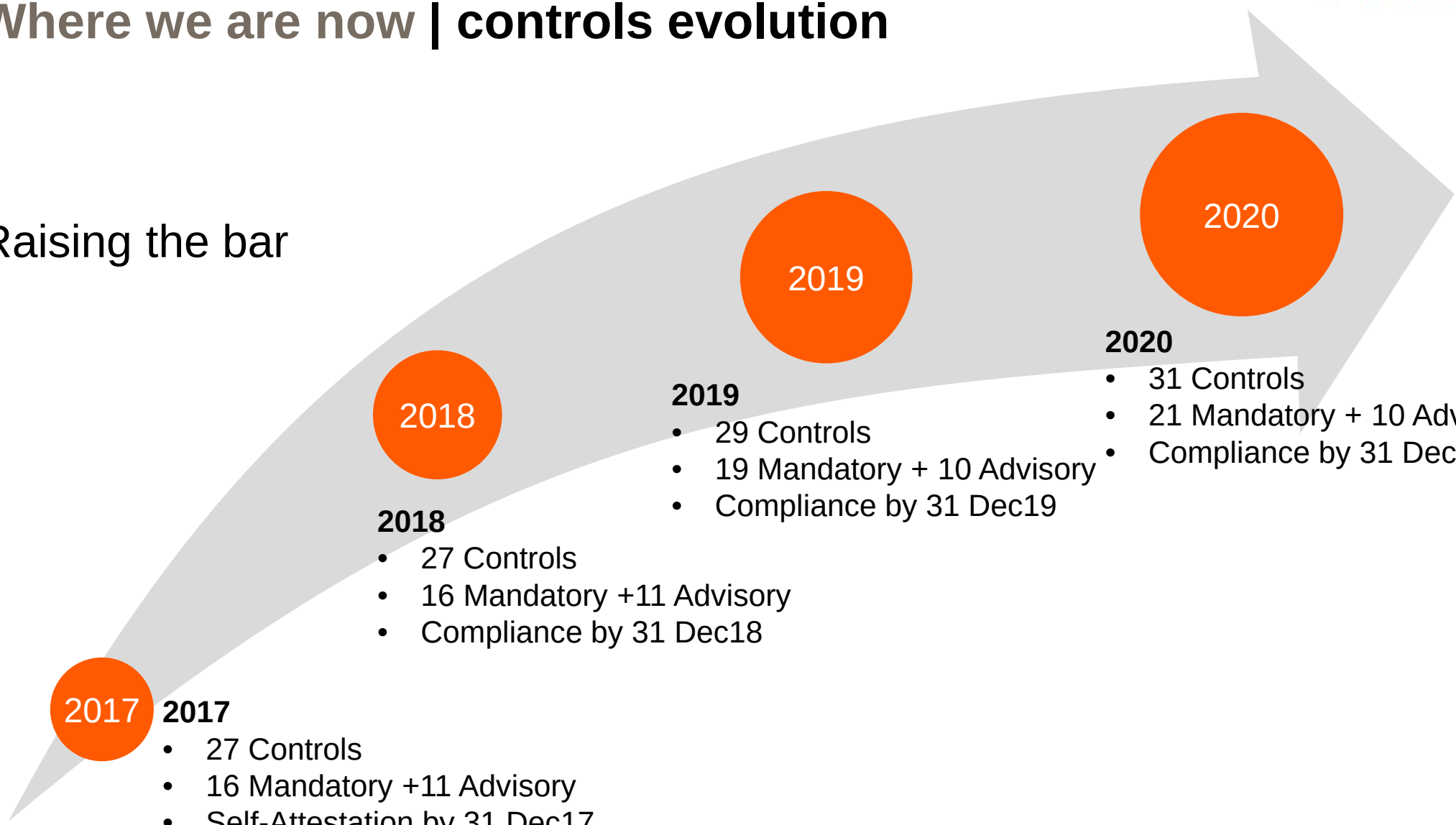
Improve cybersecurity hygiene



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

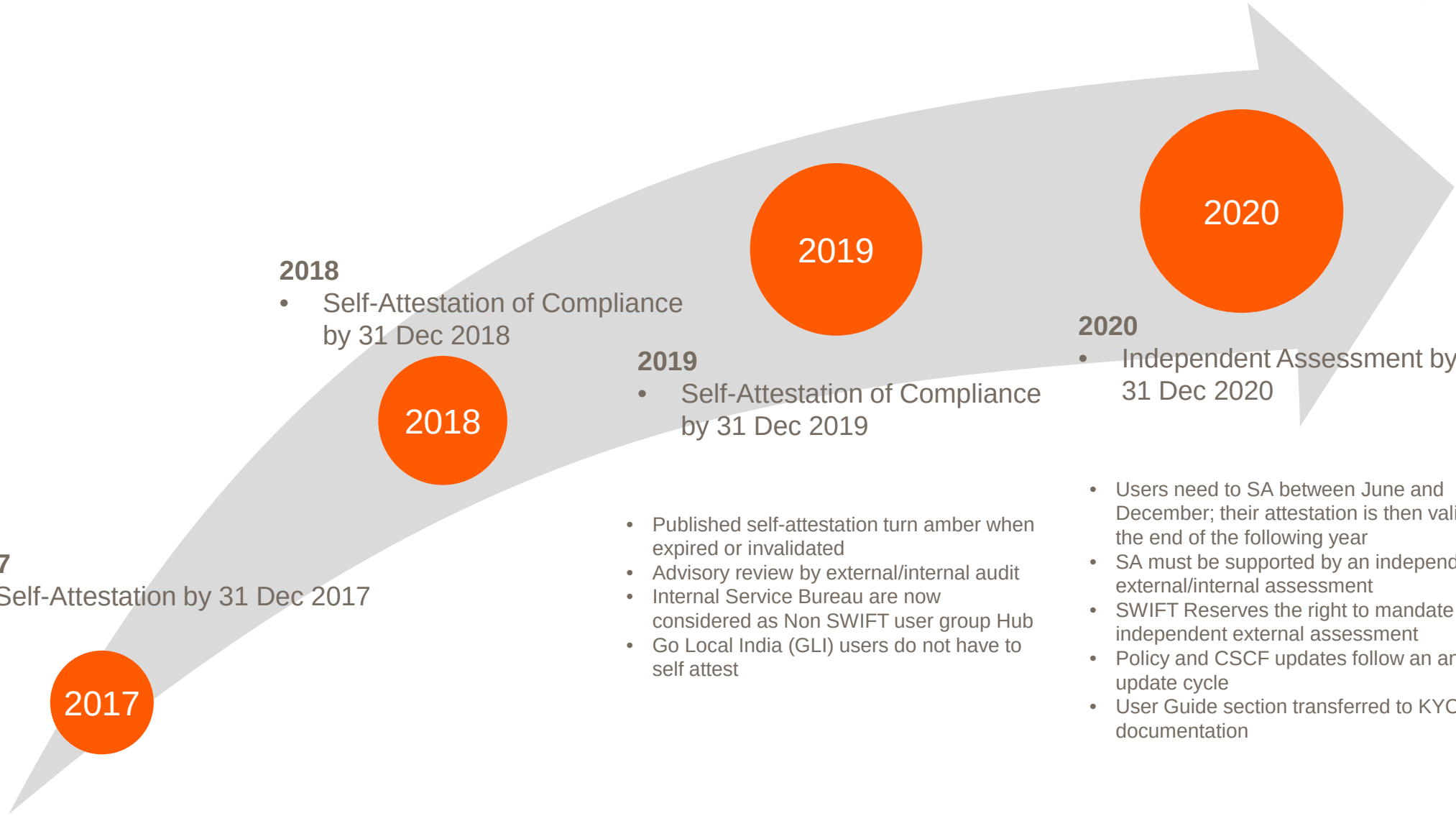
2018
- 27 Controls
- 16 Mandatory +11 Advisory
- Compliance by 31 Dec18

2019
- 29 Controls
- 19 Mandatory + 10 Advisory
- Compliance by 31 Dec19

2020
- 31 Controls
- 21 Mandatory + 10 Advisory
- Compliance by 31 Dec20

CSP | Policy Evolution

Customer Security Programme



2017
- Self-Attestation by 31 Dec 2017

2018
- Self-Attestation of Compliance by 31 Dec 2018

2019
- Self-Attestation of Compliance by 31 Dec 2019

2020
- Independent Assessment by 31 Dec 2020

- Published self-attestation turn amber when expired or invalidated
- Advisory review by external/internal audit
- Internal Service Bureau are now considered as Non SWIFT user group Hub
- Go Local India (GLI) users do not have to self attest

- Users need to SA between June and December; their attestation is then valid till the end of the following year
- SA must be supported by an independent external/internal assessment
- SWIFT Reserves the right to mandate an independent external assessment
- Policy and CSCF updates follow an annual update cycle
- User Guide section transferred to KYC-SA documentation

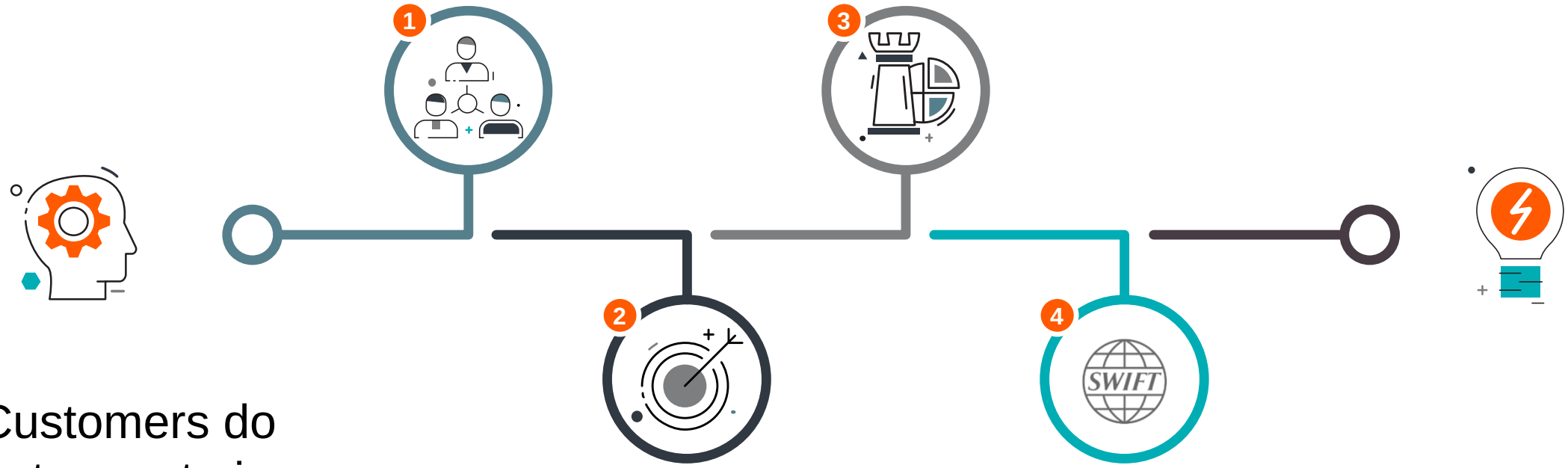
Where we are now | assurance

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 | counterparty risk management

Establish a **governance** model

Adopt cybersecurity risk **countermeasures**



Customers do not operate in a vacuum

Establish a cybersecurity **risk management** framework

Incorporate cybersecurity **attestation data** from SWIFT counterparties

SWIFT actively shares its intelligence


Questions

www.swift.com