SWIFT Customer Security Programme (CSP)

Promoting information security in the financial community

November 5th, 2017

Alain Desausoi, Deputy CISO, SWIFT

Cybersecurity trends in 2017 and beyond

- **Increase** and expansion of cyber threats against the cloud and IoT
- More and different **ransomware**
- Increase of nation-state/cyberwar issues
- **Machine learning** accelerates social engineering attacks
- "The commodification of attacks along the lines of the 2016 Bangladesh heist — with specialized resources being offered for sale in underground forums or through as-a-service schemes, will continue in 2017. **As payment systems become increasingly popular and common, this will be matched by a greater criminal interest (…)**"

Cybercrime is everybody's business *- we need a* ***systemic*** *and* ***global*** *approach to respond to this challenge*

Sources: www.govtech.com, Dan Lormann on Cybersecurity & Infrastructure, 'The Top 17 Security Predictions for 2017 ', 8 January 2017 (including Symantec, Trend Micro, McAfee, Forcepoint, FireEye, Kaspersky, Palo Alto Networks, Watchguard Technologies, Imperva, Checkpoint, Forrester, Gartner, White Hat Security, Sophos, IDC, IBM)

Impact of cyberthreats on payment operations

Impact of cyberthreats on payment operations

Customer Security Programme (CSP)

CSP Update | Modus Operandi

Step 1	Step 2	Step 3	Step 4
Attackers compromise customer's environment	*Attackers obtain valid operator credentials*	*Attackers submit fraudulent messages*	*Attackers hide the evidence*

- Attackers are well-organised and sophisticated
- Common starting point has been a security breach in a customer's local environment
- There is (still) no evidence that SWIFT's network and core messaging services have been compromised

High-level view of the Customer Security Programme

High-level view of the Customer Security Programme

CSP Update | Programme Overview

You

Secure and Protect

SWIFT Tools
Security Guidelines and Assurance

Your Community

Share and Prepare

Intelligence Sharing

Your Counterparts

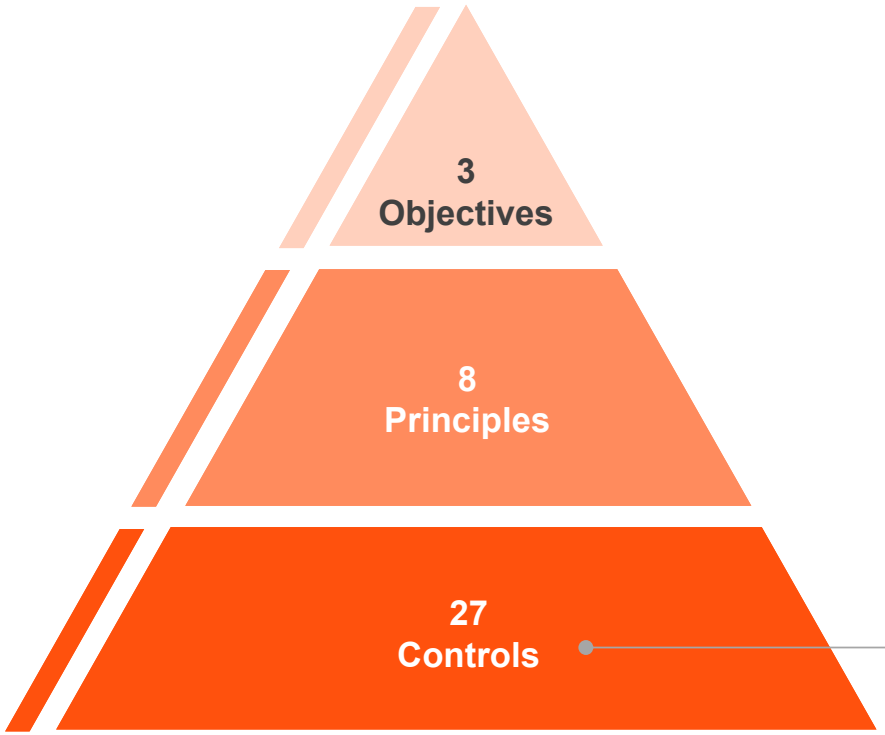
Prevent and Detect

Transaction Pattern Detection - RMA and DVR

Launched on May 27th 2016, CSP supports all customer segments, whether directly or indirectly connected, in reinforcing the security of their SWIFT-related infrastructure

CSP Update | You > Security Guidelines and Assurance

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

- *Applicable to all customers and to the whole end-to-end transaction chain beyond the SWIFT local infrastructure*
- *Mapped against recognised international standards – NIST, PCI-DSS and ISO 27002*
- *16 controls are mandatory, 11 are advisory*
- *Final version published March 31, 2017*

Customer Security Programme

CSP | Customer Security Attestation Process (CSAP): Four Main Steps

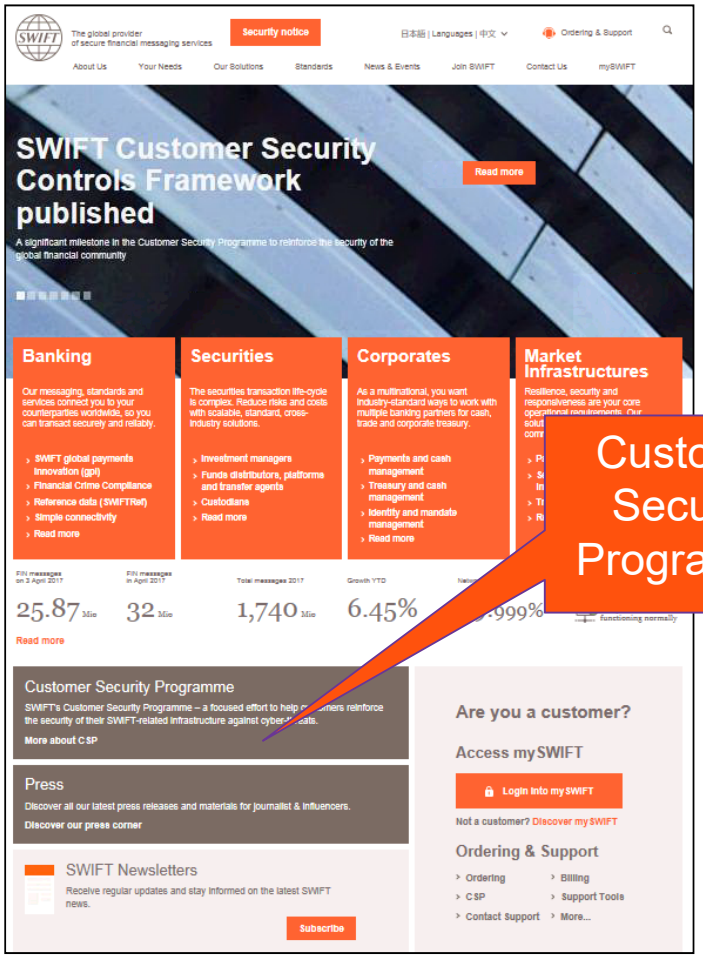
1. Submission of self-attestation

2. Grant access to counterparties

3. Follow-up activities to drive compliance and improve security

4. On-going quality checks

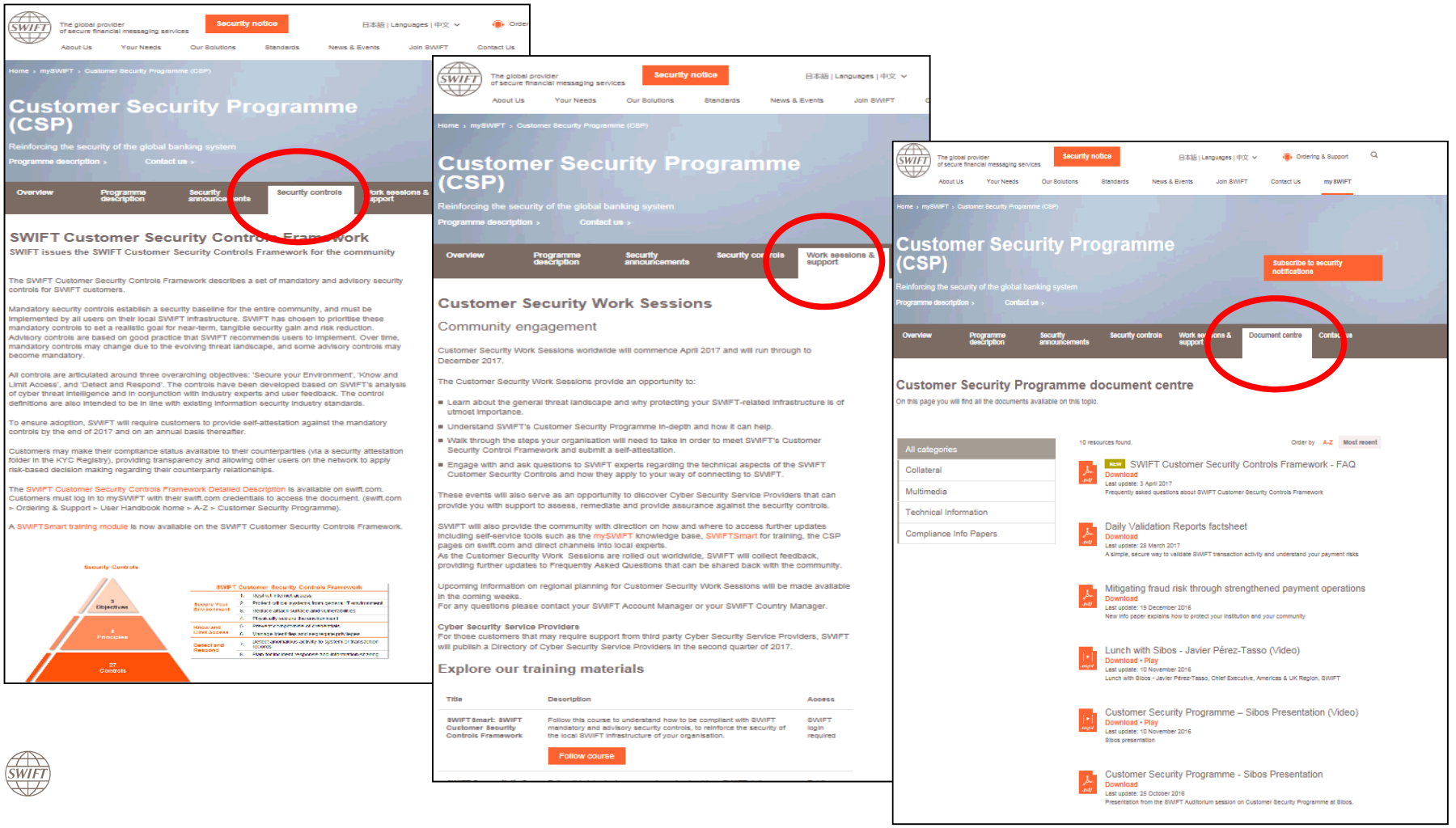
CSP | swift.com



Customer Security Programme

Customer Security Programme

CSP | swift.com/CSP



Feedback, questions and open discussion

www.swift.com