Customer Security Programme (CSP) @ SWIFT

Emerging Trends in Critical Infrastructure Protection: Preventing & mitigating potential threats

November 2016

v14

CSP | Modus Operandi

- Common starting point has been a security breach in a customer's local environment
- In all cases, the SWIFT's network and core messaging services have not been compromised
- Attackers are well-organised and sophisticated

Step 1

Attackers compromise customer's environment

- Attackers compromise the bank's local environment by introducing malware either directly at the bank or remotely, e.g. e-mail phishing campaigns, via a USB stick or rogue internet URLs
- Attack can be started from either a malicious insider or an external attacker, or both

Step 2

Attackers obtain valid operator credentials

- Attackers are looking for valid account ID and password credentials from staff who have legitimate access to payment infrastructure
- Once they obtain them, they have the 'keys' to the system
- At this stage they very often watch and wait to familiarise themselves with how banks' back office process and systems work

Step 3

Attackers submit fraudulent messages

- Once an attacker has valid credentials and enough knowledge on how to access and use the applications, they can log in, impersonate the operators from whom they stole the credentials, and submit fraudulent payments – all without raising suspicion
- Sometimes happens outside the normal bank working hours

Step 4

Attackers hide the evidence

- Attackers hide the evidence
- Numerous methods have been used, e.g. tampering with the reconciliation process; deleting or manipulating records / logs either remotely or using malware
- This wins time to make sure the transfer of funds happens without detection

CSP | Framework

Customer Security Programme

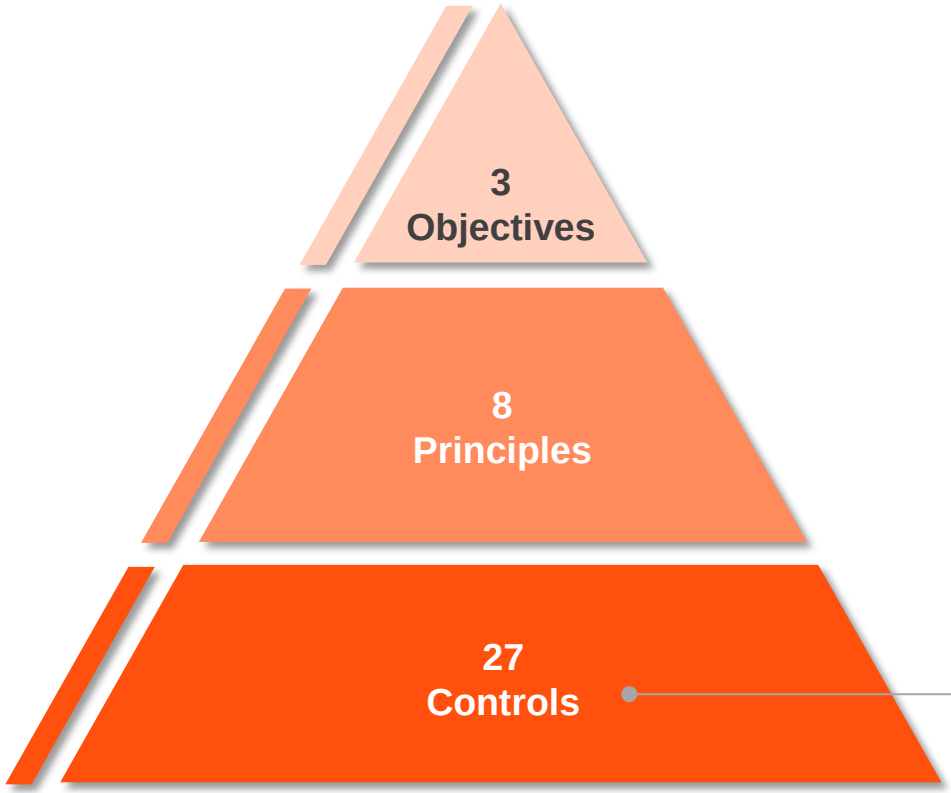
While all SWIFT customers are individually responsible for the security of their own environments, a concerted, industry-wide effort is required to strengthen end-point security

On May 27th SWIFT announced its Customer Security Programme that supports customers in reinforcing the security of their SWIFT-related infrastructure

CSP focuses on mutually reinforcing strategic initiatives, and related enablers

CSP | You > Security Guidelines and Assurance

Security Controls



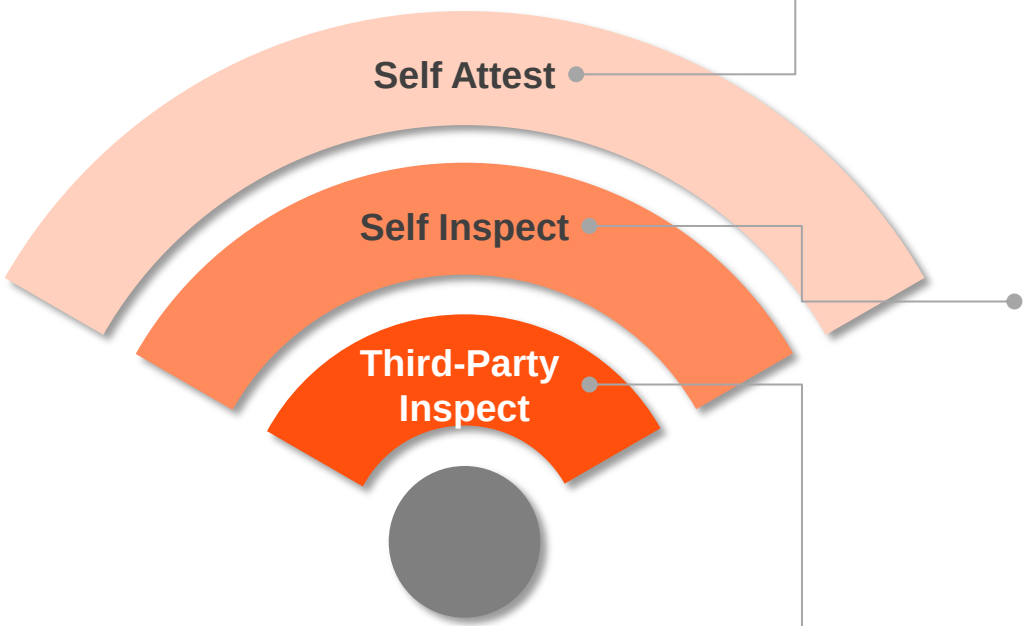
CSP Security Controls Framework

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
- Some controls are mandatory, some are advisory
- Documentation and collateral will be available by end of October

CSP | You > Security Guidelines and Assurance

Assurance Framework



Self-Attestation

- Where customer positively asserts that it meets the security requirements
- First- and second-line of defence – provided by senior management
- All customers with an interface
- All customers with a small local footprint

Self-Inspection

- Where customer's Internal Audit asserts that the customer meets the security requirements
- Third-line of defence - provided by IA function
- Risk based sample of customers with a small local footprint

Third-Party Inspection

- For an external party that provides independent validation that the customer meets the security requirements
- All traffic concentrators (extended SIP), executed by SWIFT
- Risk based sample of customers with an interface, executed by third-party auditors

CSP | Open Discussion

Questions and
open discussion

www.swift.com