Customer Security Programme / CSP

Hugo Solano – Regional Product Manager
Miguel Suarez - Head of Central America and Caribbean

August 9, 2017

The global provider of secure financial messaging services

SWIFT
in figures

30.3 million

FIN messages peak day (2016)

6.5+ billion

FIN messages per year (2016)

6.9%

Increase in FIN traffic (2016)

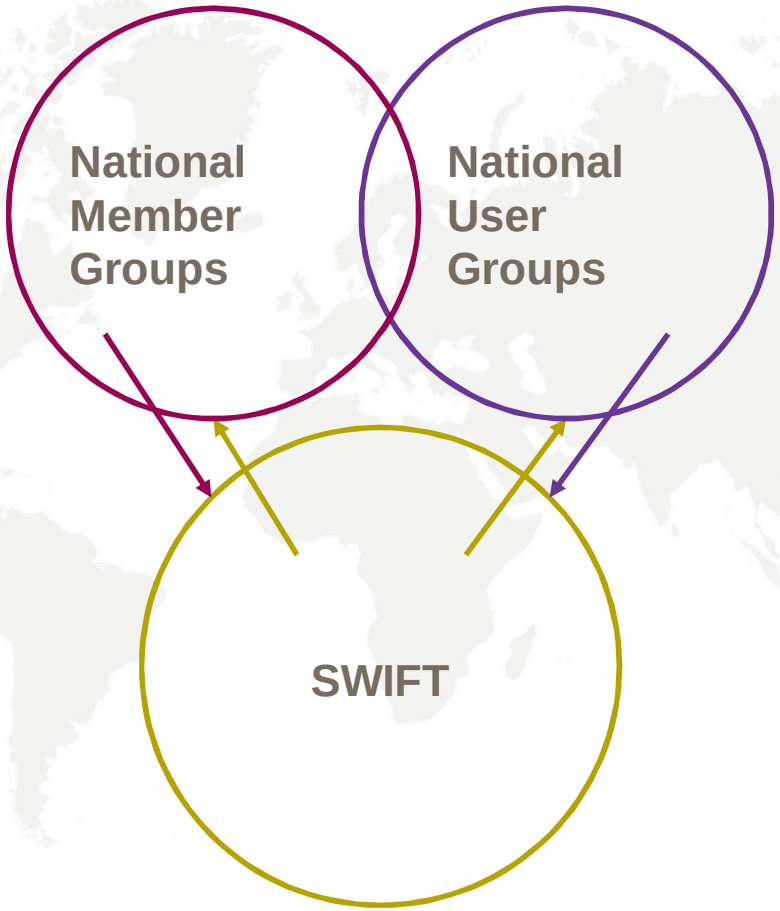
11,000+

SWIFT users

200+

Countries and territories

Global ownership, global representation

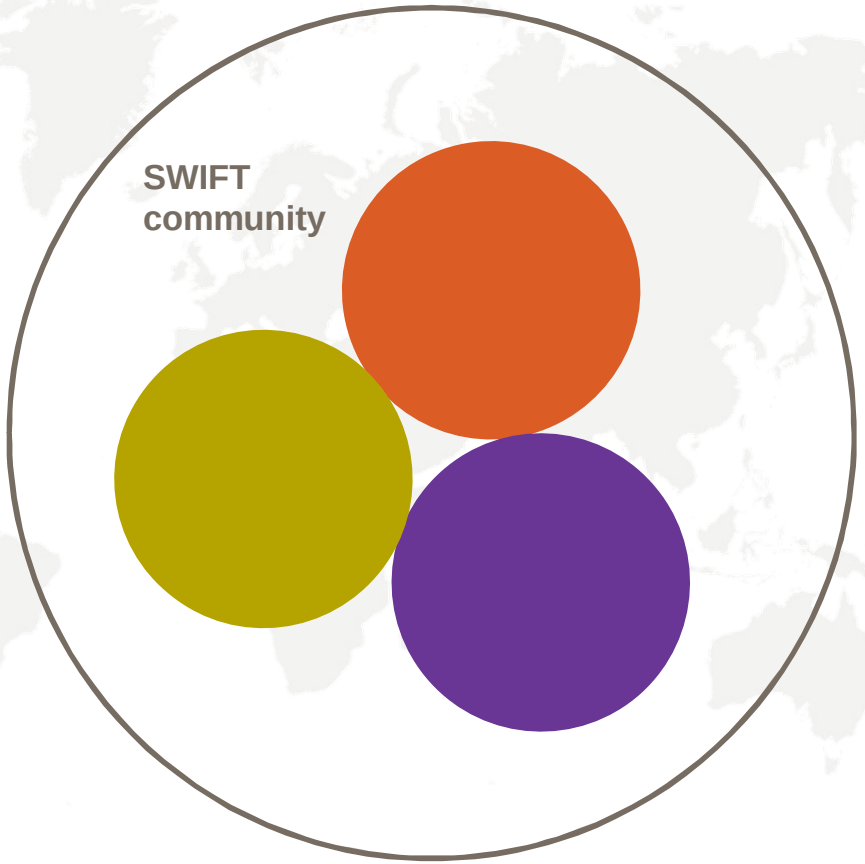


User categories

Shareholders and Supervised Financial Institutions

Non-Supervised Entities active in the financial industry

Closed User Groups / Corporates



SWIFT users

Banks Fund Managers

Central Counterparties

Clearing & Settlement Systems

Corporates Broker-Dealers ICSDs

Central Banks Global Custodians

CSDs Stock Exchanges

Depositories Trade Repositories

What is the concern?

2016 cases prove that the financial industry is at serious risk of cyber-attack

Attacks are global, sophisticated, and here to stay!

Why is it important? Cyber challenges are here to stay

Central Banks To Review Security For Wholesale Payments

By **Melissa Lipman**

Law360, London (September 16, 2016, 6:49 PM BST) -- A group of central bankers plans to review security procedures for wholesale payments involving financial institutions in light of growing concerns over cyber fraud, the Bank for International Settlements said Friday.

The BIS' Committee on Payments and Market Infrastructures — a global standard-setting body for payment, clearing and settlement services made up of central banks from G-10 countries — set up a task force to look at security used for payments involving banks, financial market infrastructures like central clearing counterparties, and other institutions.

The task force will start by reviewing the current security practices used for wholesale payments before the committee decides what to do next, according to CPMI Chairman Benoît Cœuré.

"Recent incidents of cyber fraud are of significant concern for the central banking community, and we are working to make sure there are adequate checks and balances in place at each stage of the payments process," Cœuré said. "It is premature to speculate what will result from this work."

The task force will build on other work the committee has done involving cybersecurity and efforts to bulk up financial infrastructure.

WHEN REPORTS SURFACED in February of a spectacular bank hack that sucked $81 million from accounts at Bangladesh Bank in just hours, news headlines snickered over a typo that prevented the hackers from stealing the full $1 billion they were after.

Last week the snickering stopped with new reports that the hackers struck a second bank, and possibly others—though authorities won't say if those heists were equally successful. Bank hacks have traditionally focused on stealing the login credentials of bank account holders—either individuals or small businesses. Billions have been stolen successfully in this way. But the hacks in this case targeted the banks themselves and focused on subverting their SWIFT accounts, the international money transfer system that banks use to move billions of dollars daily between themselves.

Consumers worried about falling victim to online banking fraud should consider banks that give customers card readers and avoid those which rely on text messages, according to leading security expert Graham Cluley. He was speaking as Tesco Bank continued to deal with the fallout from the "systematic, sophisticated attack" that resulted in £2.5m being taken from around 9,000 current account holders.

Meanwhile, another expert says that the Tesco attack last weekend could be the first of many, and banks should be forced by regulators to up their game.

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***

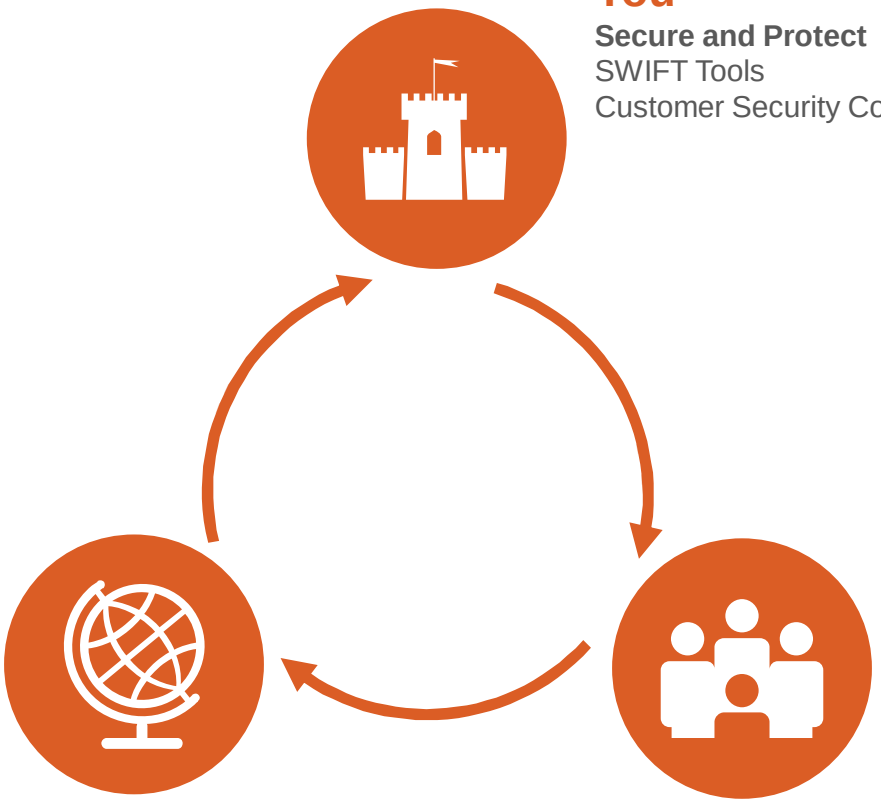
- Attackers are well-organised and sophisticated
- Common starting point has been a security breach in a customer's local environment
- There is no evidence that SWIFT's network and core messaging services have been compromised

Why is SWIFT getting involved?

SWIFT wants to help its customers to take action to **secure their local SWIFT infrastructure**, in light of cyber threats.

Customer Security Programme (CSP)

SWIFT launched the Customer Security Programme to help customers **reinforce the security of the global banking system.**



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

How will SWIFT help me to secure my local infrastructure?

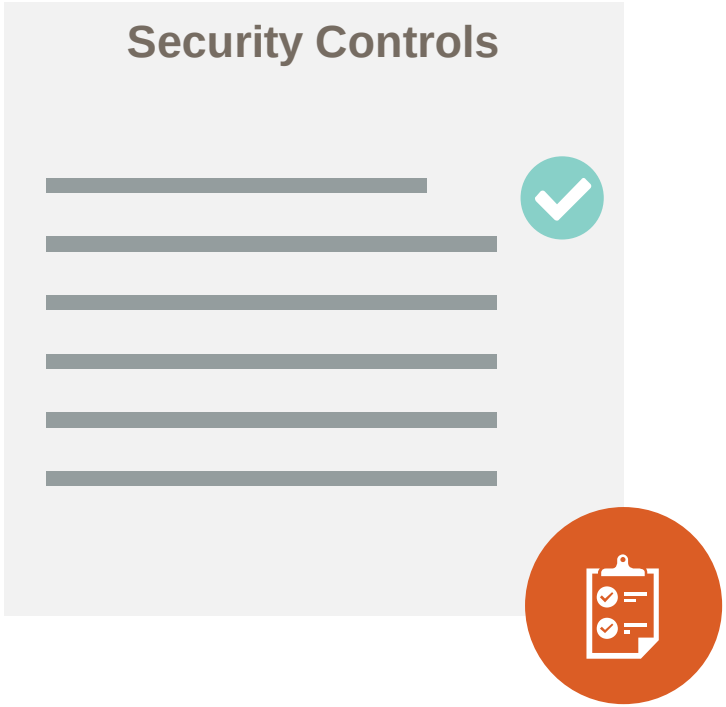
The SWIFT Customer Security Controls Framework

Customer Security Controls Framework
SWIFT is creating a security baseline

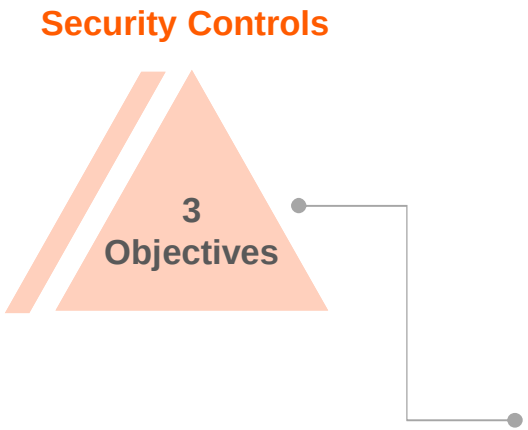
SWIFT has introduced a core set of security controls that every SWIFT customer must implement.

We are making these security controls **mandatory** for all customers to set a **security baseline** for the whole industry.

You will need to **implement the controls that are relevant to your organisation**, and attest your level of compliance **before the end of 2017**.



SWIFT Customer Security Controls Framework
3 Objectives



1. Secure Your Environment

Secure your environment from cyber attacks

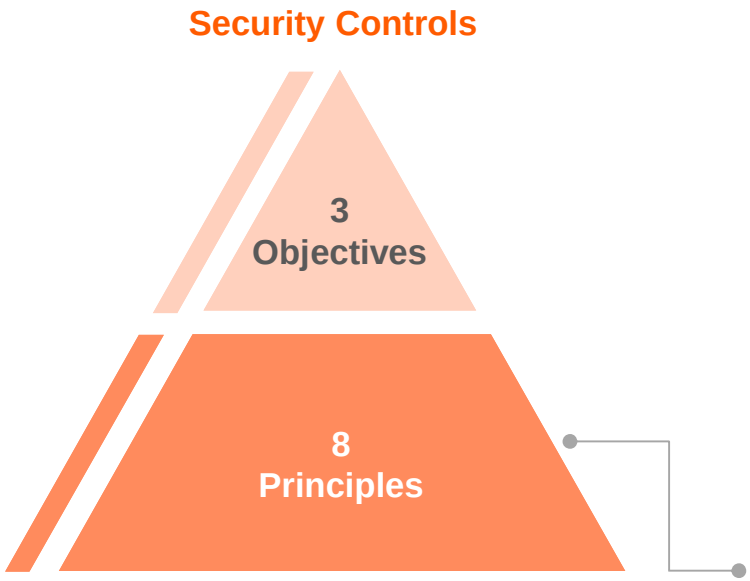
2. Know and limit access

Know and **limit access of people** to the local SWIFT environment

3. Detect and respond

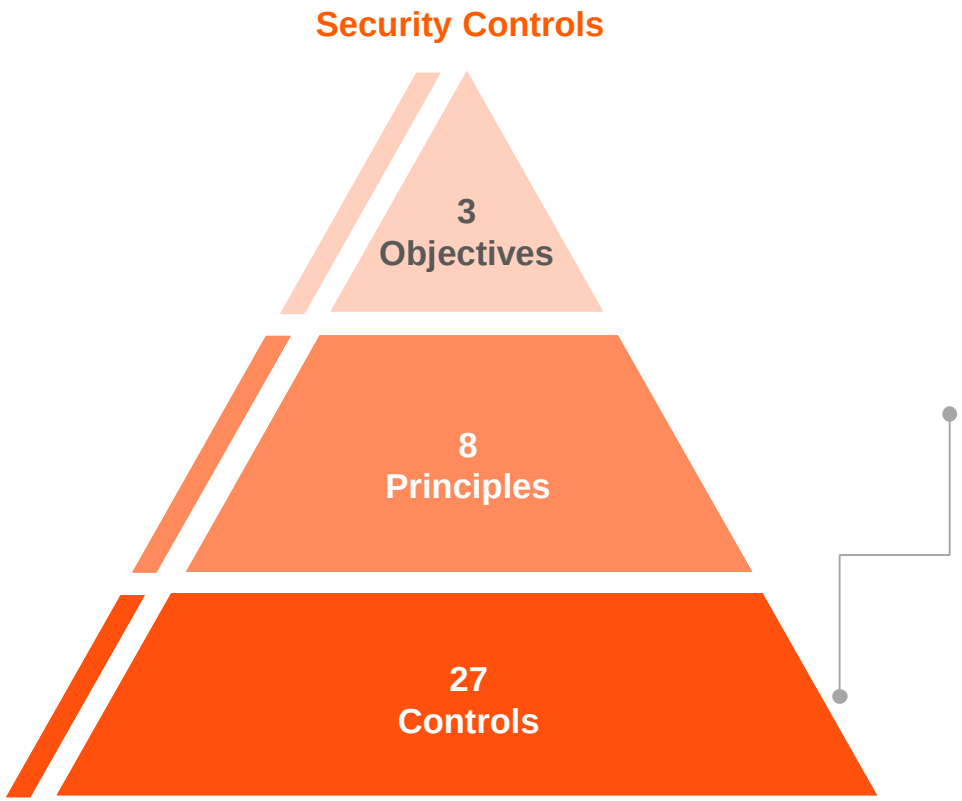
Promptly **detect and respond** in case of a cyber attack

SWIFT Customer Security Controls Framework
8 Principles



SWIFT Customer 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

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.

What is the purpose of the customer security attestation process?

It is all about driving real-world improvement and fostering transparency among SWIFT users on cyber security

What is SWIFT asking its customers to do?

All SWIFT users must self-attest their level of compliance with the mandatory security controls before end of December 2017

www.swift.com