



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

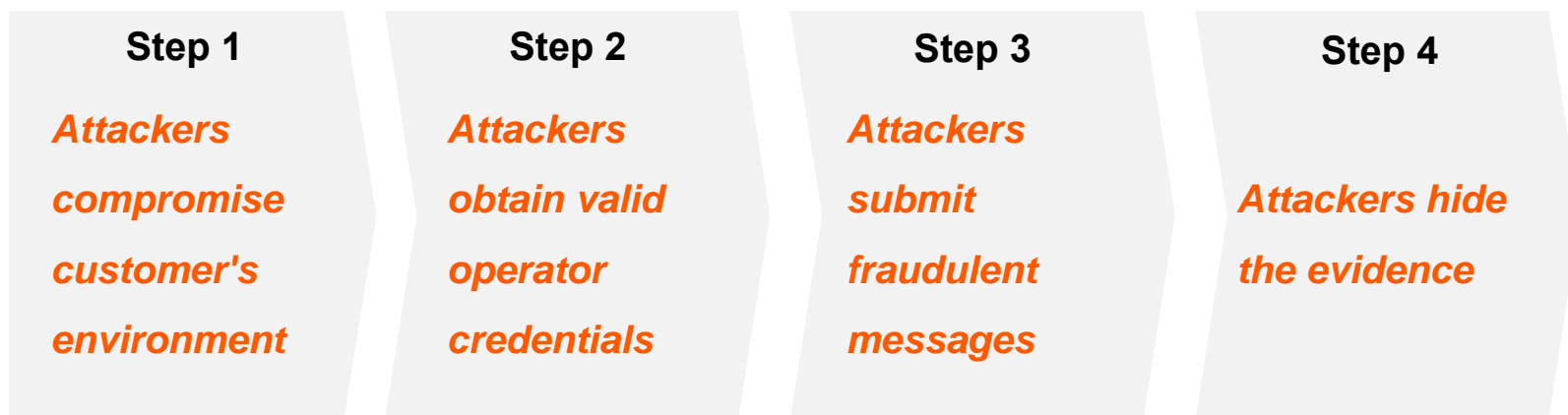




Customer Security Programme (CSP)



CSP Update | Modus Operandi



- 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



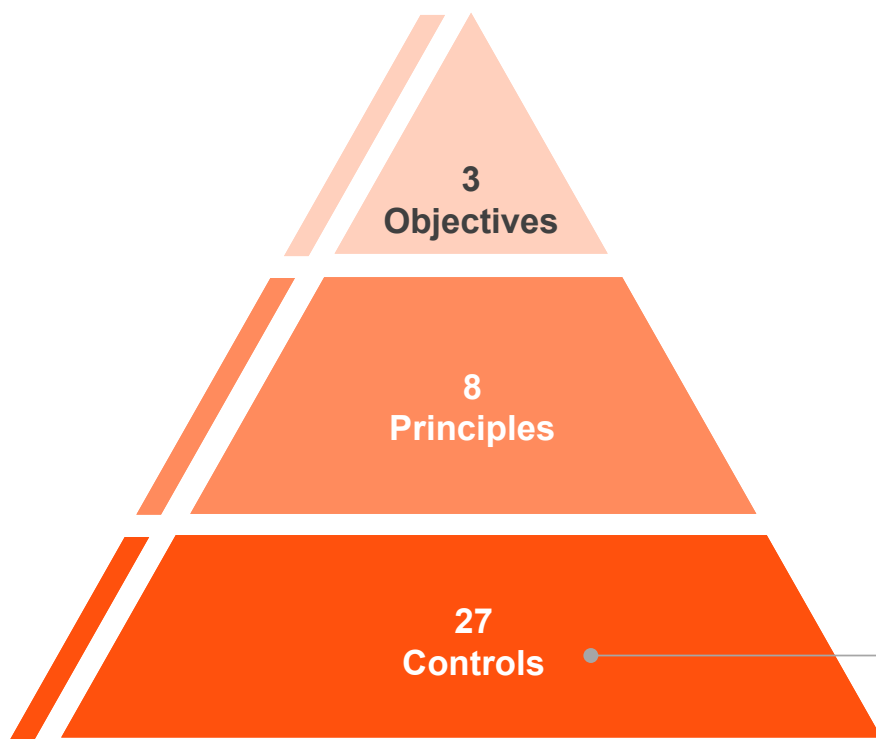
Launched on May 27th 2016, CSP supports all customer segments, whether directly or indirectly connected, in reinforcing the security of their SWIFT-related infrastructure





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*





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

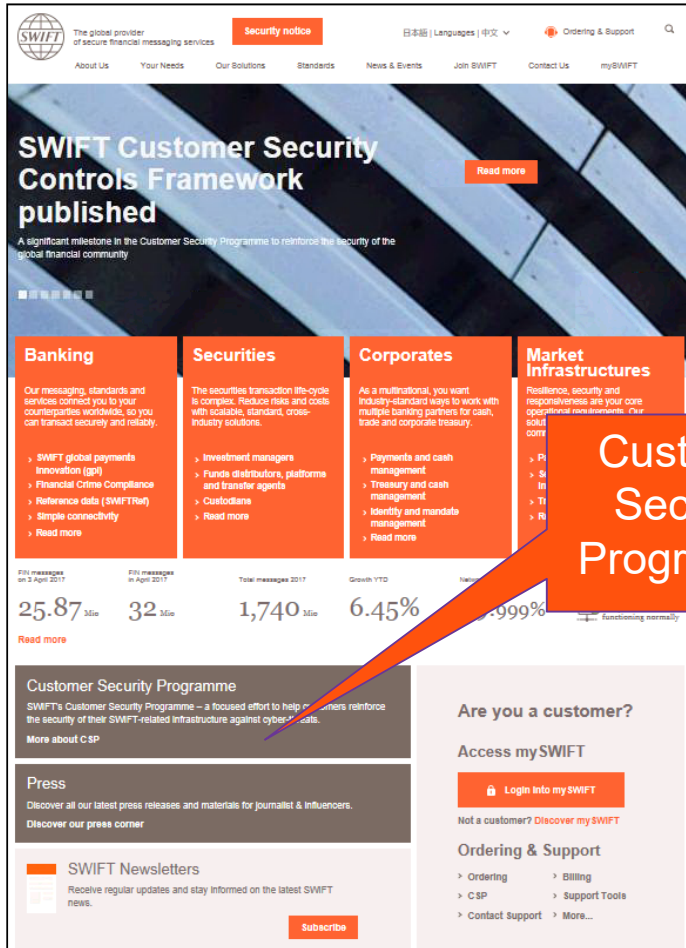
1. Submission of self-attestation

2. Grant access to counterparties

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

4. On-going quality checks





The screenshot shows the SWIFT homepage with a navigation bar at the top. The main headline reads "SWIFT Customer Security Controls Framework published" with a "Read more" button. Below this, there are four columns representing different market segments: Banking, Securities, Corporates, and Market Infrastructures. Each column contains a brief description and a list of services. A large orange arrow points from the "Customer Security Programme" text to the right. At the bottom, there are statistics for message volume and growth, a "Customer Security Programme" section, a "Press" section, and a "SWIFT Newsletters" subscription form.

Customer Security Programme




The screenshot shows the dedicated page for the Customer Security Programme (CSP). The main headline is "Customer Security Programme (CSP)" with a "Subscribe to security notifications" button. Below the headline, there is a navigation menu with options like Overview, Programme description, Security announcements, Security controls, Work sessions & support, Document centre, and Contact us. The main content area features a section titled "Safeguarding security across the banking community" with a video player and a "Reinforce the security of the global financial system" message. Below this, there are three columns: "Information Sharing", "Enhancing SWIFT-related tools", and "Guidelines and assurance frameworks", each with a "Read more" button.





The global provider of secure financial messaging services

Security notice

日本語 | Languages | 中文

Order

About Us Your Needs Our Solutions Standards News & Events Join SWIFT Contact Us

Home > mySWIFT > Customer Security Programme (CSP)

Customer Security Programme (CSP)

Reinforcing the security of the global banking system

Programme description > Contact us >

Overview Programme description Security announcements **Security controls** Work sessions & support

SWIFT Customer Security Controls Framework

SWIFT issues the SWIFT Customer Security Controls Framework for the community

The SWIFT Customer Security Controls Framework describes a set of mandatory and advisory security controls for SWIFT customers.

Mandatory security controls establish a security baseline for the entire community, and must be implemented by all users on their local SWIFT infrastructure. SWIFT has chosen to prioritise these mandatory controls to set a realistic goal for near-term, tangible security gain and risk reduction. Advisory controls are based on good practice that SWIFT recommends users to implement. Over time, mandatory controls may change due to the evolving threat landscape, and some advisory controls may become mandatory.

All controls are articulated around three overarching objectives: 'Secure your Environment', 'Know and Limit Access', and 'Detect and Respond'. The controls have been developed based on SWIFT's analysis of cyber threat intelligence and in conjunction with industry experts and user feedback. The control definitions are also intended to be in line with existing information security industry standards.

To ensure adoption, SWIFT will require customers to provide self-attestation against the mandatory controls by the end of 2017 and on an annual basis thereafter.

Customers may make their compliance status available to their counterparties (via a security attestation folder in the KYC Registry), providing transparency and allowing other users on the network to apply risk-based decision making regarding their counterparty relationships.

The SWIFT Customer Security Controls Framework Detailed Description is available on swift.com. Customers must log in to mySWIFT with their swift.com credentials to access the document. (swift.com > Ordering & Support > User Handbook home > A-Z > Customer Security Programme).

A SWIFTSmart training module is now available on the SWIFT Customer Security Controls Framework.

Security Controls

3 Objectives

2 Principles

20 Controls

SWIFT Customer Security Controls Framework

1. **Secure your Environment**
2. **Know and Limit Access**
3. **Detect and Respond**

The global provider of secure financial messaging services

Security notice

日本語 | Languages | 中文

Order

About Us Your Needs Our Solutions Standards News & Events Join SWIFT Contact Us

Home > mySWIFT > Customer Security Programme (CSP)

Customer Security Programme (CSP)

Reinforcing the security of the global banking system

Programme description > Contact us >

Overview Programme description Security announcements **Security controls** **Work sessions & support**

Customer Security Work Sessions

Community engagement

Customer Security Work Sessions worldwide will commence April 2017 and will run through to December 2017.

The Customer Security Work Sessions provide an opportunity to:

- Learn about the general threat landscape and why protecting your SWIFT-related infrastructure is of utmost importance.
- Understand SWIFT's Customer Security Programme in-depth and how it can help.
- Walk through the steps your organisation will need to take in order to meet SWIFT's Customer Security Control Framework and submit a self-attestation.
- Engage with and ask questions to SWIFT experts regarding the technical aspects of the SWIFT Customer Security Controls and how they apply to your way of connecting to SWIFT.

These events will also serve as an opportunity to discover Cyber Security Service Providers that can provide you with support to assess, remediate and provide assurance against the security controls.

SWIFT will also provide the community with direction on how and where to access further updates including self-service tools such as the mySWIFT knowledge base, SWIFTSmart for training, the CSP pages on swift.com and direct channels into local experts.

As the Customer Security Work Sessions are rolled out worldwide, SWIFT will collect feedback, providing further updates to Frequently Asked Questions that can be shared back with the community.

Upcoming information on regional planning for Customer Security Work Sessions will be made available in the coming weeks.

For any questions please contact your SWIFT Account Manager or your SWIFT Country Manager.

Cyber Security Service Providers

For those customers that may require support from third party Cyber Security Service Providers, SWIFT will publish a Directory of Cyber Security Service Providers in the second quarter of 2017.

Explore our training materials

Title	Description	Access
SWIFT Smart: SWIFT Customer Security Controls Framework	Follow this course to understand how to be compliant with SWIFT mandatory and advisory security controls, to reinforce the security of the local SWIFT infrastructure of your organisation.	SWIFT login required

[Follow course](#)

The global provider of secure financial messaging services

Security notice

日本語 | Languages | 中文

Ordering & Support

About Us Your Needs Our Solutions Standards News & Events Join SWIFT Contact Us my SWIFT

Home > mySWIFT > Customer Security Programme (CSP)

Customer Security Programme (CSP)

Reinforcing the security of the global banking system

Programme description > Contact us >

Overview Programme description Security announcements **Security controls** **Work sessions & support** **Document centre** Contact us

[Subscribe to security notifications](#)

Customer Security Programme document centre

On this page you will find all the documents available on this topic.

10 resources found. Order by: A-Z Most recent

All categories

- Collateral
- Multimedia
- Technical Information
- Compliance Info Papers

- SWIFT Customer Security Controls Framework - FAQ**
Download
Last update: 3 April 2017
Frequently asked questions about SWIFT Customer Security Controls Framework
- Daily Validation Reports factsheet**
Download
Last update: 28 March 2017
A simple, secure way to validate SWIFT transaction activity and understand your payment risks
- Mitigating fraud risk through strengthened payment operations**
Download
Last update: 19 December 2016
New info paper explains how to protect your institution and your community
- Lunch with Sibos - Javier Pérez-Tasso (Video)**
Download • Play
Last update: 10 November 2016
Lunch with Sibos - Javier Pérez-Tasso, Chief Executive, Americas & UK Region, SWIFT
- Customer Security Programme – Sibos Presentation (Video)**
Download • Play
Last update: 10 November 2016
Sibos presentation
- Customer Security Programme - Sibos Presentation**
Download
Last update: 28 October 2016
Presentation from the SWIFT Auditorium session on Customer Security Programme at Sibos.





Feedback,
questions and
open discussion



www.swift.com