Customer Security Program - supporting the community in strengthening security

September 12, 2017

Juan Martinez, Head of Latin America and Caribbean region - SWIFT
The global provider of secure financial messaging services
SWIFT in figures

30.4 million
FIN messages peak day (2016)

6.5+ billion
FIN messages per year (2016)

6.5%
Increase in FIN traffic (2016)

11,000+
SWIFT users

200+
Countries and territories
Industry Change & Challenges
The traditional model is undergoing rapid change, driven by innovation, cyber security and regulation.
SWIFT is leading 3 initiatives, that combined take correspondent banking to the next level

- CSP (Customer Security Programme)
- gpi (global payments innovation)
- FCC (Financial Crime Compliance)
Customer Security Programme (CSP)
Step 1
Attackers compromise customer's environment

Step 2
Attackers obtain valid operator credentials

Step 3
Attackers submit fraudulent messages

Step 4
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
Launched on May 27th 2016, CSP supports all customer segments, whether directly or indirectly connected, in reinforcing the security of their SWIFT-related infrastructure.
Security Controls

3 Objectives

8 Principles

27 Controls

CSP Security Controls Framework

1. Restrict Internet access
2. Segregate critical systems from general IT environment
3. Reduce attack surface and vulnerabilities
4. Physically secure the environment

5. Prevent compromise of credentials
6. Manage identities and segregate privileges

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
Scope of the Controls

In scope

Out of scope

User Environment

Local SWIFT Infrastructure

Connection to the SWIFT network

Data exchange

Operator (End User/Admin)
Scope of the Controls

Data exchange layer
- The flow of data between the back office (or middleware layer) and the local SWIFT infrastructure.

Local SWIFT infrastructure
- SWIFT-specific components managed or owned by your organisation, including applications, network components, tokens and other removable media, and supporting hardware.

Operators
- Operators are individual end users and administrators who directly interact with the local SWIFT infrastructure.

The end user or administrative computing device (typically a desktop or laptop) used to operate or maintain the local SWIFT infrastructure. If you have implemented a jump server, this is in scope of the controls.
The SWIFT Customer Security Controls Framework document

| Type A |
|---|---|
| Control Number and Title |
| 1.2 Operating System Privileged Account Control |
| Control Type |
| Mandatory |
| Control Objective |
| Restrict and control the allocation and usage of administrator-level operating system accounts. |
| In Scope Components |
| - Messaging interface |
| - Communication interface |
| - … |
| Risk Drivers |
| - Unauthorised administrative access |
| - Password compromise |
| - Deletion of activity evidence (e.g., logs) |
| Implementation Guidance |
| <Guidance details> |

To comply with a relevant control you need to:
- meet the control objective
- address the defined risk drivers
- cover the specified scope
The SWIFT Customer Security Controls Framework document

In this example, “1.” stands for principle number one: Restrict Internet access and protect critical systems from general IT environment. “2” stands for the control number two of this principle. If the control is not mandatory it will add the letter “A” (Advisory). For example 6.5A (principle 6, control 5, advisory).

The components in scope for this particular control (for example: Messaging interface, Communication interface, data exchange layer).

You must implement a solution that meets the control objective. This is the SWIFT-formulated method for control implementation.

Control Number and Title
1.2 Operating System Privileged Account Control

Control Type
Mandatory

Control Objective
Restrict and control the allocation and usage of admin accounts.

In Scope Components
- Messaging interface
- Communication interface
- …

Risk Drivers
- Unauthorised administrative access
- Password compromise
- Deletion of activity evidence (e.g., logs)

Implementation Guidance
<Guidance details>

Check here if the control applies to your organisation’s architecture type.

This section says if the control is mandatory or advisory.

This is the security goal to be achieved irrespective of the implementation method. You can implement the solution that best fits your environment, as long as it complies with the defined control objective.

The risks this control aims to mitigate. This helps you to evaluate the solutions you will apply. Some risk drivers are the same for multiple controls.
# Security Guidelines and Assurance Controls

## Mandatory and Advisory Security Controls

<table>
<thead>
<tr>
<th>Mandatory and Advisory Security Controls</th>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 Restrict Internet Access and Protect Critical Systems from General IT Environment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1 SWIFT Environment Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 Operating System Privileged Account Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2 Reduce Attack Surface and Vulnerabilities</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1 Internal Data Flow Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2 Security Updates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3 System Hardening</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4A Back-office Data Flow Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5A External Transmission Data Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.6A Operator Session Confidentiality and Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.7A Vulnerability Scanning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.8A Critical Activity Outsourcing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.9A Transaction Business Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3 Physically Secure the Environment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1 Physical Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>4 Prevent Compromise of Credentials</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1 Password Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.2 Multi-factor Authentication</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Mandatory and Advisory Security Controls (continued)

<table>
<thead>
<tr>
<th>Mandatory and Advisory Security Controls</th>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5 Manage Identities and Segregate Privileges</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 Logical Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.2 Token Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.3A Personnel Vetting Process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.4A Physical and Logical Password Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>6 Detect Anomalous Activity to Systems or Transaction Records</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1 Malware Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2 Software Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3 Database Integrity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4 Logging and Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5A Intrusion Detection</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>7 Plan for Incident Response and Information Sharing</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.1 Cyber Incident Response Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.2 Security Training and Awareness</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.3A Penetration Testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.4A Scenario Risk Assessment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Guidance on the Customer Security Controls Framework

**SWIFT Support**
SWIFT guidance on the customer security controls framework

**Customer security work session**
Hundreds of work sessions held in local communities and via Webinars to share CSP milestones and deliverables

**CSP pages**
Visit the CSP pages for programme news and updates

**The SWIFT Customer Security Controls Framework and Security Controls Policy Document**
Customers must log in to mySWIFT with their swift.com credentials to access the documents.

**SWIFTSmart**
The SWIFTSmart e-learning training platform includes a portfolio of modules, including in-depth modules on each of the mandatory security controls

**MySWIFT**
MySWIFT A self-service portal containing “how-to’ videos, guidance on frequently asked questions and Knowledge Base tips.
If customers need assessment or implementation support, they can consult the directory of cyber-security service providers on SWIFT.com to help find a suitable third-party project partner.

- The Directory of Cyber Security Providers is for SWIFT customers’ reference only.
- SWIFT does not endorse or warrant the providers (or their services) listed in the Directory.
- SWIFT users can opt to contract with other providers that are not featured in the Directory.
- **SWIFT users must always conduct their own analysis of the suitability of a Cyber Security Service Provider for their purposes.**

Available on SWIFT.com/CSP
CSP | You > Security Guidelines and Assurance

Attestation

Builds on the principles of fostering transparency between users and ensuring customers remain in control.

- Central tool to submit self-attestation status information
- Attesting user remains in control of publication of its data to counterparties
- Any other user must request access to the attesting user to view its data

The KYC Registry

A central tool
- To share compliance results with counterparties, as deemed appropriate.
- Creates transparency and allows risk management and business decision-making

Open for data submission and consumption from July 2017
- You will need to renew or reconfirm your self attestation on at least an annual basis
CSP | You > Security Guidelines and Assurance

Attestation

- Submission of self-attestation
- Grant access to counterparties
- View your counterparties’ compliance status
- Follow-up activities to drive compliance and improve security
CSP | You > Security Guidelines and Assurance
Attestation Content

Submitter and approver info

Evaluation method (self-assessment, internal audit, external audit)

Type of infrastructure (including hub owner or service bureau if applicable)

Contact information

For each control:

- I comply
  - in line with guidance
  - with alternative implementation

- I will comply
  - with qualification date field

- I do not comply

Any mandatory control with a missing response will default to “Do not comply”

Advisory controls may be left with a blank response
CSP | You > Security Guidelines and Assurance
Timeline Summary

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>22nd May, 2017: Publication of SWIFT Customer Security Controls Policy</td>
</tr>
<tr>
<td></td>
<td>July 2017, KYC Registry Security Attestation application available for data submission and consumption</td>
</tr>
<tr>
<td></td>
<td>As of end December 2017, all users must have submitted their self-attestation</td>
</tr>
<tr>
<td></td>
<td>As of Jan, 2018: SWIFT reserves the right to report users that have not submitted a self-attestation</td>
</tr>
<tr>
<td></td>
<td>As of Jan, 2019: SWIFT reserves the right to report non-attested users and non-compliance</td>
</tr>
</tbody>
</table>

---

- **CSCF Published**: CSCF Published
- **KYCR-SA Live**: KYCR-SA Live
- **Window for submitting initial self-attestation**
- **Annual renewal of attestation**
- **Reporting of non-attestation**
- **Reporting of non-compliance**
CSP | Programme
Beyond Securing and Protecting

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, DVR and Pattern Controls
RMA and RMA plus

Poor management of RMAs creates potential security risks.

Wolfsberg principles suggest that risks of RMA should be assessed. Approvals should be controlled and segregated between customer relationships and non-customers, with distinct due diligence criteria for each. Due diligence should consider the scope of message types used.

Unilateral RMA revocation is now easy and is confirmed within 15 minutes.

“RMA and RMA Plus: managing your correspondent connections” info-paper provides details on best practice.
**Daily Validation Reports**

**Activity Reporting** – reports aggregate daily activity by message type, currency, country and counterparties with daily volume and value totals, maximum value of single transactions and comparisons to daily volume and value averages.

**Risk Reporting** - highlights large or unusual message flows based on ordered lists for largest single transactions and largest aggregate transactions for counterparties, and a report on new combinations of counterparties to identify new relationships.

**New Counterparties Reporting** - highlights any new combinations of direct and indirect counterparties. Makes it easy to identify new payment relationships that may be indicative of risk, and helps you quickly understand the values and volumes of the transactions involved.
Payment Controls

SWIFT is developing Payment Controls for subscribing organisations, performing ‘in-flight’ transaction monitoring to identify payment activity that is out-of-policy or indicative of fraud risks.

Payments Controls provide an additional safeguard on top of users’ existing fraud prevention systems.

Focus on Smaller Institutions
Initially for smaller, sending organisations. Will also help protect larger organisations through reduced risks of received payments.

Secure In-Network
Using sanctions screening model to alert/release/abort payment messages in real-time. Monitoring policy defined by the subscriber.
Feedback, questions and open discussion