Three years on from Bangladesh: tackling the adversaries

Justin Coley – AM-UK Account Management

June 2019
Agenda

› Threat Evolution
› Customer Security Programme
› Controls and Framework Evolution
› CSCF v2019
› Priorities for 2019
› Counterparty Consultation of Attestation
› Risk Management & Detection Tools
› ISAC White Paper ‘Three Years Since Bangladesh
› Community Engagement
The Big Picture for the World Economic Forum

1 National governance failure
2 Unemployment
3 Social instability

1. Infectious diseases
2. Critical info infrastructure
3. Fiscal crisis
4. Regional governance failure
5. Critical infrastructure
6. Energy price shock
7. Financial institution failure
8. Adverse technology
9. Urban planning failure
10. Illicit trade

1. Weapons of mass destruction
2. Extreme weather
3. Natural disasters
4. Cyberattacks
5. Climate change
6. Water crisis
7. Biodiversity collapse
8. Interstate conflict
9. Terrorist attacks
10. Large scale migration
11. Environmental disasters
12. Asset bubbles
13. Data fraud or theft

14. Deflation
15. Unmanagable inflation

Source: 2018 WEF survey spanning 684 respondents which assessed [likelihood] and [impact] of each risk on a scale of 1 to 5 [very unlikely / minimal impact] to [very likely / catastrophic]
Cyber attacks are evolving

- Intense DDoS Attacks
- Rise in Ransomware
- Evolving Zero-Day (APTs) Advanced Persistent Threats
- Advanced Undetectable Malware
- Larger Data Breaches
- Targeting of Critical Infrastructure

Ab(use) of New Technology

- 'Arms-Race' as New Technologies Mature – Artificial Intelligence and Machine Learning
- Concentration Risk from a few Dominate Vendors
- Industry Reliance on the Cloud

Evolving Attack Vectors

- Endless (Spear) Phishing
- Rise in Insider Threats
- Race to Close the Gaps
- Deep Skills Shortage

The Weakest Link

- Wide Reaching Impact of New Regulation – e.g. GDPR and NIS Directive - Fines for PII Breaches

New Regulation
Modus Operandi

• Attackers are well-organised and sophisticated
• There is no evidence that SWIFT’s network, core messaging services or OPCs have been compromised
• All IOC details are published on the SWIFT ISAC portal

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

• Malware injected by e-mail phishing, USB device, rogue URL or insider

• Long reconnaissance period monitoring banks’ back office processes

• Keylogging / screenshot malware looking for valid account ID and password credentials

• Attacker impersonates the operator / approver and submits fraudulent payment instructions

• May happen outside the normal bank working hours / over public holiday

Gain time by:
• Deleting or manipulating records / log used in reconciliation
• Wiping Master Boot Record
SWIFT

Global provider of secure financial messaging services

Industry owned, financial services cooperative, that does not seek to maximise profit

Connecting 12,000+ institutions
200+ Countries and territories
7+ billion FIN messages in 2017
Proven network 99.999% FIN availability
Strong PKI security encryption
ISO 20022 Unique role developing standards
Customer Security Programme
2018 Highlights

94% Attestation, 99% Traffic

Compliance Re-Attestation Consultation

Your Community
- SWIFT–ISAC: STIX/TAXII
- Directory of Cyber Security Providers
- Industry engagement

Your Counterparts
- Security Attestation Application v3 – Consult
- Quality Assurance framework.
- Payment Controls Service

You
- Change Management process
- Customer Security Controls Framework (CSCF)
- Release of CSCF v2019
- Updated Customer Security Attestation Policy
- Interface Hardening – Release 7.3

Customer Security Programme
CSP | Secure and Protect – Customer Security Controls Framework v2019

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

- 19 controls are now mandatory – 3 Advisory promoted to Mandatory:
  - 2.6 M Secure Operator sessions
  - 2.7 M Yearly vulnerability scanning
  - 5.4 M Physical and Logical Password Storage
- 10 controls are now advisory - 2 additions:
  - 1.3 A Virtualisation Platform Protection
  - 2.10 A Application Hardening
CSP update | Secure and Protect - CSCF v2019 timeline and next…

Version V2 (v2019) of Security Controls

- SWIFT writes v2019 controls
- Customers budget v2019
- Customers implement v2019 controls
- v2019 attest window opens
- Cust attest against v2019
- v2019 attest window closes
- v2019 Reg Reporting

Version V3 (v2020) of Security Controls

- SWIFT writes v2020 controls
- Customers budget v2020
- Customers implement v2020 controls
- v2020 attest window opens
- Cust attest against v2020
- v2020 attest window closes
- v2020 Reg Reporting

Latest date for customer to self-attest full compliance against v2019 mandatory controls

Latest date for customer to self-attest full compliance against v2020 mandatory controls
Customer Security Controls Framework (CSCF):
• CSCF v2019 was published in Aug 18 where 3 advisory controls were ‘promoted’ to mandatory and 2 new advisory controls were added
• SWIFT will continue to ‘raise the bar’ and community consultation started in Q4 2018 for version v2020 and will continue in Q1 2019. Publication by mid-2019. Consultation will continue into Q2
• Refine CSCP Policy and publish mid-2019

Re-attestation and Compliance:
• Re-attestation / compliance status for CSCF v1 will continue to be monitored through Q1/Q2 2019, after which CSCF v2019 comes into effect. v2019 compliance deadline is end Dec 2019
• User experience enhancements to KYC-SA for re-attestation

Supervisory Reporting:
• Starting 2019, SWIFT will inform supervisors of users who do not re-attest, do not comply with all mandatory controls or connect via a non-compliant service provider. Reporting is limited to the name of the customer. It does not include the underlying control details. Any additional information is communicated bilaterally between the user and their supervisor
• In Q1 2019, supervisors can start to access non-compliance / non-attestation reports in KYC-SA

SWIFT Interface Enhancements:
• Release 7.4 is expected to be released in mid 2019. Building on R7.3 (Multi-Factor Authentication (MFA) options), R7.4 is expected to include enhanced encryption
Counterparty Risk Consultation:
• During 2019, SWIFT will undertake outreach communications on the consultation of counterparty attestations for cyber risk management, e.g. bulk access request, auto-grant and missing roles and long pending requests
• In Q1 2019, SWIFT will actively promote the ‘getting started’ guide
• Enhancements to KYC-SA for access requests - intermediate status, 4 eyes principle, bilateral granting

Anti-Fraud Tools:
• During 2019, SWIFT will promote Payment Control Service (PCS). PCS performs ‘in-flight’ transaction monitoring on ‘sent’ payment instructions and identifies activity that is out-of-policy or indicative of fraud risks. PCS either alerts or stops a fraudulent payment message in real-time using policy rules defined by the subscriber
• Throughout 2019, aside from enhancing PCS, SWIFT will monitor the adoption of fraud prevention tools by customers and will evaluate the need to extend or change its fraud offerings as required to encourage widespread adoption of fraud prevention tools
Community Engagement:
• In Q1 2019, SWIFT will promote community adoption of SWIFT ISAC / Notifications / STIX TAXII
• Throughout 2019, SWIFT will continue to engage with the community through numerous channels, e.g. direct customer meetings / webinars; liaising with cybersecurity intelligence agencies; speaking at SWIFT Business Forums; hosting CISO Roundtables; publishing quarterly newsletters; speaking at external conferences or industry association meetings and hosting sessions at Sibos
• Throughout 2019, SWIFT will (co)-author a number of cyber thought leadership White Papers, e.g. legal barriers to information sharing

Quality Assurance
• Throughout 2019, SWIFT will continue to monitor the effectiveness and quality of the CSCF controls framework through the CSP Quality Assurance (QA) programme, by reviewing unexpectedly high or low levels of compliance across the community
• In Q1 2019, SWIFT will continue to request additional evidence to substantiate the self-attestation, including audits / assessments from a select number of customers. To support, the Directory of Cyber Security Providers and Assessors will be updated
• In Q1 2019, SWIFT will share the Independent Assessment framework
CSP | Counterparty Consultation of Attestation
Users should consult counterparty attestation data and integrate this into their risk management and business decision-making processes

Using the KYC-SA, customers can share their attestation data with their counterparties and request data from others.

Customers remain in control of their attestation data – they can grant or deny requests of their attestation data.
Many customers have not (yet) established requester / granter roles in KYC-SA. A small portion of customers are Attestation Request (AR) 'senders', but most are now AR 'receivers'.
From this small portion of requesters, ARs sent have increased by 31% … however the vast majority of ARs have been sent by a very small number of customers.
Guideline is primarily intended for use by small and medium sized organisations with relatively few counterparties, and correspondent banks that act as intermediaries between originating payers and end beneficiaries.
CSP | Cyber Risk Management and Detection Tools – DVR and PCS
In the event of an attack the accuracy of data in interface systems may be compromised. DVR allows independent reconciliation

**Validate Activity**
- Validate aggregated daily activity and transactions (reference and value) for a Group or a BIC8 across the payment chain
- Daily volume and value totals, maximum value of single transactions and comparisons to 24 months historical profile

**Assess Risks**
- Assess large or unusual message flows based on different risk factors (largest transactions, largest aggregates, or deviation with average activity).
- Identifies new combinations of parties in payment chain
- Highlights transactions sent outside of business hours

**Review Behaviours**
- Ensure alignment to Compliance policy

**If invoked, DVR would have identified the vast majority (if not all) fraudulent messages across all customer incident cases to date**
CSP Detection Tools | Payment Control Service (PCS) - Features and Rules

- PCS performs ‘in-flight’ transaction monitoring on ‘sent’ payment instructions and identifies activity that is out-of-policy or indicative of fraud.
- PCS works in one of two real-time operating modes using policy rules defined by the subscriber:
  1. Message Copy and Alert, or
  2. Message Hold and Alert
- Provides a zero-footprint payment safety-net against payment risks
- SWIFT launched PCS in Oct 18 supporting MT103, MT202 and MT202 COV messages

PCS Policy Rules

- **Business Calendars**, non-business days and normal business hours
- **Currency** whitelist / blacklists, single and aggregate payment limits
- **Country** whitelist / blacklists, single and aggregate payment limits
- **Thresholds** for country, currency, single entity or group combinations
- **New Institutions**: Identify payments with new participants or chains, based upon historical message flows
- **Profiling / Learning**: Identify & protect against payment behaviour that is uncharacteristic, based upon past learned behaviour
- **Badly Formed Messages**: Identify and stop messages where preceded by repetitive NAKs to the same recipient
- **Suspicious Accounts**: Verify end customer account numbers against an institution black list of account numbers believed to be high risk
ISAC: the portal for cyber-security information.

This portal shares information related to security threats potentially impacting our customers. All information is "as is" and while SWIFT makes good faith efforts to review all content, we will not be responsible for the accuracy or completeness of information. Use of this portal is subject to the terms of use. For more information, please see the online help.

Type Keyword, Title, Tracking ID

Search

50k
Total number accesses

5800
# unique users

3300
# unique BICs

200
# unique countries
How are Cyber Security attacks evolving? → What does the data show?
Quiz Question – Up until 2 years ago, what was the most common transaction amount used in reported attacks?

A. Under 250k USD
B. Between 250k USD – 2m USD
C. Between 2m – 10m USD
D. Greater than 10m USD
Quiz Question – Up until 2 years ago, what was the most common transaction amount used in reported attacks?

A. Under 250k USD
B. Between 250k USD – 2m USD
C. Between 2m – 10m USD
D. Greater than 10m USD – Answer
Quiz Question – Today, what was the most common transaction amount used in reported attacks?

A. Under 250k USD
B. Between 250k USD – 2m USD
C. Between 2m – 10m USD
D. Greater than 10m USD
Quiz Question – Today, what was the most common transaction amount used in reported attacks?

A. Under 250k USD
B. **Between 250k USD – 2m USD – Answer**
C. Between 2m – 10m USD
D. Greater than 10m USD
Quiz Question – What is the most common currency used in fraud incidents that have been reported?

A. Philippine Piso (PHP)
B. Hong Kong Dollar (HKD)
C. US Dollar (USD)
D. Thai Baht (THD)
Quiz Question – What is the most common currency used in fraud incidents that have been reported?

A. Philippine Piso (PHP)
B. Hong Kong Dollar (HKD)
C. US Dollar (USD) – Answer
D. Thai Baht (THD)
Quiz Question – Where are the fraudulent payments being sent to? (ie where is the beneficiary account)

A. Middle East  
B. Asia Pacific (APAC)  
C. Europe  
D. Latin America
**Quiz Question** – Where are the fraudulent payments being sent to? (ie where is the beneficiary account)

A. Middle East  
B. **Asia Pacific (APAC) – Answer**  
C. Europe  
D. Latin America

The below graph illustrates the regional location of Beneficiary accounts used in fraudulent transactions since July 2018.
CSP | Supporting the Community
Where can I go if I need help?

CSP pages
Visit the CSP pages for programme news and updates

mySWIFT
A self-service portal containing “how-to” videos, guidance on frequently asked questions and Knowledge Base tips.

SWIFT ISAC Portal
Consult the portal for information related to security threats

User Handbook
- SWIFT Customer Security Controls Policy
- SWIFT Customer Security Controls Framework
- KYC-SA Registry Baseline
- KYC-SA Registry User Guide
- Counterparty Cyber Risk Management

Knowledge Base
KYC-SA Quick-Start User Guide: Tip 5021858
How-to video’s:
- Tip 5021825: KYC-SA Role Families
- Tip 5021826: KYC-SA Administration
- Tip 5021827: KYC-SA Data Contribution
- Tip 5021828: KYC-SA Data Consumption
- Tip 5021823: CSP Frequently asked questions
SWIFTSmart
The SWIFTSmart e-learning training platform includes a portfolio of modules, including in-depth modules on each of the mandatory security controls.

SWIFT Customer Support
SWIFT Customer Support teams are on hand 24/7 to answer specific queries if you don’t find the information resources you are looking for.

Directory of Cyber Security Service Providers
If you need practical, on-the-ground implementation support, you can consult the Directory of Cyber Security Service Providers on SWIFT.com to help find a third-party project partner that may be suitable for your needs.

SWIFT Services
To support best practices in infrastructure implementation and management SWIFT offers services such as the SWIFT infrastructure security review, Security bootcamps, SWIFT Admin. and Operation certifications, and recurring support contracts such as Alliance Managed Operations, Local support and Premium custom support.
Call to action for SWIFT customers

1. Stay up to date with SWIFT software releases

2. Sign up for Security Notifications and use of the SWIFT ISAC information sharing portal, which includes STIX/TAXII feeds

3. Undertake bilateral agreements with your counterparties to consume and utilise attestation data for counterparty risk management

4. Consider SWIFT’s anti-fraud tools (Payment Controls, Daily Validation Reports, RMA clean-ups, etc.)

5. Always inform SWIFT immediately if you suspect a cyber-attack on your SWIFT-related infrastructure

6. Ensure that you fully comply with all the mandatory security controls and attest by end December 2019
Questions?