Customer Security Programme Newsletter

Reinforcing the security of the global banking system

March 2019

Welcome to the fifth edition of our quarterly newsletter – designed to provide you with the important information you need to know about SWIFT's Customer Security Programme (CSP).

2018 attestation status results

SWIFT's Customer Security Controls Framework (CSCF) goes from strength to strength as the financial industry continues to work together to tackle the ongoing threat of cyber-attacks.

The community achieved an impressive result with 94% of all SWIFT customers, representing 99% of SWIFT's traffic, attesting their level of compliance with the mandatory security controls by the 31 December 2018 deadline. This achievement improves on the already strong 89% rate of attestation at the end of the previous year.

Importantly, customers can start to register their self-attestation of compliance against the next version of the CSCF Controls (v2019) using the KYC-SA tool from 1 July 2019. Attestation needs to be completed by the year-end. CSCF v2019 is available in various languages here, and SWIFTSmart training modules are also available.

Counterparty risk management and the 'Getting Started' guide

SWIFT has recently published a new guide to assist financial institutions in assessing levels of cybersecurity risk in their counterparties and incorporate it into their risk management frameworks.

Assessing Cybersecurity Counterparty Risk - A Getting Started Guide, provides a series of practical, but non-binding information and recommendations, including how to establish a governance model, create a cybersecurity risk management framework and how to adopt cybersecurity risk countermeasures.

Though relevant to all financial institutions, the guide 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. This is the latest addition to SWIFT's Customer Security Programme (CSP) to promote best practice in security among SWIFT's thousands of users worldwide.

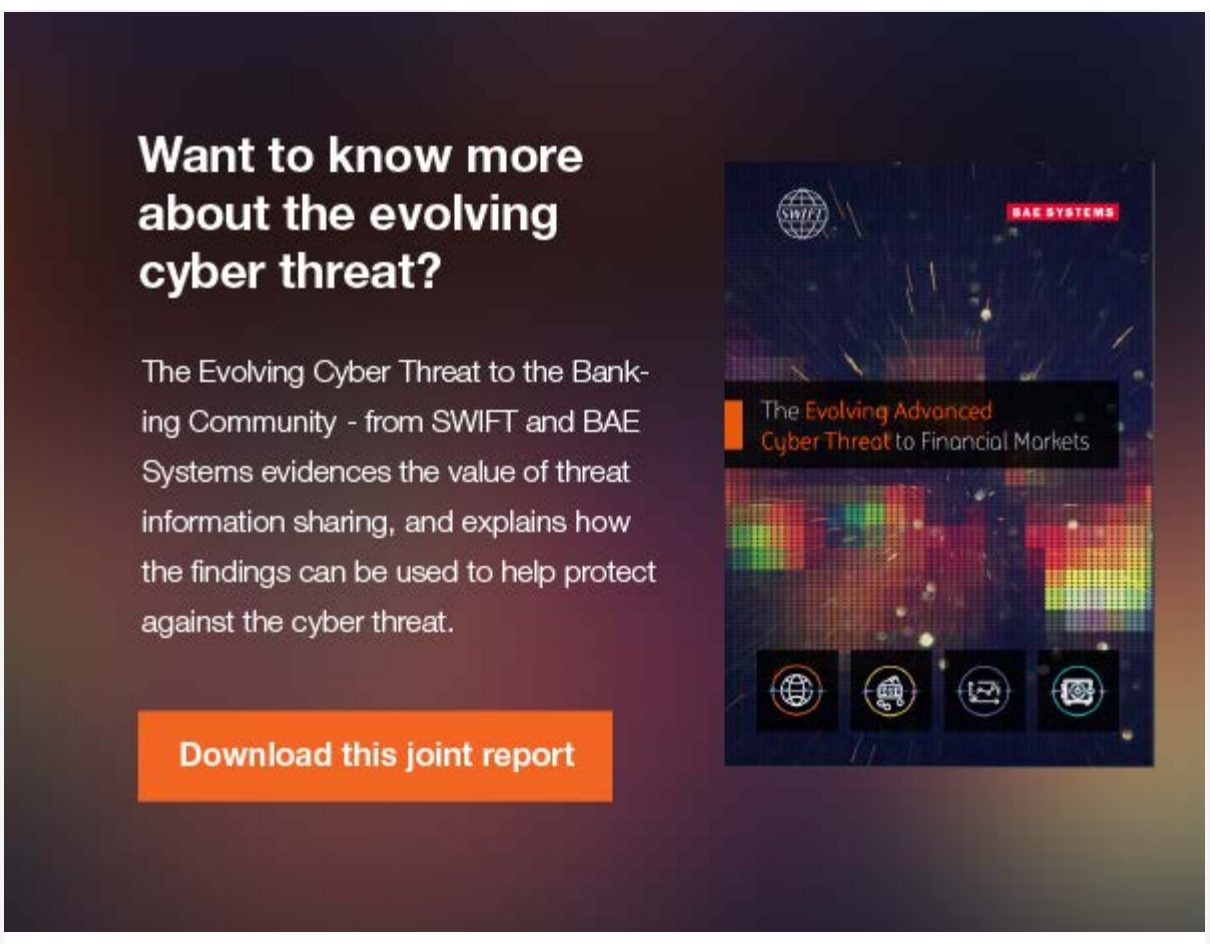
Local language translation versions of the *Getting Started Guide* (French, German, Spanish, Russian, Japanese, Korean, Chinese – both traditional and simplified) will be available by end April 2019.

.pdf Download now ›

Karel De Kneef joins BAE expert to discuss the security challenges

SWIFT's new Chief Security Officer, Karel De Kneef, speaks with Szu Ho, Principal Consultant at BAE Systems, in a podcast to discuss the security challenges in financial markets, his first interview since becoming SWIFT's Chief Security Officer.

In the BAE podcast De Kneef discusses some of the themes raised in a recent joint SWIFT and BAE Systems report, which looks at areas cyber criminals could target next, noting how the highest level threat actors run their operations "like businesses". In the podcast Ho and De Kneef consider the new threats, address the opportunities and risks presented by the use of common standards and discuss the importance of intelligence and information sharing.



Independent Assessment Framework

SWIFT will shortly publish its *Independent Assessment Framework*, which will provide users and assessors with a comprehensive overview of the independent assessment process.

The framework is designed to support SWIFT users and assessors to carry out their responsibilities throughout the CSCF assessment process. In particular, its purpose is to support users in verifying that their self-attestations correspond with their actual level of security control implementation.

The framework covers three assessment types:

1. User-Initiated Assessments

Voluntary in nature and may be executed by a user to support a given self-attestation. These assessments may be undertaken by either internal or external parties. User-Initiated assessments will be replaced by ‘Community Standard Assessments’ for all users from mid-2020.

2. Community Standard Assessments

Starting with new attestations submitted in 2020 under CSCF v2020, all attestations will need to be independently assessed through either:

- *External assessment*, by an independent external organisation which has existing cyber security assessment experience, and individual assessors who have relevant security industry certification(s), or
- *Internal assessment*, by a user’s second or third line of defence function (such as compliance, risk management or internal audit), which is independent from the first line of defence function that submitted the attestation (such as the CISO office). As per external assessors, those undertaking the assessment work should possess recent and relevant experience in the assessment of cyber-related security controls.

3. SWIFT Mandated Assessments

Separate and distinct from the above two categories, SWIFT also reserves the right to seek independent external assurance to verify the veracity of their self-attestation. These ‘SWIFT Mandated Assessments’ began in 2018, with a small sample of users required to conduct independent external assessments.

The framework also includes links to standardised Excel-based assessment templates to be used by assessors in capturing the details and results of assessments.

Community engagement

2019 started off with a number of industry working groups covering overall cyber resilience, endpoint security and a series of CISO Roundtables which will continue throughout the year.

At these events we share best practice, experiences and community-wide knowledge on how best to defend against cyber threats. Please do look out for invitations to upcoming events in your locality.

Stay connected