Customer Security Programme Updates

Reinforcing the security of the global banking system

March 2020

Welcome to the SWIFT Customer Security Programme (CSP) update – designed to provide you with the latest important information and updates relating to the CSP.

SWIFT publishes attestation rate for CSCF v2019

More than 91% of customers, representing over 99% of SWIFT's traffic, have attested to their compliance with controls mandated by SWIFT's Customer Security Controls Framework (CSCF) v2019, a key aspect of the Customer Security Programme (CSP).

The 2019 version was the most stringent to date, with 19 mandatory and 10 advisory controls. It also marked the second year that customers were required to attest to their compliance. For those customers that did not attest, or did not fully comply with all of the mandatory controls, SWIFT reserves the right to report the customer to their local regulator.

Brett Lancaster, Head of CSP at SWIFT, commented: “We would like to thank our community for their hard work in implementing the controls set out in the CSCF v2019. We recognise it’s not easy, but it is vital for our community to continue to stand strong against the growing and evolving cyber threat. We look forward to continuing to work closely together as we further strengthen cyber defences with the implementation of CSCF v2020.”

Planning for CSCF v2020

Looking forward, the CSCF v2020 has a number of changes from v2019 and includes 21 mandatory and 10 advisory controls. Two controls, 1.3 and 2.10, listed as advisory in 2019 have been elevated to mandatory. They aim to protect and reduce potential vulnerabilities on critical interface components as well as critical systems where virtualisation is being used more frequently.

The CSCF v2020 will become effective in the KYC Security Attestation application (KYC-SA), the online repository for customer attestations, in July 2020.

Furthermore, to enhance the overall integrity of attestations across all customers, all submitted attestations for CSCF v2020 must be supported by an **independent assessment** – either **internally**, by a second or third line of defence (e.g. risk, compliance or internal audit), or **externally**, by a third-party. To help support customers, SWIFT will be expanding its Cyber Security Service Providers directory with external CSP assessment providers.

Once again, attesting compliance against the CSCF v2020 will be mandatory by the end of 2020. You can access the CSCF v2020 here. (SWIFT login ID required).

Please note that CSCF v2018 has now expired and CSCF v2019 will expire on 31 December 2020. This means that **if you have attested in 2020 against v2019, you have to re-attest against**

v2020 between July and December 2020 to have a valid attestation by year-end.

Independent Assessment Framework update

We have published a revised version (v2020) of the Independent Assessment Framework (IAF), which supports users and their independent assessors in carrying out their responsibilities as part of the CSP.

The section 1.3 gives an overview of the changes; one of them includes the option for service providers to be submitter of the attestation and/or independent assessment provider for their customers. For details, please refer to section 9 of the IAF v2020.

Changes to KYC-SA

We would also like to make you aware of a number of changes to KYC-SA, the tool designed for users to submit their self-attestation data, which confirms their organisation's level of compliance with SWIFT's customer security controls.

- 'SWIFT payment operations contact' is a new mandatory field introduced in KYC-SA; this contact is used when potential fraud has been identified and a customer needs to be contacted quickly to verify the veracity of payment transactions. It is not shared with counterparties.
- Currently it is possible to put N/A for Controls 5.2, 5.4, 6.1. As from now, if N/A is selected, a clarification must be provided.

SWIFT joins forces with other major EU infrastructures to fight cyber threat

SWIFT, as part of the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) information sharing working group, established by the European Central Bank, was instrumental in the launch of an initiative to share vital cybersecurity threat information across major European infrastructures. It aims to help protect European citizens and financial instutions from cybercriminals.

Brett Lancaster, Head of the Customer Security Programme at SWIFT and Chair of the ECRB intelligence sharing working group, commented: “Research shows that the exchange of relevant and timely cyber threat intelligence has proved critical in effectively detecting and preventing attacks. This is why we set out to create a framework which we will implement that simplifies the process of intelligence sharing by re-using proven components, adding value through disseminating strategic information and allowing each member to implement it at their own pace. This, we hope, will make it easier for those involved to protect consumers as well as the financial industry from cybercriminals.”

“This is the first time that major financial infrastructures, Europol and the European Union Agency for Cybersecurity (ENISA) have jointly taken steps against cyber risk,” said ECB Executive Board member and ECRB Chair, Fabio Panetta. “We hope this will be an inspiring model for other jurisdictions to tackle one of the biggest threats of our time. Cybercriminals are increasingly stealing money, and therefore sharing information will help us to prevent attacks and ultimately protect people’s money.”

In the coming months, the ECB will publish the framework for the CIISI-EU sharing initiative to encourage other jurisdictions to follow suit.

See the full article on our website

SWIFT speaks to Finextra about cybersecurity trends to expect in 2020

Last month, Dries Watteyne, Head of Cyber Fusion Centre at SWIFT, spoke to Finextra about his views on a number of 2020 cybersecurity trends including artificial intelligence, the growing sophistication of cyber attackers and ethical hacking.

When asked about artificial intelligence, Watteyne said he recognised its potential but thinks its widespread adoption is a couple of years down the line. He also said: “I think there’s still a lot to be done around basic security hygiene and companies need to continue to focus on getting this in place first.”

On the growing threat of distributed denial-of-service (DDoS) attacks, Watteyne said: “DDoS attacks are used to obstruct or disrupt an organisation, rather than to fraudulently obtain money, so I don’t think it falls under the umbrella of what cybercriminals are using to target financial institutions in the payments space but that doesn’t mean we can ignore them.”

He also predicts a growth in ethical hacking programmes in 2020: “We see bounty programmes, where of course there’s a reward, but in most cases ethical hackers aren’t driven by financial gain, they want to help others win cyber battles.”

Download 'The Future of Cybersecurity: 2020 Predictions'.

‘Follow the money’ report with BAE

SWIFT and BAE will be publishing the latest in a series of cybersecurity reports on swift.com in the coming weeks, which will unpick the money laundering techniques cyber heists.

The report will share insights into the nature and extent of cyber-attacks on the banking and financial services sector, the size, cost, growth of cybercrime and techniques such as placement, layering and integration.

It will also include the wider implications for the financial industry and what we, as a community, can do to protect ourselves.

Stay connected 

About SWIFT

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging, standards for communicating and we offer products and services to facilitate access and integration; identification, analysis and financial crime compliance. Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way. As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.