SWIFT Customer Security Programme

The cyber-security challenge

Addressing the fast moving cyber threat environment is one of the most significant challenges for any institution involved in sending or receiving payments. Banks are clearly important stakeholders when it comes to cyber security, but CFOs and Corporate Treasurers also need to ensure strong preventive and detective measures to safeguard their treasury management, and to effectively secure their payment flows.

Recently publicised cases of cross-border payment fraud have occurred due to sophisticated attacks targeting banks' local infrastructure. SWIFT has no indication that its own network or core messaging services have been compromised, however breaches in some banks' local infrastructure have led to the theft of legitimate user credentials, providing an entry point for attackers to introduce malware and/or send fraudulent transactions over SWIFT. In some cases, the evidence of such fraud was subsequently hidden through the manipulation of data logs. While corporates have not been directly impacted in cases known to SWIFT, the security of *all* payments environments is an area of heightened concern, requiring vigilance from both banks and corporates alike.

SWIFT's Customer Security Programme

SWIFT has introduced a dedicated Customer Security Programme (CSP) in collaboration with its customers to help its community to address ongoing cyber threats. The programme addresses three key aspects: the security and protection of customers' local environments, their counterparty relationships, and the role the financial community can play by acting together to stay a step ahead of cyber-attacks. Actions on the programme include the introduction of mandatory security controls, new services to prevent and detect fraudulent activity, and community-wide information sharing initiatives to prepare for, and exchange information in order to avoid future attacks.

Measures covered by the programme are applicable to all SWIFT customers, including the 1700 + corporates who use SWIFT for multi-bank connectivity, whether connecting to SWIFT directly via Alliance Lite2 (or Lite1), or indirectly, for example via a Lite2 for business applications provider or via a service bureau.

Your bank relationships

As many corporates on SWIFT are multi-banked, with in excess of 20+ banking relationships worldwide, it is vital that corporates have confidence in the integrity of information exchanged between them and their banking partners. Connecting to SWIFT provides a standardised way of working with multiple banks, and a single channel to manage these relationships which already reduces operational complexity and associated risk. With SWIFT's Customer Security Programme now in place helping banks to reinforce their cyber-security and increasing levels of transparency on their security status, corporates will have even more information available to stay informed and to ensure confidence in those business relationships.

Securing your own local environment

Alongside banks, corporates should also directly take all necessary preventive and detective measures to ensure that their local environments and connectivity workflows are not open to compromise, whether they connect directly via SWIFT or use third party providers. Any opportunity to introduce malware or generate unauthorised payments can be an opening for cyber criminals and potentially lead to compromise and ultimately, fraud.

To reinforce industry-wide action, SWIFT has announced plans to introduce a set of core security standards that *all* customers must meet to strengthen the security of their local environments. Detailed security controls (16 mandatory and 11 advisory) have been published on swift.com together with a draft supplementary guide[1].The SWIFT security framework will apply from April 2017.

The controls cover areas of important basic security hygiene which apply to corporates such as security updates, limited access and privileges to SWIFT-related systems; segregation of duties for sensitive operations and the use of multi-factor authentication to strengthen user authentication. (The use of authentication tools such as 3SKey is just one measure to help support security efforts in this context). Going forward, SWIFT will also be providing regular updates to its software and tools to make the requirements of the mandatory controls as easy as possible to implement, and will be working with a network of service partners to assist customers if they need specific hands-on support to implement the controls in their local environment.

To ensure adoption, SWIFT will start requiring customers to provide self-attestation against the mandatory security controls from Q22017 onwards. The controls and self-attestation requirement will be fully effective from January 2018, including inspections from internal or external assurance providers conducted with samples of customers to provide additional assurance regarding the accuracy of their self-attestation. Details of the compliance status of each customer will be made available to their counterparties, which will allow corporates to check their partner banks' status and provide similar information to others.

Corporates using a cloud based infrastructure such as Alliance Lite2 will have fewer directly applicable requirements than those with installed on-premise interfaces. Nevertheless all in-scope mandatory security controls must be adhered to, and self-attestation will also be expected of corporate customers. During the first half of 2017, SWIFT will be conducting roadshows across markets worldwide to support customers in understanding the requirements of the security controls framework and related attestation and assurance process. The roadshows will also help customers identify service partners offering practical assistance with implementation.

In the case of corporates using a service bureau, each corporate will still have direct responsibility for its own self-attestation, so the requirements on Alliance Lite2 customers and those using a service bureau are alike. Customers are responsible for their choice of third-party product and service providers, and should satisfy themselves that the cyber security standards of their service providers (e.g., vendors or service bureau) are appropriate and comprehensive. This includes carrying out your own checks, due diligence and risk assessments. In addition, every SWIFT certified service bureau will be subject to enhanced security inspection by 2018 as part of SWIFT's Shared Infrastructure Programme. Customers are encouraged to check the latest certification status as published in the Service Bureau Directory on swift.com.

What you can do

Make sure you are aware of SWIFT's security controls framework and get ready to implement the mandatory controls, and return your self-attestation to SWIFT starting from Q2 2017. SWIFT will be working with service partners to help support customers with this process. For service bureau users, you may wish to check that your service bureau is also taking appropriate action. Customer information on SWIFT's security controls framework, and the latest security guidance documents on Alliance, Alliance Lite2 and third party interfaces can be found on KB tip 5020786. Please also ensure you and/or your service bureau install any mandatory software updates from SWIFT that relate to security within the defined deadlines.

[1] Available on Knowledge Base Tip 5020786

Preventing and detecting fraud

Companies do not operate in a vacuum and many corporates are receivers as well as senders of messages over SWIFT. Even with strong security measures in place, attackers are very sophisticated and it has to be assumed that attacks may happen. That's why SWIFT is urging all customers to manage security risk in interactions and relationships with counterparties.

Corporates, as for any connected institution, should consider the risks associated with payment relationships. RMA is the SWIFT Relationship Management Application that enables the controlled exchange of financial messages. With RMA, any unwanted traffic is blocked at the sender level, reducing the operational and fraud risks associated with handling unwanted messages. SWIFT is asking all connected institutions, including corporates, to review their SWIFT relationships and to consider removing unused or dormant RMAs. SWIFT is also encouraging the use of RMA Plus, an enhanced RMA service which allows an institution to specify and control which message types they receive from various counterparties.

To support smaller institutions in particular, SWIFT has launched new anti-fraud reporting tools to provide customers with daily activity or validation reports which provide a daily SWIFT-generated record of their transaction activity over SWIFT. These Daily Validation Reports offer both a means of reconciling transactions to prevent and detect fraud and a focused review of large or unusual flows. These reports are available to assist customers even if their own environment has been compromised and their local SWIFT transaction records altered.

Detection measures need to be put in place to increase the chances of stopping fraud in case your environment is breached. An area of good practice is the review of message confirmations and end-of-day statements. Payment confirmations should be generated whenever a legitimate transaction is made. Checking that these confirmations match the transactions shown on a SWIFT generated daily validation report is a simple process which can help all institutions avoid the risk of falling victim to fraud. Similarly, end-of-day statements should also be checked. Discrepancies between actual and reported payments could indicate fraudulent transactions and should be investigated immediately. Even where there are no discrepancies in settlement processes, unusual or uncharacteristic payments should be given extra scrutiny and there should be increased focus on new supplier and payment relationships, or the changes in the payment details associated with these relationships. In the event fraudulent payments are identified, following proper market practice with appropriate and timely cancellation messages to counterparies may reduce the impact of any fraud that does take place and increase the likelihood of recovery of funds.

What you can do

Ensure that you have appropriate processes in place to reconcile on a daily or more frequent basis confirmation and statement messages so that discrepancies due to fraud can be quickly and easily identified. Ensure that you are aware of the processes required for message cancellations and the response process for cancellations. Review your RMA relationships and ensure that they are appropriate for your business needs, and look to adopt RMA Plus to provide enhanced control of message flows.

Stronger together

The techniques and approaches of cyber-criminals change rapidly, which is why corporates need to be on high alert in order to ensure effective protection and control of their local SWIFT environment, as well as their overall technology systems. SWIFT is supporting its community of users by sharing intelligence, which will aid in strengthening collective defences with a view to avoiding repeat attacks.

All SWIFT users have an obligation to share relevant information with SWIFT if they experience fraud or suspect a security breach relating to their SWIFT connectivity. SWIFT has a dedicated Customer Security Intelligence team that shares anonymous information on Indicators of Compromise (IOCs) and details the modus operandi used in known attacks, sharing that information back with the wider community. Regular updates are provided via SWIFT's Security Notification Service which all customers should subscribe to in order to be able to act upon that information as fast as possible.

While larger corporates may have their own cyber threat analysis / SIEM capabilities, some may receive only business segment cyber intelligence, for example, specific to the healthcare or aviation industries. SWIFT is currently expanding its own information sharing platforms, to share broader cyber intelligence on SWIFT-related infrastructure as widely as possible.

For further information visit the Customer Security Programme pages on swift.com. For additional questions visit Customer Support.

What you can do

Sign up to SWIFT's security notification service to ensure you receive the latest information and updates to assist in preventing attacks. To do so, visit the customer section of swift.com and sign up to the security notification service in the newsletter section. It is also important that you register your CISO with SWIFT, so that SWIFT has up to date contacts to reach you. You can register on the Customer Security Programme page on SWIFT.com.

57248 - January 2017