VIR Vietnam Investment Review

A comprehensive approach to SWIFT security assessment

11:33 | 06/04/2021

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a vast messaging network used by banks and other financial institutions to quickly and securely send and receive information, such as money transfer instructions.

Tran Phuong Hong, IT Advisory director, KPMG Tax and Advisory Vietnam and Do Kim Hien, senior solution consultant, KPMG Tax and Advisory Vietnam

In Vietnam, we have had vast opportunities in conducting SWIFT system security gap assessment projects for Vietnamese banks, and there are best practices that clients should consider while implementing and securing the system according to a SWIFT Customer Security Control Framework (SWIFT CSCF).

The SWIFT CSCF describes a set of mandatory and advisory security controls for users. Mandatory security controls establish a security baseline for the entire community and must be implemented by all users on their local SWIFT infrastructure. The SWIFT has chosen to prioritise these mandatory controls to set a realistic goal for near-term, tangible security gain, and risk reduction.

Advisory controls are based on good practice that SWIFT recommends. Over time, mandatory controls may change due to the evolving threat landscape, and some advisory controls may become mandatory.

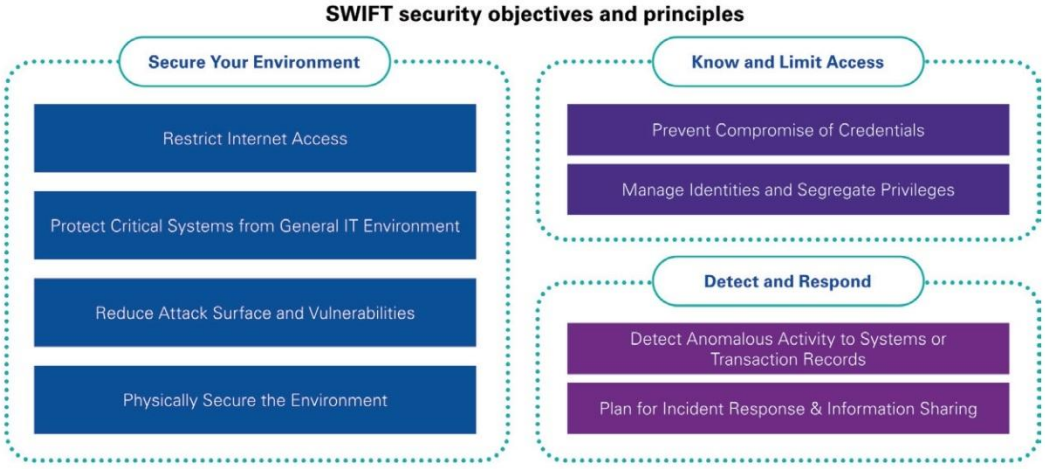
All controls are articulated around three objectives: 'Secure your Environment', 'Know and Limit Access', and 'Detect and Respond'. Controls have been developed based on SWIFT analysis of cyber threat intelligence and in conjunction with industry experts and user feedback. Control definitions are also intended to be in line with existing information security industry standards.

SWIFT CSCF version 2021 has defined 31 security controls (22 mandatory and nine advisory controls) that underpin these objectives and principles. The controls are intended to help mitigate specific cybersecurity risks that users face due to the cyber threat landscape. Within each security control, SWIFT has documented the most common risk drivers that the control is designed to help mitigate.

Addressing these risks aims to prevent or minimise undesirable and potentially fraudulent business consequences, such as unauthorised sending or modification of financial transactions; processing of altered or unauthorised SWIFT inbound transactions; business conducted with an unauthorised counterparty; and confidentiality or integrity breach of business data, computer systems, or operator details.

Ultimately, these consequences represent enterprise-level financial, legal, regulatory, and reputational risks.

Common violations



During the gap assessment for the SWIFT system, we have noticed a number of common issues that financial institutions often violate compared to SWIFT CSCF requirements.

Firstly, the network micro-segmentation for applications and SWIFT systems is not carried out clearly and completely. For example, email or active directory applications still have common connections to the SWIFT system.

Secondly, security policies and procedures (for example security vulnerability management procedure, and malware prevention procedure) are not detailed, accurate, or aligned to the current situation of the system.

Next, system hardening guidelines/standards are not fully and completely developed, and they are not periodically reviewed and updated. Additionally, the security vulnerability scanning is only conducted on important applications and servers. For network devices, virtualisation platforms, or databases, the scanning is almost ignored.

Finally, the password policy is only applied to Windows servers and not applied on network devices, security devices, or Unix/Linux platforms.

In order to fully assess the security controls of the SWIFT environment, the following important points should be noted.

Understanding client's SWIFT architecture: The current architecture of SWIFT is divided into four types - A1, A2, A3, and B. Each architecture has a difference in components and the connection from the client to SWIFT. So, understanding each type of architecture will help you identify the scope and assess the relevant systems involved that may affect the security of the SWIFT environment.

Understanding security controls: SWIFT's security controls are only applied to a certain scope - SWIFT systems and indirect infrastructure related to it. You need to be aware of connections and determine which scope would apply security controls to avoid assessing unnecessary components that are outside the scope.

Understanding mandatory and advisory controls: SWIFT's security controls are divided into mandatory and advisory controls. Depending on the requirements of the customer and the scope of the assessment, you should decide which controls should be reviewed and evaluated in the most appropriate way.

Understanding the objective of each control: SWIFT CSCF 2021's security controls are divided into eight groups. Understanding the objective of each control makes it easier to identify alternative controls if they exist and avoid misjudging the customer's current security level because during the assessment, it is realised that customers could use different security controls than required by SWIFT and still meet the final objective and ensure the safety of the system.

Understanding purpose and role of SWIFT components: SWIFT includes many components with different roles such as messaging interface, communication interface, SWIFTNet Link, connector, and more. These components connect, interact, and have mutual security relationships. Therefore, understanding the roles and functions of each component helps you determine which security controls are appropriate for which component, thereby assessing most accurately and effectively for potential risks.

As international transactions and commerce become more popular, SWIFT becomes one of the important components of financial institutions, especially banks. Therefore, its security needs to be paid close attention to properly minimise fraud in international transactions, protect user data, and safeguard the reputation of the organisation.

Tran Phuong Hong, IT Advisory director and Do Kim Hien, senior solution consultant, KPMG Tax and Advisory Vietnam

Article's Link: https://www.vir.com.vn/a-comprehensive-approach-to-swift-security-assessment-83494.html