Privileged Access and the

SWIFT

Customer Security Control Framework

SWIFT (the Society of Worldwide Interbank Financial Telecommunication) provides financial messaging services to banks, financial institutions and corporations all over the world. The technology is used to exchange sensitive information about financial transactions by more than 11,000 customers in over 200 countries.

Unsurprisingly, with so much sensitive data and financial information being transferred using SWIFT, it has become a major target for cybercriminals. In fact, over the past five years, international cyber criminals have been increasingly targeting SWIFT infrastructure to complete a number of high-profile fraudulent transfers.

It’s big business with big numbers.

This is just the tip of the iceberg. A recent SWIFT report – Three years on from Bangladesh: Tackling the adversaries[5] – found that cybercriminals are targeting smaller amounts ($250,000 to $2 million) to fly under the radar of authorities and financial executives.

2018 **$100M+** theft via fraudulent transfers through SWIFT by North Korean government hackers, known as APT38. They were outted by U.S. cyber security firm FireEye as having a sophisticated hacking campaign against banks in Asia and Africa [4].

2018 **$13.5M** India’s Cosmos Bank[3] lost $13.5 million in an attack using unauthorised SWIFT transactions.

2016 **$81M** the Central Bank of Bangladesh[2] lost to attackers, who attempted to steal nearly $1 billion.

2015 **$12M** was stolen from Ecuadorian bank Banco del Austro[1] using SWIFT.

As a direct result of this, SWIFT has put in place its own stringent internal security measures, and it has also created its Customer Security Controls Framework (CSCF). The CSCF is a collection of mandatory security controls designed to establish a security baseline for the entire SWIFT community – they must be implemented by all users on their local SWIFT infrastructure.

As the company explains on its website, these controls aim to set a "realistic goal for near-term, tangible security gain and risk reduction". And with the threat landscape evolving, SWIFT continues to update its CSCF requirements on a regular basis. The latest update, CSCF v2019[6], sees a number of new mandatory controls put in place, including: secure operator sessions, yearly vulnerability scanning, and physical and logical password storage.

This white paper sets out how Thycotic's Privileged Access Management solution can help banking and finance teams deliver best-of-breed security to SWIFT environments and meet SWIFT CSCF requirements.

The Critical Role of Privileged Access for SWIFT

Controlling access credentials is a critical part of protecting your data.

33%

OF CYBER CRIMINALS PRIORITISE IDENTIFICATION AND ACCESS TO PRIVILEGED CREDENTIALS AS A STRATEGIC OBJECTIVE[7].

80%

OF SUCCESSFUL BREACHES LEVERAGE A PRIVILEGED ACCOUNT[8].

Specifically, when it comes to banking and finance firms, it has been revealed that they face four times the number of attacks[9] as other businesses – and SWIFT credentials form a critical target for cyber criminals within this. Teams also need to ensure the entire SWIFT environment and surrounding networks are secured to prevent lateral movement and privilege escalation.

The following section shows how the Thycotic PAM solution can be used to meet specific requirements within the SWIFT CSCF.

Mapping SWIFT CSCF to Thycotic PAM Suite Capabilities

Mandatory Security Controls	Control Objective	Thycotic Solution
SWIFT Environment Protection	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	Thycotic's Privileged Access Management suite enables SWIFT teams to isolate and control SWIFT and other sensitive privileged sessions. Role-based access control, behavioural analytics, and session control ensure that a principle of least privilege is established for users and systems, delivering advanced security to SWIFT environments. All privileged administration is controlled, logged, monitored, and reported on by Thycotic. White, grey, and black-listing of applications is also made possible through the Thycotic platform.
Operating System Privileged Account Control	Restrict and control the allocation and usage of administrator-level operating system accounts.	Thycotic provides privileged access management at the account and admin level. This means that access to any critical system credentials, including SWIFT environments and OS level admin, can be made subject to a range of different controls at the application and command level. These include: role-based access control, password masking, credential rotation, workflows, session isolation, reporting, behavioural analytics, session monitoring, and session control.

Reduce Attack Surface and Vulnerabilities

Mandatory Security Controls	Control Objective	Thycotic Solution
Security Updates	Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.	Thycotic's role-based access functionality can ensure that access to SWIFT systems and the wider environment is configured based on the security needs. During periods of potential vulnerability, admin access can be scaled back to meet the security concern. Thycotic can also enable application policies to be configured on critical systems to limit exploitation of vulnerabilities on systems.
System Hardening	Reduce the cyber attack surface of SWIFT-related components by performing system hardening.	The Thycotic platform enables hardening of the SWIFT system and environment at multiple levels. Role-based access control ensures visibility of privileged access and enables the minimum admin credentials to be in place for optimal operation of the environment. At the server and endpoint level, hardening is possible by implementation of intelligent application policies (white, grey, and black-listing), and the de-provisioning of Local Admin rights from critical systems.
Vulnerability Scanning*	Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process and act upon results.	Vulnerability scanners can be integrated with Thycotic for secure authentication. This ensures that vulnerability scanners have secure and agile access to the environment.

Physically Secure the Environment

Mandatory Security Controls	Control Objective	Thycotic Solution
Physical Security	Prevent unauthorised physical access to sensitive equipment, workplace environments, hosting sites, and storage.	The Thycotic vault can also be used to store general credentials for access in physical environments. These can be securely retrieved from the mobile app as required. This ensures role-based access control and auditing is possible at the physical level.
Password Policy	Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.	The Thycotic suite enables advanced credential security across a vast number of environments and systems. All of this can be managed through a single pane of glass with broad and granular configurations available. This password management extends across traditional privileged admin and root accounts, service accounts, cloud and SaaS credentials, hard-coded credentials in scripts and DevOps environments, and sensitive financial admin accounts such as SWIFT. Credentials can also be masked and automatically injected at the inception of sessions launched using Thycotic. This means passwords remain unknown to privileged users. Password policy can be configured to meet custom requirements both in terms of complexity and the frequency of change.

Physically Secure the Environment

Mandatory Security Controls	Control Objective	Thycotic Solution
Multi-Factor Authentication	Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.	Thycotic integrates multi-factor authentication to strengthen the authentication and authorisation process for all privileged identities. With the advanced behavioural analytics in place, Thycotic also employs a sophisticated threat identification algorithm. This forces users to reauthenticate using multi-factor authentication (MFA) for continued access if their threat score exceeds the base line they have been assigned.

Manage Identities and Segregate Privileges

Mandatory Security Controls	Control Objective	Thycotic Solution
Logical Access Control	Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts.	Thycotic enables the principle of least privilege to be enforced at the account, application, and command level. All administrative functions can be subject to the same granular role-based access control, ensuring that only the right people have access to the necessary privileges at the right times.
Physical and Logical Password Storage*	Protect physically and logically recorded passwords.	The Thycotic vault can be used to protect credentials for physical systems, as well as high-privilege admin rights and hard-coded credentials. This breadth of application ensures that all privileged credentials are controlled and audited from a single pane of glass.

Detect Anomalous Activity to Systems or Transaction Records

Mandatory Security Controls	Control Objective	Thycotic Solution
Malware Protection	Ensure that local SWIFT infrastructure is protected against malware.	Thycotic Privilege Manager enforces intelligent application control meaning that only whitelisted applications can run on critical systems. Greylists and blacklists can also be used to ensure intelligent elevation. Integrations with Cylance and Virus-Total enable dynamic policies based on intelligence feeds.
Logging and Monitoring	Record security events and detect anomalous actions and operations within the local SWIFT environment.	Thycotic's threat analytics automate the detection of suspicious and anomalous privileged activity. The machine learning algorithm analyses standard user behaviour to build a baseline for every user based on variables such as IP address, time of day, and privileged activity. The analytics solution then automates remediation based on configurable preferences. Suspicious and anomalous users have their access revoked and can be: 1. Disallowed reauthentication for a set time period 2. Forced to request access 3. Forced to reauthenticate using two-factor authentication

Plan for Incident Response and Information Sharing

Mandatory Security Controls	Control Objective	Thycotic Solution
A Virtualisation Platform Protection*	Secure virtualisation platform and virtual machines (VMs) hosting SWIFT-related components to the same level as physical systems.	Thycotic can extend protection to the virtual environments and their root credentials, ensuring that only the right users have access at the right times.

Reduce Attack Surface and Vulnerabilities

Mandatory Security Controls	Control Objective	Thycotic Solution
A Back Office Data Flow Security	Ensure the confidentiality, integrity, and mutual authenticity of data flows between back office (or middleware) applications and connecting SWIFT infrastructure components.	For privileged sessions, Thycotic encrypts all data in transit using SSL/TLS certificates. The Protocol Handler enables communication from the client machine to the platform via a launcher (such as RDP or PuTTY). Communication is over HTTP(S). Credentials are retrieved securely using signed and AES-256 encrypted messages.
A Critical Activity Outsourcing	Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.	Due to session isolation capabilities, Thycotic is able to control and monitor remote access to privileged systems. Third parties and high-risk remote users can be subject to a more carefully constructed experience that includes functions such as: • Request to access workflows • Session recording and live session monitoring • Application and command policies • Behavioural analytics and automated remediation • Role-based access control on the account, system and application level

Detect Anomalous Activity to Systems or Transaction Records

Mandatory Security Controls	Control Objective	Thycotic Solution
A Intrusion Detection	Detect and prevent anomalous network activity into and within the local SWIFT environment.	Thycotic's threat analytics automate the detection of suspicious and anomolous privileged activity both for those launching sessions, and those administering the solution. The machine learning algorithm analyses standard user behaviour to build a baseline for every user based on variables such as IP address, time of day, and privileged activity. The analytics solution then automates remediation based on configurable preferences. Suspicious and anomalous users have their access revoked and can be: • Disallowed reauthentication for a set time period • Forced to request access • Forced to reauthenticate using two-factor authentication

* new advisory controls

Conclusion: The Thycotic Solution for SWIFT

Thycotic Privileged Access Management platform enables businesses to get visibility of privileged accounts, users, systems and operations in order to enforce role-based access control and a principle of least privilege across the environment. It enables IT to force strong and intelligent authentication for all users and applications that require privileged access, and automates the identification of anomalous behaviour and its successful remediation.

Specifically for banking and finance teams, this means that they can control, monitor, and audit the SWIFT environment to deliver best-of-breed security and meet SWIFT CSCF requirements.

Ready to move forward?

Trying out Thycotic's PAM solution is simple.

Thycotic offers free trial licenses for our Privileged Access Management solutions on premise and as SaaS. You can find these on our website, along with free discovery and templating tools for PAM projects.

Sources

1. https://www.bankinfosecurity.com/another-swift-hack-stole-12-million-a-9121.
2. https://www.databreachtoday.com/bangladesh-bank-attackers-hacked-swift-software-a-9061
3. https://www.reuters.com/article/cyber-heist-india/indias-cosmos-bank-loses-135-mln-in-cyber-attack-idUSL4N1V551G
4. https://www.bankinfosecurity.com/north-korean-hackers-tied-to-100-million-in-swift-fraud-a-11579
5. Three years on from Bangladesh: Tackling the adversaries: https://www.swift.com/resource/three-years-bangladeshtackling-adversaries
6. https://www.swift.com/myswift/customer-security-programme-csp/security-controls
7. 2017 Black Hat Hacker Report https://thycotic.com/resources/black-hat-2017-survey/
8. The Forrester Wave™: Identity Management And Governance, Q3 2018
   https://www.forrester.com/report/The+Forrester+Wave+Identity+Management+And+Governance+Q3+2018/-/E-RES142635
9. https://www.csoonline.com/article/2938767/report-banks-get-attacked-four-times-more-than-other-industries.html

ABOUT THYCOTIC

The easiest to manage and most readily adopted privilege management solutions are powered by Thycotic. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility and control.

www.thycotic.com

thycotic