The Coastal Business Journal

Volume 18 | Number 1 Article 2

December 2021

A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches

Xiang Michelle Liu
Marymount University

Recommended Citation

Liu, Xiang Michelle (2021) "A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches," *The Coastal Business Journal*: Vol. 18 : No. 1 , Article 2.
Available at: https://digitalcommons.coastal.edu/cbj/vol18/iss1/2

The Coastal Business Journal

ISSN: 2163-9280 Fall 2021
Volume 18, Number 1

A Risk-based Approach to Cybersecurity: A Case Study of Financial Messaging Networks Data Breaches

Xiang Michelle Liu, School of Technology and Innovation, Marymount University

ABSTRACT

With banking becoming increasingly global and largely digital, a magnitude of data breach incidents resulted from cyberattacks have been observed and can be frequently traced to ineffective security practices and procedures. Cyberattacks do not require physical proximity, nor are they deterred by national borders. Cybercriminals can remain undetected for a long period of time. Such breaches inevitably result in losses of reputation, customer confidence, and in some instances, productivity. The purpose of this study is to take a deeper look into various breaches of the SWIFT (Society for Worldwide Interbank Financial Telecommunication) messaging network to illuminate vulnerabilities inherent in the international banking system and the channels through which a series of advanced, persistent threats (APT) can take place. The author discusses a variety of venues for banks to embrace new cybersecurity mindsets and incorporate governance mechanisms into their risk management processes as it relates to security control, data retention, and continuous monitoring. The study further calls for financial institutions to make a collective effort in taking proper precautions to safeguard the banking ecosystem. The paper concludes with the lessons learnt and the future research directions.

Keywords*:* SWIFT, cyberattack, risk management, data breaches, security control

BACKGROUND INTRODUCTION

The SWIFT is an international messaging network for conducting financial transactions. Since founded in 1973, the network has grown from 239 customer banks to over 11,000 financial institutions across 200 countries. However, the cybersecurity measures implemented in the SWIFT network seemingly could not keep abreast with its rapid growth and expansion. For instance, during the last decade or so we have witnessed a string of cybercrimes targeting the SWIFT member banks that resulted in the loss of millions of dollars. The SWIFT messaging system has been regarded as the "weakest link" in a banking ecosystem. One of the major motivations of this study is to investigate various SWIFT data breach cases and seek root causes of those breaches. Particularly, the study aims to identify the gap between the extant state of SWIFT as an electronic banking platform and the desired state of fund transferring processes. By examining vulnerabilities associated with the SWIFT banking platform, this paper is to draw more attentions to current security postures that financial institutions take and their impacts on data privacy and security, the reputations of these institutions, and ultimately global banking.

The strategic goal of this research is to assess the vulnerability level in an international banking system to cyberattacks, and examine the necessity for financial institutions to form global alliances to safeguard their systems. By presenting the case studies on a series of cyberattacks exploiting vulnerabilities in the SWIFT system, this paper illustrates the importance of conducting risk assessment plans in financial institutions when facing with advanced, persistent threats (APTs).

The rest of the paper will review a series of data breaches on the SWIFT network and their impacts. The threat and vulnerability factors faced by SWIFT member banks are assessed and the level of cyber risks within the banking and payments sector are examined as well. Further, existing regulations are reviewed based on an extensive survey of the current industry practices. Countermeasures taken by the SWIFT are discussed next, followed by a step-by-step illustration of integrating a risk management framework into the SWIFT Customer Security Control Program. The last section reiterates the importance of developing a cybersecurity culture and outlines an overarching work plan by SWIFT member banks.

RESEARCH METHODOLOGY

The research was conducted using a case study methodology. The author examined a series of SWIFT breaches, focusing on why the member banks fell for social engineering and insider threat attacks, the implications of those breaches, and how it could potentially be resolved. Case study method has been widely applied in social science and behavioral studies, which is utilized when an in-depth investigation is required. The rationale of utilizing case study method lies in that such approach is particularly suitable to explore ‘how’ or ‘why’ questions about a contemporary set of events (Yin 2014). Therefore, the research questions and focus of this study would be well supported. The author followed the five major steps of case study research identified by Yin (2014):

- Identify the research phenomenon;
- Design the study with research questions;
- Collect data by gathering literature, secondary data, and relevant technical reports;
- Analyze the results for the research questions; and
- Interpret findings.

To locate the relevant literature on the surge of SWIFT data breaches and contributing factors to those breaches, the author has used multiple literature search strategies, including online search of major databases and manual search of references. Specifically, the author focused on several major online databases including ProQuest, ABI/INFORM, ACM Digital Library, and Security Management Practices. The initial search was based on combination of a series of key words such as SWIFT, data breach, financial section, and security program.

A CLOSER EXAMINATION OF SWIFT DATA BREACHES

Technology is changing and shaping how organizations do work and how people perform tasks. The growth in information technology (IT) has enabled organizations in the banking sector to serve customers and manage high volumes of assets in a more effective and streamlined manner. At the same time, the financial industry also becomes a highly profitable target for criminals due to various cybersecurity challenges.

Criminals have launched a series of cyberattacks on the global banking system through the SWIFT messaging system. One of the high-profile heists in the early days involved phony transfers of $81 million from the central bank of Bangladesh in February 2016. Hackers first introduced a malware into the bank's server to steal login details for the SWIFT messaging system. They then successfully covered their infiltration traces by removing evidence from printed SWIFT messages in real time (Al-Mahmood, 2016). In addition, several other unauthorized bank transfers with the similar infiltration mechanism surfaced in other parts of the world. The criminals were able to operate the infiltration schemes successfully without being detected for months until the damages were done (Sharma, 2017).

Analysis

According to a report by Reuters, SWIFT issued a private alert in April 2016 about fraudulent transfers across its network but withheld names of victims and the losses from those attacks (Finkel, 2016). The warning was the first indication that the popular Bangladesh attack was not a standalone event but one of related criminal schemes targeting the messaging platform. Later in the summer of the same year, an executive of the organization told a group of the association of banks in Singapore during a meeting that it was looking into twenty-six attempted attacks on banks (Burne & Sidel, 2017).

Researchers at Symantec discovered evidence in the Philippines bank hack which was related to the group involved in the hacks in Bangladesh central bank and Tien Phong Bank in Vietnam (Symantec, 2016). An examination of SWIFT's practices indicated that it was not fully prepared for the toughest challenges the attacks brought (Burne & Sidel, 2017). Even though it thoroughly locked down the heart of its network, the emergence of reports of subsequent attacks continued raising concerns about vulnerabilities in the messaging system run by SWIFT.

In a Cyber Security and SWIFT hacking conference organized by the National Banking Institute of Nepal with an audience of over 150 bankers, it was discovered that virtually all the bankers present did not use genuine software at their offices (Sharma, 2017). Pirated software has been regularly cited as a major vulnerability source resulting in out-of-date patches, updates, and cybersecurity safeguards. This worrisome fact further corroborates the belief that more rigorous and effective cybersecurity framework and standards are much needed to be enforced across the SWIFT member banks.

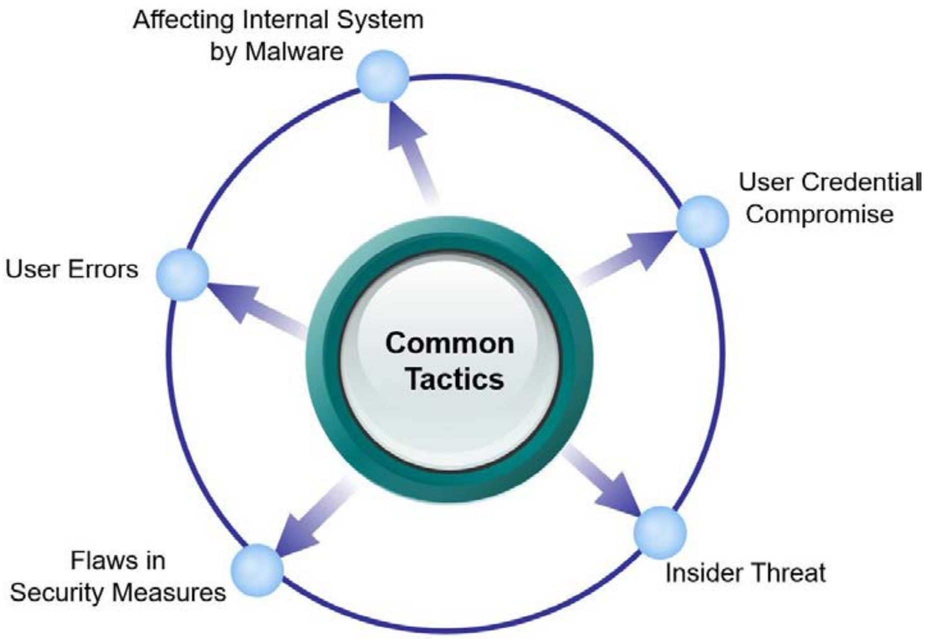
The SWIFT network attacks were carried out in the same pattern. Virtually all the attacks involved the use of malware on the banks' network systems. The attackers combined this method with employee credentials to get on the banks' networks but none of those attacks affected SWIFT's core network directly. The success of the attacks was mostly the outcome of the weaknesses in the security measures put in place by those banks. When examining the major attacks closer, a common pattern can be found across different data breaches in terms of attack vectors, mechanisms, and vulnerabilities. First, the attackers used state-of-the-art skills to gain access to the banks' networks, then instituted command and control to direct information using a backdoor for their secret hideouts. Soon as they gained access to the banks' networks, the next thing was to sort out major transaction applications like the SWIFT messaging network applications. Once sorting out, the attackers studied the flow of information and collected credentials for the SWIFT Alliance Access (SAA), SWIFT Alliance Web Platform and SWIFT Alliance Gateway (SAG), looking for resources with the necessary characteristics such as IP addresses, port numbers, files, Web pages and digital certificates. After the surveillance was completed, the onslaught method was then created using gained resources about the banks' operations, server distribution, credentials, and SWIFT's application units. Armed with these details, the attackers could then set up phony messages or alter actual messages to allow transfers to controlled accounts. Finally, when the money got into the controlled accounts, it was then moved immediately either as cash or transformed into bitcoin and scattered around to frustrate the evidence trail.

Three strains of malware used to exploit the SWIFT networks in South-East Asia are named as Backdoor.Fimlis, Backdoor.Fimlis.B, and Backdoor.Contopee (Symantec, 2016). One piece of interesting forensics evidence is that Backdoor.Contopee shared part of the common source code with another malware named Trojan.Banswift that was used to manipulate transactions in the Bangladesh attack (APSM, 2016). It further corroborates the speculation that Lazarus group who was blamed for the Sony Entertainment attack was involved in some of those SWIFT data breaches as well.

In summary, these attacks are indications of the continuous threats cybercriminals posing to payment systems, through which they can access large amounts of money transferred to SWIFT and its wide community. Furthermore, these incidents also imply the need for stronger security protocols throughout the organizations. Common attack tactics (F-Secure, 2018) are illustrated in Figure 1.

Figure 1.

Common Attack Tactics Carried Out in SWIFT Hacks


Affecting Internal System by Malware
User Credential Compromise
User Errors
Common Tactics
Flaws in Security Measures
Insider Threat

A more structured detailing of each case with a comparison across all ten cases is demonstrated in Table 1.

Table 1

Summary of Ten SWIFT Hacking Cases from 2013-2018

Bank (Location)	Timeframe of the Heists	Hacking Tactics Used	Monetary Loss (in $)
Sonali Bank, Bangladesh	January 2013	• Keyloggers were used to steal employee credentials • Located SWIFT connected systems	$250,000
Banco del Austro, Ecuador	January 2015	• Employee credentials stolen • Altered transfer request details	$12,000,000
A bank in the Philippines	October 2015	• Affected the bank's internal system by malware	Unknown
Tien Phong Bank, Vietnam	December 2015	• Affected the bank's internal system by malware	$1,130,000 (attempted)
The Bank of Bangladesh, Bangladesh	February 2016	• Affected the bank's internal system by malware	$81,000,000 (of $951,000,000)
The Far Eastern Bank, Taiwan	October 2017	• Affected the bank's internal system by malware • Compromised SWIFT operator credentials	$160,000 (of $60,100,000)
NIC Asia Bank, Nepal	October 2017	• Employees used a designated computer (only for SWIFT transactions) for other purposes	$580,000 (of 4,400,000)
City Union Bank, India	February 2018	• Compromised employee credentials	$2,000,000
A bank in Russia	February 2018	• Gained access to an internal computer	$6,000,000
Bank Negara, Malaysia	March 2018	Unknown	Halted, so no monetary loss

Regulations and Legislations

While SWIFT could advise its member banks to adopt certain minimum-security standards, no designated organization was in charge of how central banks and financial institutions should secure their payment networks. The SWIFT data breaches shed light on the primary challenge in fighting cybercrimes, which is the blanket nature of online environments as well as the complexity involved in investigations and prosecution.

The cross-border nature of cybercrime creates a huge obstacle for countries to successfully trace the origins and hold them accountable without help from others (Brenner, 2007). Despite the efforts by many nations across the world to combat cybercrimes, criminal activities continue to flourish and become heightened in Africa and Asia (Butkovic et al., 2019). For example, cybercrimes committed in Europe or the U.S. stand a higher chance of being punished than those committed in other regions because of the attitude of government in those places. Another reason is the difference in lawmaking patterns that do not touch on all areas involved in cybercriminal activities. Such gap introduces a lot of exploitable legal means of escape, which increases the likelihood of cybercrime in those countries.

Cybersecurity-related incidents are usually not reported, and when they are, the prosecutors are opposed by difficult challenges. For instance, many developing nations do not have laws that address cybercrimes. The extant laws formulated for the security of tangible properties are not armed to handle their counterparts in the cyberspace. Even in the areas where legislation exists for cyber offences, investigations and prosecution of these type of crimes are often obstructed due to the constraints in investigative competence and difficulties of collecting digital evidences across the country’s judicial structure.

Multiple daring cyberattacks on banks across the world within several years woke up executives from complacence to a world of digital truth. Prior to these attacks, security requirements for the network was prescribed in a handbook with guidelines that were mostly voluntary and rarely enforced. Such situations have changed since SWIFT revised its procedures in 2017 to require member banks of a demonstration of annual security compliance with new protocols in response to the attacks (Baert, 2016). Sixteen new controls were rolled out, including tighter password security (e.g., two-factor authentication) and an order for banks to update their software regularly (Burne & Sidel, 2017). An anomaly detector designed to flag and suspend unusual payment instructions was also part of the controls. It was believed the new security toolkits and controls could easily mitigate the recent heists if a version of the tool was implemented earlier instead of relying on banks to safeguard their own security (Burne, 2017).

In early 2017, as part of SWIFT's global payments innovation (GPI) initiative, private blockchain was carried out in a closed environment, with specific profiles and strong data controls, privileges, and access being diligently monitored (SWIFT, 2017). After SWIFT took all these measures to protect its customers, fresh attacks were still recorded in the following years as highlighted in some of the cases above, proving these criminals had more advanced knowledge and capability on manipulating the banking system than previously believed.

DISCUSSION

In the major attacks highlighted above, malware was the key technology component used for the attacks, which might be due to older versions of anti-malware software running or software being put on a periodic detection mode for the performance purpose. Investigations by the FBI revealed evidence that one or more of Bangladesh bank employees may have assisted in the theft although that possibility was initially played down by cyber investigators, who suggested the entire operation could have been carried out remotely. Further investigation showed the central bank of Bangladesh neither used a two-factor authentication on its systems nor changed its SWIFT default password till the hackers breached the bank's systems (Burne & Sidel, 2017).

The investigations implicated multiple channels and factors leading to the breaches. For instance, SWIFT used third-party vendors for part of the work, which probably increased the bank’s exposure to potential threats. On the other hand, all services were performed according to the instructions of local banks. It could not have deviated from the agreements without the bank’s consent. Security breaches of protocols such as the use of personal emails on dedicated computers attached to SWIFT’s servers might have been a possible avenue to corrupt the banks' systems with malware. The biggest consensus on the Bangladesh case is that the bank provided poor firewall protection and used a second-hand network switch worth $10. All four accounts in Rizal Commercial Banking Corp (RCBC) in the Philippines, to which the stolen funds from Bangladesh were transferred into, were opened in May 2015 and were never used before the Bangladesh money transfer. The driver’s licenses used as identity documents in opening those accounts were fraudulent (Chilkoti et al., 2016). The above evidence pointed to the fact that this attack was planned well in advance. These were huge red flags, indicating the affected banks never conducted due diligence in the account opening process nor verified received funds. Verification and validation procedures should have been implemented for such large transfers. In addition, certain pre-existing conditions for those accounts should have been stipulated as part of protocols and enforced in local banks.

Some of the software purchased by NIC Asia Bank from so-called reliable vendors were found to be pirated. The fact that the use of pirated software is rampant among financial institutions in Nepal prevents these institutions from installing new patches or upgrading software and building a robust IT infrastructure. In the case of the Vietnamese bank hack, its risk warning and oversight systems played a key role in stopping the scam because it has enforced a strong internal control process since 2014. These components were missing in the other cases highlighted above.

Unfortunately, the recovery of money stolen by cybercriminals is not a simple process. As shown by the Bangladesh experience, all of the money stolen from Bangladesh disappeared after reaching the Philippines and Sri Lanka, where they were spread into casinos. The hunt for the $81 million in the Philippines was complicated by the restricted scope of the Philippine's anti-money-laundering laws that do not include gambling facilities. Although SWIFT has an authentication protocol that prevents transfers to individuals or businesses under sanctions, this protocol does not protect customers from unauthorized transfers or recalls when they happen.

Even though SWIFT took steps to pass information to its member banks regarding security measures, it did not go further to enforce the standards by conducting periodic audits or stipulating mandatory compliance. On the other hand, banks cannot rely solely on SWIFT to prevent these cyberattacks. The responsibility of preserving and defending their assets remain with the individual banks since these transactions take place in their environments and on their premise. A common theme emerging from various reports is the mode of occurrence of these attacks, which presented similar patterns across all cases. The attackers compromised the bank's environment, obtained credentials with authority to initiate transactions, approved and sent messages on network, and then hid evidences by removing traces of fraudulent messages.

The Bangladesh case provides shocking evidence of the vulnerability of the banking system and a clear case of combined human factors. The biggest lesson from the Bangladesh bank heist and others is the cost of noncompliance is way higher than not building a proper IT infrastructure, even if it is capital intensive. Noncompliance of these banks with SWIFT's extensive and repeated security guidance for its customers was one of the contributing factors to their falling victims of cyberattacks. This should also serve as a lesson to Nepali banks and a warning to other financial institutions that generally hesitate to invest in IT infrastructure, and building a sound team that can frustrate criminal attempts from collapsing their entire system.

In summary, a series of successfully repeated attacks suggest hackers may have found ways into the messaging system the SWIFT member banks rely on to move money around the world. It is only a matter of time before we hear of more attacks if nothing is done to fortify networks. The immediate discovery of cybersecurity incidents like an attack is challenging due to the constantly changing threat environment.

COUNTERMEASURES

As seen in the case studies above, APTs are quite difficult to detect and tend to be complex in nature. Although the generic stages are the same, the exact vulnerability(ies) used in performing APTs could change from one to another. Therefore, a critical task when developing approaches to deal with threats would be to build systems that can respond to the constantly changing threat environments with agility and resilience. The author first reviewed the latest actions taken by SWIFT to strengthen defenses against cyberattacks. Then, a comprehensive framework was proposed to complement the SWIFT customer security control framework with the NIST risk management framework (RMF).

SWIFT Customer Security Program

SWIFT recently published an update to its Customer Security Program (CSP) and Customer Security Controls Framework (CSCF), a key aspect of the CSP (SWIFT, 2019a). The member institutions need to attest compliance with the CSCF v2019 by the end of 2019. SWIFT began enforcing these updated cybersecurity controls in more than 11,000 member institutions, partly responding to a series of cyberattacks between 2013 and 2018 and ultimately aiming to reinforce the security of the global banking system. According to one of the latest updates from SWIFT (2020a), more than 91 percent of customers (which represents over 99 percent of SWIFT’s traffic) attested to their compliance with controls mandated by SWIFT’s CSCF v2019.

The major goal of SWIFT CSP is to ensure the confidentiality, integrity, and availability of the systems that connect to the SWIFT network. It addresses a range of aspects including the protection of members’ local environments, preventing and detecting fraud in counterparty relationships, and working with members of the financial services industry to prevent future cyberattacks (Rut, 2019). Within the program, the CSCF is expanding to the 19 mandatory and 11 advisory security controls as of 2019, which are articulated around three overarching objectives: “Secure your Environment”, “Know and Limit Access”, and “Detect and Respond” (SWIFT, 2020b). There are three ways to comply with the SWIFT requirements: self-assessment, internal audit, or external audit (Koetsier & Diemont, 2018). Each type of compliance requires different degrees of independence, depth, and reliability of the attestation data.

Among the CSCF security controls, two important mandatory security measures are worth highlighting. First, it is mandatory for all member institutions to implement and enforce effective password policy and multi-factor authentication (MFA, mandatory controls

4.1 and 4.2) to prevent credential compromise. The use of hardware tokens is allowed, provided the member institutions properly manage and track the tokens (mandatory controls 5.2) during issuance, use, and storage to prevent unauthorized access to the SWIFT system. Furthermore, compliance can be achieved through the use of a management interface that facilitates assigning and tracking of each individual token (SWIFT, 2018). Secondly, a "secure zone" should be created by complying with all 30 controls collectively. "Secure zone" is where all local SWIFT infrastructure will reside, which isolates all local SWIFT systems from the wider enterprise network and restricts access and privileges on all systems within this secure zone.

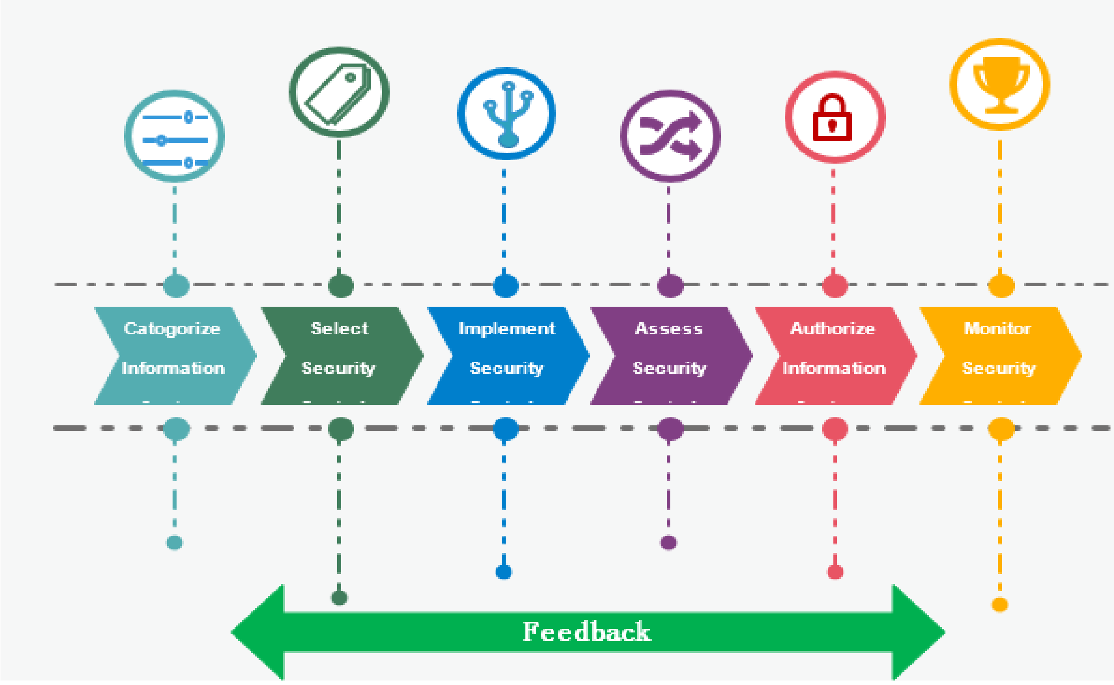
Applying The NIST RMF To Enhance Security Controls

Despite the enforcement of CSCF security controls in all SWIFT local systems, two major aspects of the "bigger picture" are omitted. First, the concept of "secure zone" only focuses on local SWIFT systems. However, a number of upstream systems and counterparties within financial institutions are out of scope of the CSCF (F-Secure, 2018). Another concern lies in a commonly observed trend that organizations treat CSCF as a stand-alone security framework serving only one purpose: to meet SWIFT security requirement (Koetsier & Diemont, 2018).

There is a pressing need for a SWIFT member institution to adopt a risk management mindset and conduct a comprehensive risk assessment of its networks (including both internal networks and external networks with counterparties) instead of focusing on "secure zone" only. In order to enable these SWIFT member institutions to better understand the nature of the threat landscape and implement security controls from a holistic perspective, the author recommend a risk management framework as another countermeasure. An organization within the banking ecosystem can approach the assessment of cybersecurity risk by integrating the National Institute of Standards and Technology (NIST) risk management framework (RMF) to complement its existing security control. The framework leads to a comprehensive and multi-level risk management process that can be implemented throughout an enterprise (NIST, 2018, 2019). The steps included in the RMF is demonstrated in Figure 2. Each of the six steps in the RMF is illustrated with more details and examples next.

Figure 2

Risk management framework (RMF)



1. *Categorize information systems.* The framework enables SWIFT as well as its customers to categorize their information systems based on the severity of a likely worst-case or adverse impact on their businesses. For instance, the impact level could be determined as low if the resulting loss has limited impact or moderate if the loss has a serious impact and high when losses have catastrophic impacts on the business' integrity. This also includes examining the enterprise network perimeter in order to identify which systems communicate with the SWIFT infrastructure and the administration procedures surrounding these systems.
2. *Select security controls.* Security controls would be selected from the outcome of the initial categorization of information systems and risk assessment using appropriate baselines determined by the banks' risks tolerance levels. Furthermore, as covered in the previous section, the SWIFT CSCF establishes a security baseline of mandatory and advisory controls for the entire user community (SWIFT, 2019a, 2020b). For instance, by selecting an MFA access control approach, the Bank of Bangladesh heist in 2016 could have been simply prevented because it would be more difficult for the hackers to obtain both login credentials and hardware tokens possessed by bank employees at the same time.

3. *Implement security controls.* After security controls are selected, they can then be integrated into an organization's security architecture and system using quality security engineering practices as well as employee trainings. Financial institutions need to develop a thorough plan regarding which permissions and actions privileged users should have access to and how an attacker could subvert or abuse these privileges. If these actions are necessary and cannot be prevented, an organization should follow the mandatory controls delineated in the CSCF closely. One challenge to follow the CSCF controls lies in the framework that defines the guidelines at a macro-level without details. Therefore, a strong focus should be placed on establishing controls on mail gateway, endpoint devices, and account control (F-Secure, 2018).
4. *Assess security controls.* The next step in the suggested framework guide requires SWIFT and the banks to test the effectiveness of the selected controls to find out if they were correctly implemented and working as intended. The controls surrounding each of these steps should then be assessed to confidently determine whether or not they would prevent such actions. This process should include security assessments of all controls along the path as well as establishing an understanding of the legitimate use cases for all components. For instance, in the NIC Asia Bank data breach, the pirated software was cited as one of the major contributing factors because it prevented the bank from upgrading software and building a robust IT infrastructure. If the bank followed the process of assessing security controls, installing and running pirated software on bank computers would not be allowed in the first place.
5. *Authorize information systems.* The framework provides the guidelines to support "consistent, well-informed, and ongoing security authorization decisions (through continuous monitoring), transparency of security and risk-related information, and reciprocity of security assessment results" (NIST, 2019). It emphasizes the importance of the official management decision given by a senior organizational official to authorize operation of a system and to explicitly accept the risk to organizational operations and assets based on the implementation of an agreed-upon set of security controls.
6. *Monitor security controls.* The controls implemented for the systems should be monitored continuously for signs of changes or attacks and regularly reassessed for effectiveness through an integrated enterprise-wide monitoring program. It is crucial that financial institutions continuously log all key servers within the environment and maintain visibility of servers and endpoint devices. For instance, NIC Asia Bank heist was caused by unintentional insider threats in which several employees accessed a

designated computer for SWIFT transfers and used it for other purposes. Implementing a continuously monitoring and detection system would have flagged such abnormal behavior and halted further activities on the designated computer. A network-based intrusion prevention system (IPS) could be installed for detection of any known attacks against SWIFT systems and prediction of some unknown attack patterns and trends.

CONCLUSION

Companies in the financial services industries keep remaining a high-profile target for cybercriminals and APT groups. A series of data breach cases targeting the SWIFT system presented in our paper corroborate that the international banking system is a lot more vulnerable to cyberattacks than previously understood. This study presents an opportunity for banks to embrace new security mindsets and change their risk management processes as it relates to information protection, data retention, and network architecture. For some banks, this change could be incremental, while those without the right infrastructure will have some considerable climb to make in a short period of time. Larger banks could have many of the requirements already in place, but also have a lot of complexity and legacy systems or processes to overcome while smaller banks with fewer resources, especially those in less developed countries, may face challenges implementing them on time.

To address the concerns of SWIFT network security and prevent potential cyberattacks targeting the financial services and insurance industries, the author suggests the SWIFT member banks to integrate the NIST risk management framework into the security controls mandated by the CSCF. The NIST RMF, which presents a holistic and a comprehensive risk management process, can be tailored as needed and applied throughout an enterprise as a practical and useful approach to fortify networks.

This study has been mainly focused on APT groups’ attack methods and patterns with most of the information obtained from secondary data, thus, leaving the study of insider actors outside the scope of the paper. It is noted that SWIFT or the affected banks have not made the full details publicly available on their sites due to concerns of reputational embarrassment. It could be interesting to consider these breaches from a different perspective, such as analyzing insider actors and their roles in the breaches if more relevant information would be made public.

Financial institutions need to interact and transact with various stakeholders and counterparties on a daily basis. Therefore, cybersecurity risks need to be managed together with other types of risk (e.g. operational, financial, and regulatory) and integrated into an organization’s existing risk assessment processes. It is crucial for financial institutions to make a collective effort in taking proper precautions to safeguard the banking and payment ecosystem. In addition to the NIST RMF, further research on a couple of other active response and defense frameworks would be beneficial, including the Diamond Model of Intrusion Analysis (Caltagirone, Pendergast, & Betz, 2013), kill chain modeling of APTs (U.S. Department of Defence, 2013), and corresponding response of the attacks.

Acknowledgement

The author gratefully acknowledges the valuable contributions of Ngbede Otowo. The author thanks the anonymous reviewers whose feedback and suggestions helped improve and clarify this manuscript.

REFERENCES

Al-Mahmood, S. Z. (2016). Hackers Lurked in Bangladesh Central Bank’s Servers for Weeks. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/hackers-in-bangladesh-bank-account-heist-part-of-larger-breach-1458582678

APSM. (2016). SWIFT Attackers’ MalwareLlinked to More Financial Attacks. *Asia Pacific Security Magazine*. Retrieved from https://www.asiapacificsecuritymagazine.com/swift-attackers-malware-linked-to-more-financial-attacks/

Baert, R. (2016). Following SWIFT Breaches, Scrutiny Intensifies. *Pensions & Investments, 44*(13). Retrieved from https://www.pionline.com/article/20160627/PRINT/306279982/following-swift-breaches-scrutiny-intensifies

Brenner, S. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *Journal of Criminal Law & Criminology*, *97*(2), 379–475.

Burne, K. (2017). North Korean Banks Under U.S. Sanctions Remain on Swift Network. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/north-korean-banks-under-u-s-sanctions-remain-on-swift-network-1489483805

Burne, K., & Sidel, R. (2017). Hackers Ran Through Holes in Swift's Network. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/hackers-ran-through-holes-in-swifts-network-1493575442

Butkovic, A., Mrdovic, S., Uludag, S., & Tanovic, A. (2019). Geographic Profiling for Serial Cybercrime Investigation. *Digital Investigation, 28*, 176-182.

Caltagirone, S., Pendergast, A., & Betz, C. (2013). The Diamond Model of Intrusion Analysis. Retrieved from http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Carnegie Endowment for International Peace, & BAE Systems. (2020). Timeline of Cyber Incidents Involving Financial Institutions. Retrieved from https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

CFO Innovation Asia. (2018). Malaysia's Central Bank Suffers Cyber Attack. Are You Vulnerable? Retrieved from https://www.cfoinnovation.com/risk-management/malaysia-s-central-bank-suffers-cyber-attack-are-you-vulnerable

Chilkoti, A., Gray, A., Mallet, V., McLannahan, B., & Scannell, K. (2016). Bangladeshi Job: How Cyber Heist Netted $81M. *Financial Times*, *3*. Retrieved from https://search-proquest-com.proxymu.wrlc.org/docview/1781667208?accountid=27975

F-Secure. (2018). Threat Analysis: SWIFT Systems and the SWIFT Customer Security Program. Retrieved from https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-threat-analysis-swift.pdf

Finkel, J. (2016). SWIFT Network Says Aware of Multiple Cyber Fraud Incidents. Retrieved from https://www.reuters.com/article/us-cyber-banking-swift-exclusive-idUSKCN0XM2DI

Koetsier, P., & Diemont, T. (2018). The Impact of SWIFT Security Requirements on the Banking Community. *KPMG: Insights*. Retrieved from https://home.kpmg/be/en/home/insights/2018/09/the-impact-of-swift-security-requirements-on-the-banking-communi.html

NIST. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (SP 800-37 Rev. 2). . Retrieved from https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

NIST. (2019). Risk Management Framework (RMF) Overview. Retrieved from https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

Riley, C. (2016). Hackers Stole Millions in Third Attack on Global Banking System. Retrieved from https://money.cnn.com/2016/05/20/news/swift-bank-attack-global-ecuador/index.html

Rut, M. (2019). The 2019 Update to the SWIFT CSP Customer Security Programme: Key Facts and Requirements. *OneSpan: Cybersecurity and Strong Authentication*.

Retrieved from https://www.onespan.com/blog/2019-update-swift-csp-customer-security-programme-key-facts-and-requirements

Schwartz, M. J. (2016a,). Another SWIFT Hack Stole $12 Million. Retrieved from https://www.databreachtoday.com/another-swift-hack-stole-12-million-a-9121

Schwartz, M. J. (2016b). Report: Bangladesh Probes 2013 Bank Hack via SWIFT. Retrieved from https://www.databreachtoday.com/report-bangladesh-probes-2013-bank-hack-via-swift-a-9143

Schwartz, M. J. (2016c). Vietnamese Bank Blocks $1 Million SWIFT Heist. Retrieved from https://www.databreachtoday.com/vietnamese-bank-blocks-1-million-swift-heist-a-9105

Sharma, R. (2017). Cyber Threat Corners Banks. *The Kathmandu Post*. Retrieved from https://kathmandupost.com/money/2017/12/01/cyber-threat-corners-banks

SWIFT. (2017). SWIFT Explores Blockchain as Part of its Global Payments Innovation Initiative. Retrieved from https://www.swift.com/news-events/press-releases/swift-explores-blockchain-as-part-of-its-global-payments-innovation-initiative

SWIFT. (2018). Interface Certification – Security Conformance Requirements. Retrieved from https://www.swift.com/resource/security-conformance-requirements-v2019-certified

SWIFT. (2019a). SWIFT Customer Security Controls Framework v2019. Retrieved from https://www.swift.com/myswift/customer-security-programme-csp_/security-controls/2019

SWIFT. (2020a). Customer Security Programme Updates - March 2020. Retrieved from https://www.swift.com/file/67941/download?token=eMlyvugL

SWIFT. (2020b). Customer Security Programme (CSP): Reinforcing the Security of the Global Banking System. Retrieved from https://www.swift.com/myswift/customer-security-programme-csp/security-controls?tl=en#topic-tabs-menu

Symantec. (2016). SWIFT Attackers' Malware Linked to More Financial Attacks. *Global Security Magazine*. Retrieved from https://www.globalsecuritymag.fr/SWIFT-attackers-malware-linked-to,20160527,62449.html

Tripathy, D. (2018). India's City Union Bank CEO Says Suffered Cyber Hack via SWIFT System. Retrieved from https://www.reuters.com/article/us-city-union-bank-swift/indias-city-union-bank-ceo-says-suffered-cyber-hack-via-swift-system-idUSKCN1G20AF

U.S. Department of Defence. (2013). Joint Publication 3-60 Joint Targeting. Retrieved from https://www.justsecurity.org/wp-content/uploads/2015/06/Joint_Chiefs-Joint_Targeting_20130131.pdf

Vu, T., & Burne, K. (2016). Vietnam's Tien Phong Bank Targeted in Bangladesh-Like Cyberattack. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/vietnamese-bank-says-it-was-target-of-attempted-cyber-heist-1463405095

Yin , R. K. (2014). *Case Study Research: Design and Methods* (5th. ed.). Thousand Oaks, CA: Sage Publications.