CLEIMUN20

"Diplomacy in a Challenging Global Environment"

A Research Report

COMMITTEE: Economic and Environmental Committee (ECOE)

QUESTION OF: The Protection Against Cyber Attacks on Monetary Transfer Systems

AUTHOR: Evan F. Cihlar & Diana Lucic

Introduction and Background

Recently the International Monetary Fund (IMF) published Working Paper "Cyber Risk, Market Failures, and Financial Stability" (WP/17/185). This working paper concluded that cyber risk has emerged as a significant threat to the global financial system. In accordance with these reports, all types of banks, monetary transfer services, and third party payment processors have seen their systems compromised. Financial market districts have been attacked and the effects from website downtimes (times when a website is unavailable due to code failure or hacks) and service disruptions due to successful attacks have the potential to be widespread and systematic without being able to pin-point the source of the problem. Many of these cyber-attacks evolve quickly and are highly dynamic by nature, which results in complications in risk assessment. Just in one year alone, successful attacks have already "resulted in data breaches in which thieves gained access to confidential information and stole $500 million from the Coincheck cryptocurrency exchange." (SOURCE) In accordance with Christine Lagarde, an IMF staff modeling exercise estimated that "annual losses to financial institutions from cyber-attacks could reach up to $350

billion USD" which results in the erosion of bank profits and potentially threatening financial stability. Surveys have consistently shown that risk managers and other executives at financial institutions worry most about cyber-attacks than eminent geopolitical risks or recent revelations such as Brexit.

Why are Banks Vulnerable?

The financial sector of any nation plays a crucial role in intermediating funds in political and societal stability and prosperity. A simplistic look on the outcomes of the euro crisis in countries such as Portugal, Ireland, and Greece is enough evidence to understand the criticality of the financial sector stability. That is exactly the reason why banks are attractive targets and hence vulnerable to cyber-attacks. The greatest vulnerability highlighted by the IMF Working Papers is that many financial institutions ineffectively use and manage Secure Socket Shell (SSH) keys. An SSH key enables ongoing automatic connections from one system to another, often without the use of a second authentication factor. These keys provide a way for computers to establish secure connections on an unsecure network. These now-secure network connections allows for a persistent trust relationship, one that cyber criminals and malicious insiders are eager to access and misuse.

A recent study in 2017 studied how well 100 financial organizations in the U.S., U.K., and Germany implemented security controls for SSH keys. The results show that most financial service organizations are not prepared to protect against SSH-based attacks, with fewer than half following industry-best practices for securing SSH keys. In accordance with this survey, SSH keys are routinely untracked, unmanged, and unmonitored. In fact, financial service

organizations do not set policies and controls that limit how SSH keys can be used, managed, and monitored. The findings of both studies shed light on the fact that financial institutions have several millions of SSH keys - and that they have no provisioning and termination processes in place for key-based access. Financial institutions do not have records of who provisioned each key and for what purpose, and they allow their system administrators to change permanent SSH key-based transactions without policies, processes, or oversight from financial institutions.

What Makes SSH Keys and Cyber-Attacks Hard to Regulate?

Imagine a time where all of the internet sites of major banks are malfunctioning. ATMs are not working, and the said banks' internal accounting systems are going haywire. Millions of people are being affected, and some have become the victim of a cybercrime. This briefly describes what *could* happen during a cyber-attack on a monetary transfer system, however, since each attack is unique in nature, anything is possible.

When a cyber-attack occurs, government officials usually debate whether such an attack deserves military intervention. Even if policy makers decided that military intervention was necessary, 95 percent of the time governments are unable to designate where the attack originated. Without being able to attribute the attack, or if there was any uncertainty about who was responsible, it would be very hard to strike back.

Unlike conventional attacks, cyber-attacks can be difficult to attribute with precision to specific actors. If a country strikes back with military force with weary forensics, the retaliation will have unnecessarily and inadvertently started a war. Even in cases where an attack is linked to one specific country, it could be hard to know for sure whether it was directed by the Russian

government. This is due to state-sponsored cyber attacks that rely heavily on third parties to develop their cyber weapons and conduct their attacks. This offers the state many benefits - deniability being one of them, but if also offers them less control over what their cyber warriors actually do - created a so-called "principal-agent problem." In other words, an attack that originates from within the Russian cyber-world might be the work of the Kremlin - or it might not. This further complicates a nation's choice of response. Some advisors might push for a cyber counter-attack that would inflict an equal amount of damage on the guilty party, but this is not always possible. If the perpetrator is a party like North Korea, then there is no equivalent financial system to target. Some countries may want to use conventional military weapons lie a cruise missile, but a strike like that would clearly risk serious escalation of the conflict. Even if a state knows who sponsored or executed the attack, there is a level of caution due to unknown consequences, unlike conventional military attacks where damage can be controlled in some form. Cyber weapons do not operate like missiles or tanks as they attack underlying network or computer systems. The possibility of unexpected effects in the cyber world is much greater and unknown.

Combating State-Sponsored Cyber-Attacks

A 2017 study concluded that 23 of 94 cyber attacks on banks and monetary transfer systems were sponsored by different countries. A majority of the attacks were sponsored by the nations of Iran, Russia, China, and North Korea. Because of these attacks, the U.S. Federal Reserve Chairman, Jerome Powell, and Japan's central bank chief Haruhiko Kuroda earlier this year said cyberattacks are currently the largest risk to financial institutions. In January, state-based hackers

from North Korea infiltrated the Bank of Chile's ATM network and siphoned off $10 million USD. Last year, Nork Koreans hacked the systems of India's Cosmos Bank and siphoned off nearly $13.5 million through simultaneous withdrawals across 28 countries. The ubiquity of reliance on the Internet for doing business, combined with lax cybersecurity processes, has created the opportunity for state actors to achieve foreign policy objectives via cyber-attacks. Law enforcement performs an essential role in achieving a nation's cybersecurity objectives by investigating a wide range of cyber crimes, from theft and fraud to child exploitation, and apprehending and prosecuting those responsible. So the question still remains, how does the United Nations combat these state-sponsored cyber-attacks and cyberwarfare?

Cyber-Attacks on Developing Nations

Unfortunately, cybercrime is a growing problem in developing countries, where customers often conduct financial transactions over insecure mobile phones and transmission lines that are not designed to protect communications. In Africa, the number of successful attacks against the financial sector doubled in 2017, with the largest losses hitting the mobile financial services sector. Digital financial services (DFS) providers must adopt stronger cybersecurity incidents and are at various stages of implementing cybersecurity measures in their organizations. While they are still most concerned about better-known types of fraud in DFS, such as malicious employees and agents, they are seeing themselves confronted with four types of risks emerging in cyberspace.

Social Engineering

In a social engineering attack, the criminal tricks the victim into revealing sensitive information or downloading malware, which opens the doors to physical locations, systems, or networks. The idea is to exploit a vulnerable person rather than a vulnerable system. DFS providers from Ghana, Kenya, Tanzania, Uganda, and Zambia reported that fraudsters had duped their employees into sharing their user login details and then accessed corporate information systems.

Most DFS providers consider careless or unaware employees to be a major factor in their organization's cyber-risk exposure, but DFS customers are a vulnerability, too. The newly banked are more likely to fall victim to this type of scheme because of their limited experience with digital fraud. Providers can guard against social engineering through regular awareness and education campaigns, and it is also important to appropriately manage user access rights, introduce system log monitoring processes and require two individuals for completing sensitive transactions (i.e., maker-checker controls).

Data Breaches

Using malware or social engineering, hackers can gain access to valuable information, such as credit card numbers, customer personal identification numbers, login credentials, and government-issued identifiers. Weak patch management, legacy systems, and poor system log monitoring were cited as the main reasons why DFS providers' systems are susceptible to hacking attacks.

In addition to financial losses that can result from a data breach, providers' reputation and customers' trust are at risk. In 2017, thieves breached a DFS provider's systems in Kenya and stole hundreds of customers' identities. The fraudsters accessed sensitive customer information,

such as account types and last transactions, which allowed them to pass as legitimate customers and apply for loans in the victim's name. To protect against these breaches, DFS providers need to regularly update their systems and software, patch their systems, use strong encryption for data at rest and in transit and implement 24/7 system log monitoring.

Outages and Denial of Service Attacks (DOS)

DFS providers sometimes experience system outages during routine system upgrades or patches. Earlier last year, an upgrade gone awry lef DFS users in Zimbabwe without access to their digital money for two days. Systems unavailability can also be the result of a cyber-attack. For example, in 2017, M-Shwari customers in Kenya were left without access to their savings and loan products for five days, and after the outage, several found inconsistencies in their account balances. The most frequent form of attacks that cause system unavailability are denial-of-service attacks.

In a denial-of-service attack, cyber criminals overwhelm a server by flooding it with simultaneous access requests, depriving legitimate users of access to the system. In most cases, the objective is to harm the business. Yet, in some cases, cyber criminals have launched DOS service attacks to distract attention from an attempt to gain access to the system. Effective countermeasures include continuous network traffic monitoring to identify and detect attacks while allowing legitimate traffic to reach its destination, a solid and tested incident response plan that allows for quick reaction in an emergency and strong change management processes and disaster recovery planning.

Third-Party Threats (TPT)

DFS providers rely on third parties for a range of services, such as mobile network, information technology and data storage solutions. Sometimes, these providers misuse their system rights to access confidential customer information that they can sell or use for social engineering. Also, a third party that handles sensitive information may not have appropriate safeguards against cyberattacks, putting at risk the confidentiality and integrity of the DFS provider's customer data. To address third-party threats, DFS providers should implement due diligence reviews of current and potential partners, including reviews of their security policies and practices.

Past Efforts to Solve the Problem

In 2017, the United Nations Security council unanimously adopted resolution 2341, the Council encouraged all States to make collective and syncronized efforts to to raise awareness and expand knowledge of challenges posed by cyber terrorist attacks on financial infrastructure, so as to be better prepared for such attacks. Additionally, in 2012, UN Secretary-General Ban Ki-moon appointed the group of 15 experts from the five permanent members of the UN Security Council plus Argentina, Australia, Belarus, Canada, Egypt, Estonia, Germany, India, Indonesia, and Japan to carry out a mandate from the UN General Assembly to "study possible cooperative measures in addressing existing and potential threats" related to the use of information and communications technologies (ICTs). More individual efforts have been made independently by independent United Nations member states.

Possible solutions

Though, many efforts have been made to solve this issue, none have been completely effective in solving the issue at hand, as it is still, currently a prevalent issue. Individual nations can create more secure systems and security measures. Additionally, an international database, that records all suspicious behavior towards and from either third party or international monetary transfer systems could potentially solve the issue at hand. In order for the issue to be solved, the council must collaborate effectively to create an effective solution. All nations must work together while keeping in mind the principle of national sovereignty and following their nation's policies.

Cyber-attacks on monetary transfer systems are a serious threat to one of the most crucial networks in the world today. Combating these attacks can be challenging, but necessary to fight against evil powers and states. Although all of the information you will need to debate this topic has been outlined for you in a straightforward and unbiased perspective, it is up to all delegates to solve the crisis that the world is facing every day.

Works Cited

"Arms Control Today." *The UN Takes a Big Step Forward on Cybersecurity | Arms Control Association*, www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity.

"Arms Control Today." *The UN Takes a Big Step Forward on Cybersecurity | Arms Control Association*, www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity.

"Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341 (2017) | Meetings Coverage and Press Releases." *United Nations*, United Nations, www.un.org/press/en/2017/sc12714.doc.htm.