eastnets

Fall 2019

Eastnets Survey:

How Banks are Combating Cyber Attacks on Their SWIFT Payments

By Deya Innab
Deputy CEO
Eastnets

Eastnets Survey:
How Banks are Combating Cyber Attacks on Their SWIFT Payments

Summary

Two-thirds of the banks surveyed said they had experienced an increasing number of cyber attacks since 2016 related to their SWIFT payments, and there is strong evidence that banks are not adequately preparing themselves to combat the threat. In addition to various high-profile incidents of bank theft using the SWIFT messaging network, an Eastnets' survey conducted in July found that cybercriminals have targeted more than four-in-five banks since 2016. Banks indicated that the problem has been getting worse. Common solutions, namely SWIFT's Customer Security Program, are helping but banks must do more. Banks have various practices and tools at their disposal to harden their security posture. We discuss what these are and reveal the survey findings.

12 Key Findings

1. Since 2016, more than 4 out of 5 banks in the U.S., Europe, Gulf Cooperation Council (GCC) countries, and Asia-Pacific have been targeted by cyber criminals attempting to use the SWIFT messaging network to fraudulently transfer money across country borders. The rate rises to 90% in GCC and 100% in Asia-Pacific countries.

2. The vast majority (84%) of these attempts were cyber-based attacks committed by hackers, and in all regions surveyed at least 80% of these attacks were done through computer hacking. Moreover, only two-fifths of banks are "very confident" they have detected all cyber SWIFT fraud attempts since 2016.

3. Of the banks that have been targets of SWIFT cybercrimes, two-thirds said such attempts have been increasing since 2016. Yet there is evidence that banks are not taking the threat seriously enough.

4. Smaller financial institutions (with assets from USD $1 billion to $10 billion) appear to be subject to more of the rise, with 88% reporting an increase in SWIFT fraud attempts since 2016. Yet the majority of banks with more than $100 billion in assets (60%) also say such crime has increased.

5. Many banks are struggling to get their various internal departments affected by SWIFT cyber fraud to work together to fight the threat. Only 20% said their people collaborate "very strongly" across functions to mitigate SWIFT fraud, and the survey group as a whole said that getting departments to collaborate was a top challenge.

6. In addition to collaboration, other top challenges banks face around SWIFT fraud include dealing with business email compromise and educating customers about how to reduce the risk.

7. About 1 out of 7 banks say that bank insiders have been involved in SWIFT fraud attempts since 2016, with Asia-Pacific banks reporting the highest percentage of insider involvement (17%).

8. Current solutions are often falling short. Some 80% of banks believe SWIFT's Customer Security Program (CSP) adequately protects them, and 70% have software designed to prevent SWIFT fraud. Yet most said they have been attacked, revealing weaknesses in their defenses.

9. About one in five banks lacks basic policies and practices for combatting SWIFT cyber fraud such as enforcing the least-privilege principle, restricting access to the SWIFT interface, implementing user-behavior analytics, and preparing disaster recovery of the SWIFT messaging interface.

10. Banks need a comprehensive program that includes enforcing good policies and practices, deploying defensive IT systems, implementing autonomous fraud prevention, and using artificial intelligence and machine learning technologies to track transaction and user behavior.

11. In comparing "leaders" (banks that say they have been effective at addressing SWIFT cyber fraud) with "laggards" (banks reporting less effectiveness at dealing with it), a number of differences show up. Leaders were more likely to use behavioral analytics software on their IT users, conduct attack simulations, and have procedures to address reputational damage from attacks. They are also more likely to have strong cross-functional collaboration in setting controls to protect against SWIFT fraud, and on average spend 75% more to reduce the risk.

12. New banking trends may make it easier for criminals to commit fraud against bank payments in the near future, and harder for banks to stop them unless they take corrective measures.

Introduction: Many Banks Aren't Sufficiently Prepared for the SWIFT Fraud Menace

Since it replaced telex machines in 1977 as a way for banks to communicate instructions on cross-border payments, the SWIFT messaging platform has become a lynchpin of the global payment system. SWIFT (short for the Society for Worldwide Interbank Financial Telecommunication) is a vital tool for banks and their customers around the world.

This July, more than 11,000 financial institutions in over 200 countries and territories worldwide were using the SWIFTNet messaging platform, issuing more than 15 million messages on payments daily.[1] The Belgium-based cooperative is fundamental to global commerce, facilitating more than $40 trillion in cross-border payments in 2018.[2]

However, the SWIFT system has been under concerted attacks in recent years. A series of high-profile cyber-related robberies has called attention to the problem of SWIFT payment-transfer fraud, in which criminals issue fraudulent payment transfer requests. These robberies — committed remotely, using keystrokes rather than force, and often involving many millions of dollars — have alarmed bankers across the globe. (See Sidebar, "The Iceberg's Tip: Publicly Known Cases of Swift Fraud.")

Yet these publicly known cases appear to represent just a small fraction of the problem. Banks

[1] SWIFT web page, https://www.swift.com/about-us
[2] SWIFT press release, Feb. 28, 2019, on total value of payments made via SWIFT gpi in 2018. https://www.swift.com/news-events/news/swiftgpi-reaches-major-adoption-milestone-surpassing-40-trillion-in-sent-payments

are generally under no obligation to reveal publicly when they have been attacked. As such, SWIFT fraud crimes frequently remain opaque, obscuring details of the problem and the identity of the perpetrators.

A growing body of evidence, including a recent Eastnets survey unveiled in this report, has begun to shed new light on how common SWIFT fraud attacks are, and how prepared — or frequently unprepared — banks are to combat them.

At least seven hacking collectives are actively seeking to perpetuate fraud on banks' SWIFT payments, says one cybersecurity expert, and most attacks go unreported, according to a 2018 report.[3]

According to a recent news article, a confidential United Nations report alleges that North Korea has amassed some $2 billion for its weapons of mass destruction program using "widespread and increasingly sophisticated" cyberattacks against banks and cyber-currency

The Iceberg's Tip: Publicly Known Cases of Swift Fraud

Eastnets' secondary research on SWIFT fraud since 2016 found at least 14 cases that led to more than USD $380 million in combined losses. Nine cases were in the Asia-Pacific, three were in Eastern Europe or Russia, and two were in South American countries.

Most famously, in 2016 hackers allegedly from North Korea used malware to break into Bangladesh Bank's IT systems. Over a holiday weekend, they used the SWIFT network to issue nearly three dozen transfers requests, amounting to $951 million, to the Federal Reserve Bank of New York. Five of the requests were executed, resulting in more than $101 million in transfers.

Although about $35 million has been recovered, the rest was laundered through Philippines casinos.[5] [6] If strange and misspelled transfer requests had not raised suspicions, the losses may have been far worse, according to one report. [7]

In an even larger case, junior bankers at a branch of the Punjab National Bank (India's second-largest state-run lender) used the SWIFT network to issue payment instructions amounting to $1.8 billion.[8] The transfers went on for years before they were detected. There are many other cases. In 2017, hackers took $60 million from the Far Eastern International Bank in Taiwan, reportedly by using malware to get credentials.[9] The same year, hackers stole about $6 million from a Russian bank via SWIFT. [10]

[3] Kvantor, "Top 5 biggest SWIFT hacks," Medium.com, May 1, 2018, Accessed at https://medium.com/@kvantorcom/top-5-biggest-SWIFT-hacks-52fca78145c

[4] Michelle Nichols, "North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report" Reuters, Aug. 5, 2019, Accessed at https://www.reuters.com/article/us-northkorea-cyber-un-/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

[5] "Exclusive: NY Fed first rejected cyber-heist transfers, then moved $81 million," Krishna N. Das, Jonathan Spicer, Reuters.com. June 3, 2016. Accessed at https://www.reuters.com/article/us-cyber-heist-bangladesh-exclusive-idUSKCN0YQ041

[6] "Bangladesh sues Philippine bank over cyberheist at New York Fed," Jonathan Stempel, Reuters.com, Jan. 31, 2019 Accessed at https://www.reuters.com/article/us-cyber-heist-bangladesh/bangladesh-sues-philippine-bank-over-cyberheist-at-new-york-fed-idUSKCN1PQ3BG

[7] "In Bangladesh Cyberheist, Strange Requests, Odd Misspellings and Little Scrutiny by Fed," Katy Burne, Wall Street Journal, Aug. 15, 2016, Accessed at https://www.wsj.com/articles/in-bangladesh-cyberheist-strange-requests-odd-misspellings-and-a-lack-of-scrutiny-by-fed-1471192772

[8] Deborah D'Souza, Punjab National Bank $1.8B Fraud Raises Questions About SWIFT Security, Investopedia, Feb. 20, 2018. Accessed at https://www.investopedia.com/news/punjab-national-bank-fraud-should-SWIFT-be-less-vulnerable-more-responsible/

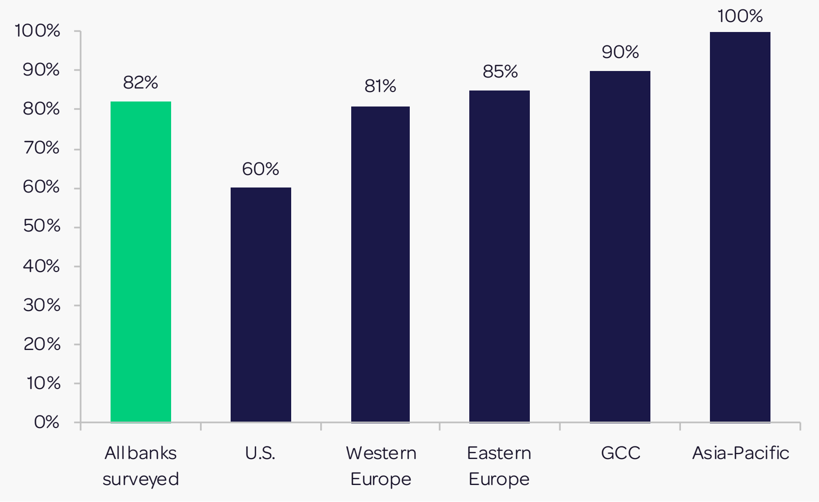
[9] Iain Thompson, "Hackers nick $60m from Taiwanese bank in tailored SWIFT attack," The Register, Oct. 11, 2017, Accessed at https://www.theregister.co.uk/2017/10/11/hackers_SWIFT_taiwan/

[10] "Hackers stole $6 million in Russia bank attack via SWIFT system," Deutsche Welle, Feb. 16, 2018. Accessed at https://www.dw.com/en/hackers-stole-6-million-in-russia-bank-attack-via-SWIFT-system/a-42616207

Exhibit 1

Four-in-five banks have been targeted by SWIFT fraud attemps

% of banks that have been subject to cyber attempts at SWIFT payment fraud (whether or not they led to financial losses)



> “More than four out of five banks (82%) said they have been targeted by criminals attempting to use the SWIFT network to fraudulently transfer money.”

Heists committed using the SWIFT payment messaging network, however, often remain opaque. Most cases are not revealed publicly, and are kept quiet even within financial institutions.

Through Eastnets' work as first responders in investigating fraud, we are aware of various SWIFT fraud attempts at banks that have taken place at night but by morning were handled, with banking services restored. In these cases, very few individuals outside of those banks' top management were aware of the attacks.

The Eastnets survey, which polled 200 banks from Asia, Europe, the Middle East and the United States in the summer of 2019, found that cyber-criminal attempts to defraud the SWIFT network are extraordinarily common. The survey also identified several worrisome trends on how banks are responding to the threat.

More than four out of five banks (82%) said they have been targeted by criminals attempting to use the SWIFT network to fraudulently transfer money. The rate rises to 90% in Gulf Cooperation Council (GCC) countries, and 100% in our Asia-Pacific sample. (See Exhibit 1.)

The vast majority (84%) of attempts were cyber-based attacks committed by hackers.

About one-in-seven (14%) of SWIFT fraud attempts involved insiders; this number rises to 17% in the Asia-Pacific region. (See Exhibit 2.) While this may not seem like a high percentage, it nonetheless should be worrisome for banking leaders who believe SWIFT fraud is never committed from within. The incidence of insider involvement is evidence that some banks have weak internal controls over SWIFT payments.

Meanwhile, 67% of banks surveyed said the crime has been on the rise since 2016. Smaller institutions, with assets from $1b to $10b, appear to be bearing the brunt of the rise, with 88% reporting an increase. Banks in the Asia-Pacific region were far more likely (35%) than average (24%) to say SWIFT fraud attempts are “increasing substantially.”

SWIFT fraud is, by its nature, a problem that demands cross-functional collaboration among a bank's IT, cyber-security, risk management, client relationship managers, finance and other departments. Yet banks are struggling to get these departments working together to fight the threat.

Exhibit 2

In 1 out of 7 cases, the perpertator is within

Please estimate the percentage of cyber-related SWIFT payment fraud attempts at your bank since 2016 that involved insiders (employees, contractors working for your bank, etc.)? (164 surveys)

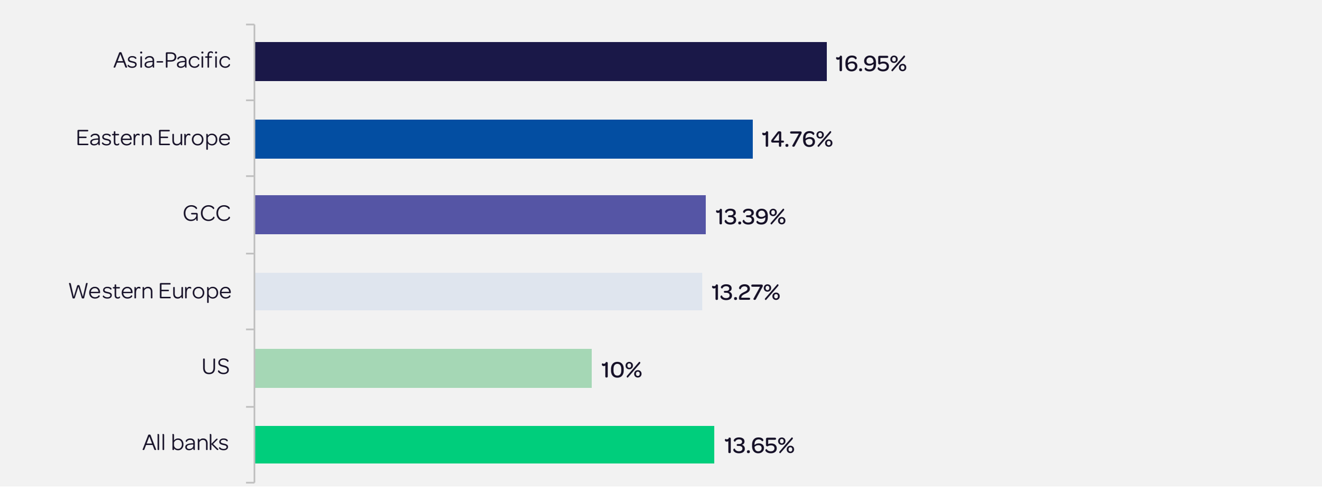


Exhibit 3

Cross-functional collaboration to reduce cyber fraud on banks' SWIFT payments could be stronger

How strongly do people in the functions responsible for mitigating SWIFT payment fraud collaborate in establishing effective controls to protect against bank's SWIFT payments? (200 surveys)

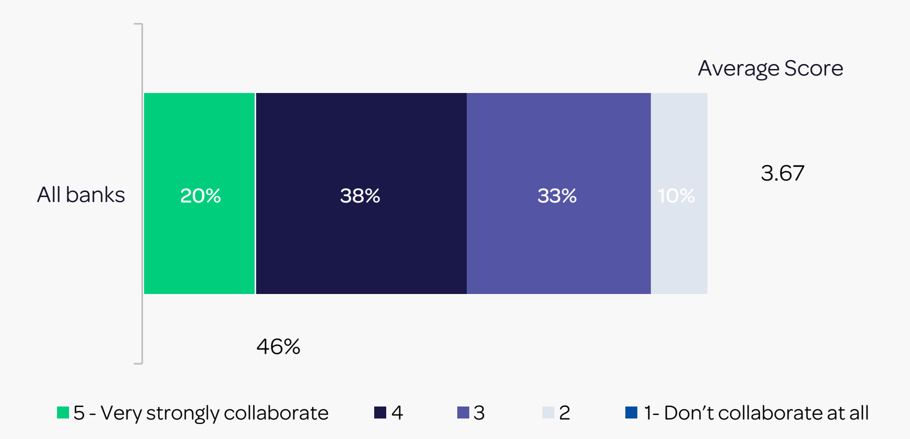
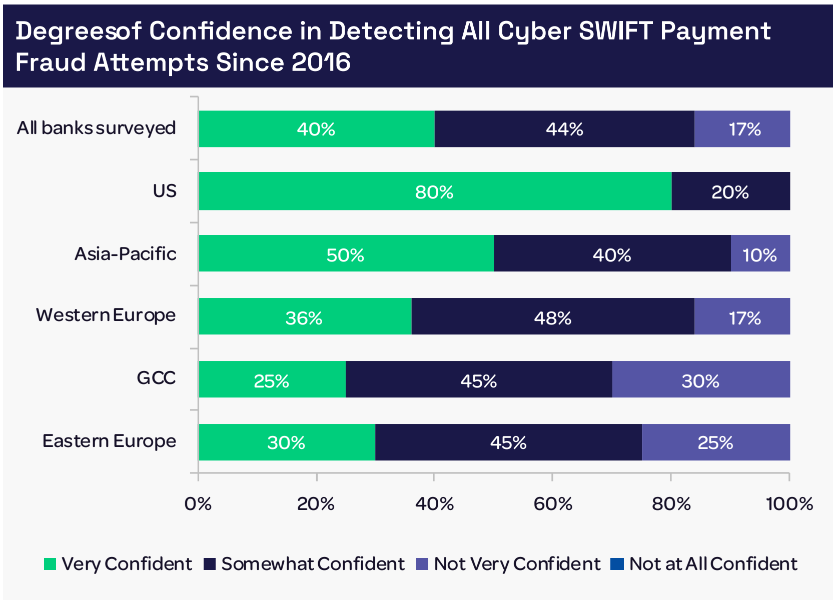


Exhibit 4

Banks lack strong confidence in detecting all attempts



Only 20% said their people collaborate "very strongly" across functions to mitigate SWIFT payment cyber fraud by establishing effective controls. Some 43% reported average to weak collaboration. (See Exhibit 3.)

This lack of collaboration renders banks more vulnerable. It is among the biggest risk factors behind the high level of insider involvement in fraud attempts. It raises questions about how well banks are prepared for the next wave of SWIFT attacks.

Perhaps most worryingly, banks are uncertain about whether they can reliably detect the threat. Only 40% were very confident they had detected all cyber SWIFT-payment fraud attempts since 2016. This percentage rises to 80% in the U.S. and falls to 30% in Eastern Europe and 25% in GCC. Most said they were either somewhat confident (44%) or not very confident (17%) that they had detected all SWIFT cyber fraud attempts. (See Exhibit 4.)

Our study also identified what appears to be a disconcerting lack of apprehensiveness in face of the threat.

Banks ranked management's level of concern over SWIFT fraud below business email compromise fraud, credit card fraud and online banking fraud. This could signal inadequate awareness of how widespread, serious and complex SWIFT fraud is, and how inadequate commonly deployed defenses are.

Given that SWIFT transactions involve correspondent relationships, this lower level of concern should be alarming to all banks. Even the best-performing banks could find themselves at risk due to the vulnerabilities of poorly prepared partners.

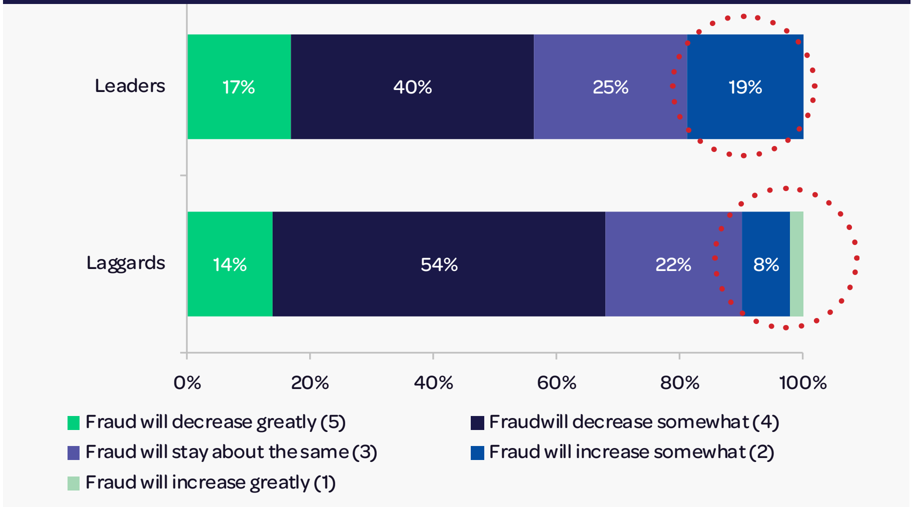
Likewise, with the exception of the some of the best-performing banks, we found that banks overall are blasé about how the threat would impact them in the future. Most (69%) expect SWIFT fraud to decline in the coming three years. Only 17% expect it to stay the same.

Yet when we compared the views and practices of leaders (who reported "great success" in addressing cyber-related SWIFT fraud) vs. laggards (those who characterized their success as average or below), many differences can be seen.

Exhibit 5

Both leaders and laggards see SWIFT fraud declining over the next 3 years, but twice as many leaders see it rising

Which of the following statements best fits your view on SWIFT cyber payment fraud attempts over the next three years? (200 surveys)



Leaders are more than twice as likely (19%) as laggards (8%) to believe that SWIFT fraud attempts in the next three years will increase greatly. (See Exhibit 5.)

SWIFT fraud has enormous impacts on all financial institutions. In addition to financial losses that can far outstretch conventional thefts, banks face reputational risk and the potential for lost business.

Obviously, bank customers and partners alike are not eager to conduct business with an institution whose assets may appear to be unsafe. Moreover, every financial institution that uses the SWIFT system is a potential victim, regardless of size, level of sophistication or maturity. The 2016 Bangladesh Bank case involved deposits at the Federal Reserve Bank of New York, one of the world's most advanced financial institutions.

No matter whether a bank has been targeted, SWIFT fraud introduces substantial new compliance and security costs.

Furthermore, banks are increasingly "de-risking" by eliminating counterparties when they are not confident in their security protocols. Due-diligence costs associated with high-risk counterparties can reach as high as $50,000 per year, according to SWIFT.[11] De-risking means lost business, for both the institution and the former counterparty. It also makes it more difficult to conduct business in locations where de-risking is prevalent.

Why SWIFT's Customer Security Program (CSP) is Not Sufficient

Following the high-profile cyber theft against Bangladesh Bank, SWIFT has taken several important steps to combat fraud that corrupts its messaging system. It has heightened collaboration with industry experts, threat-intelligence teams and incident-response teams. In addition, it has created a customer security intelligence team to "investigate customer incidents and share back anonymized information with the community." [12]

[11] "The Decline in Access to Correspondent Banking Services in Emerging Markets" World Bank, 2018, p. 37, Accessed at http://pubdocs.worldbank.org/en/786671524166274491/TheDeclineReportlow.pdf
[12] "Three years on from Bangladesh - Tackling the adversaries" Aug. 22, 2019, Accessed at https://www.SWIFT.com/resource/-three-years-bangladeshtackling-adversaries

The backbone of SWIFT's efforts is its Customer Security Program (CSP). SWIFT refers to it as "a concerted effort to drive industry-wide collaboration against the cyber threat and to help reinforce and safeguard the security of the wider ecosystem."[13] To use the SWIFT network, banks must self-attest that they comply with its mandatory controls. (It should be noted that only a very limited number of institutions are chosen for compliance inspection, so it is impossible to know what portion of banks actually abide by the standard.)

Many banks we know believe that to have an adequate defense against SWIFT fraud, they simply have to follow the measures prescribed by CSP. In fact, our survey found that 80% of banks believe this to be the case. This notion is risky, however. To the extent that some banks are complacent about the threat of such fraud, the belief that CSP alone will protect them is misconceived.

Surely, CSP has helped many banks deal better with SWIFT cyber fraud by introducing security controls and implementation guidelines, and by requiring banks to self-attest their compliance with them.

Yet CSP is not a comprehensive solution, and does not, on its own, effectively protect financial institutions. CSP is more of a framework than an actual solution. For instance, it mandates securing the zone where SWIFT transactions take place. But given the increasingly open and rapid nature of banking, it is growing more and more difficult to infallibly secure this zone.

CSP calls for "application blacklisting" to prevent unsafe applications from being introduced into the secure zone. In our experience, this is good but not enough. We also suggest "application whitelisting" so that only administrator-approved applications can be executed.

The latter practice lets administrators review software applications prior to installation, which can dramatically reduce the chances of introducing malicious applications that have not yet been discovered to be malicious.

In addition, to prevent the execution of arbitrary software code, CSP merely requires typical malware protection software — a host-based in trusion prevention system that notifies administrators.

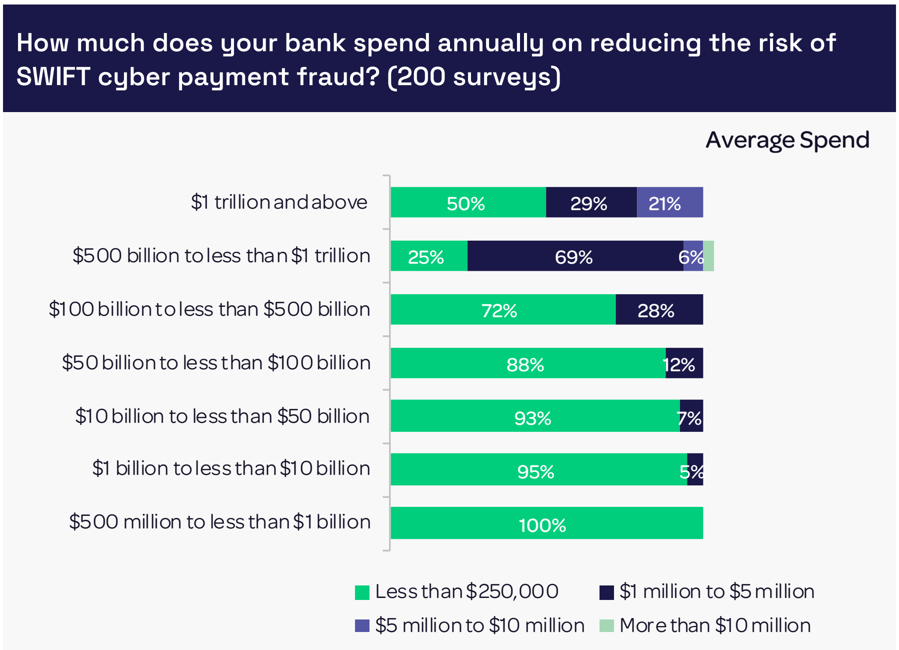
This software only has to be updated daily and run periodically. In Eastnets' experience, this is inadequate. In 100% of the cases that we have investigated, the institution had multiple anti-malware applications installed on their compromised systems. Those systems still failed to detect SWIFT cyber fraud attempts.

As well, we believe CSP measures are largely based on combatting methods that cybercriminals used in the past. But those methods don't necessarily protect banks against new hacker fraud techniques. Therefore, CSP does not establish an impenetrable fortification against cyber criminals.

[13] "Three years on from Bangladesh - Tackling the adversaries" Aug. 22, 2019, Accessed at https://www.SWIFT.com/resource/-three-years-bangladeshtackling-adversaries

Exhibit 6

Big banks spend lots more to reduce risk (which works)



Meanwhile, despite the widespread trust in CSP, cyber threats have persisted, and for good reason. Criminals increasingly see SWIFT fraud as an effective, low-risk way to perpetrate thefts. We believe they will continue to search for new and innovative ways to exploit the inherent weaknesses of the modern open banking system. Or as SWIFT has stated, "Sending fraudulent high-value payment instructions can lead to large rewards."[14]

How Leading Banks Reduce SWIFT Fraud

As is nearly always the case in life, money matters in the fight against SWIFT fraud. The banks we surveyed are spending money to reduce the risk of SWIFT cyber payment fraud, with the average per-bank spend of $850,000 annually for those between $1 billion and $500 billion in assets, and $2.6 million for those of $500 billion or more in assets. (See Exhibit 6.) Additionally, leaders in fighting SWIFT fraud outspend laggards by 75% annually — $1.4 million per bank (leaders) vs. $800,000 for the average trailing bank.

While money tends to matter, there is no one solution that foils criminals while maintaining the speed and openness of the modern banking system. As an example, we found that 70% of banks have anti-fraud software specifically developed to prevent SWIFT fraud. Despite this, 82% of banks report being targeted. In other words, software solutions, while helpful, do not offer a fail-proof solution and are far from impenetrable.

Yet there are numerous measures that financial institutions can take to dramatically reduce their vulnerability to SWIFT fraud. These solutions work best when they are used in tandem, as part of acomprehensive program to combat the threat. We group these practices into four categories:

- Enforcing good policies and practices
- Deploying defensive IT systems and architecture
- Implementing autonomous fraud prevention
- Using AI and machine learning technology to monitor transaction behavior

[14] Ibid.

Let's look at each one.

1. Enforcing Good Policies and Practices

Independent research conducted by Eastnets has found that while some attacks — such as advanced persistent threats (APT) — are highly sophisticated, the majority rely on relatively simple security lapses. Robust internal controls are the first and most important line of defense such lapses.

Internal controls include basic security and IT hygiene, such as requiring appropriate password practices for employees and customers, revoking credentials when employees leave, and safeguarding the physical security of the SWIFT system to prevent unauthorized access. In one incident we investigated, the attacker used an inadequately stored password on some operating systems to compromise other systems on the same network.

This let the attacker gain access to the operating system underlying SWIFT Alliance Access, using valid user accounts.
As SWIFT fraud attacks become more commonplace and sophisticated, banks also need to implement more specialized measures. They need to deploy internal employee-monitoring tools to detect risky behavior, and regularly review which employees can access the SWIFT system.

Lowering the balance of Nostro accounts has proven to be a key measure, ensuring that additional verifications are conducted before large transfers are approved.

It is also essential to segregate the duties of message creation from payment approval, and apply the principle of "least privilege," limiting users' permissions to the bare minimum required to perform their work. Our survey found that many of these measures are not being adequately implemented, including some that are actually mandated by SWIFT's CSP. In particular:

- 19% said their bank fails to adequately restrict access to the SWIFT messaging interface.
- 11% lack strict policies governing access to their SWIFT payment system.
- 14% do not regularly review employee access to the SWIFT payment system.
- 18% have not deployed internal employee monitoring tools to detect risky employee behavior.
- 20% fail to apply least-privilege principle and segregate duties in message creation from payment approval.

Considering that banks tend to have hundreds of correspondent banking relationships, there is a strong chance that they are doing business with partners that lack sufficient basic controls. (See Exhibits 7 and 8 for further details.)

Banks must also conduct simulated SWIFT fraud attacks, engaging the full range of departments potentially involved in an emergency response. Banks whose employees are well aware of the threat and have practiced how to address it are better prepared to do so in the event of an emergency.

Our survey found that leaders are more likely (90%) than laggards (80%) to conduct such attack simulations. Given that the SWIFT fraud threat is more common than previously believed, a strong, well-planned response is of paramount importance.

Exhibit 7

Many banks lack essential anti-fraud policies...

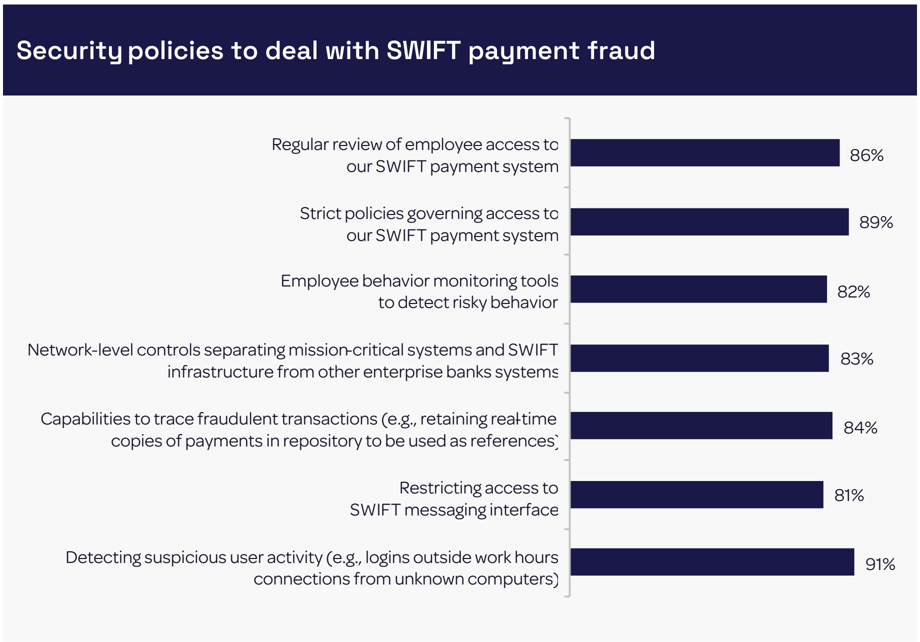
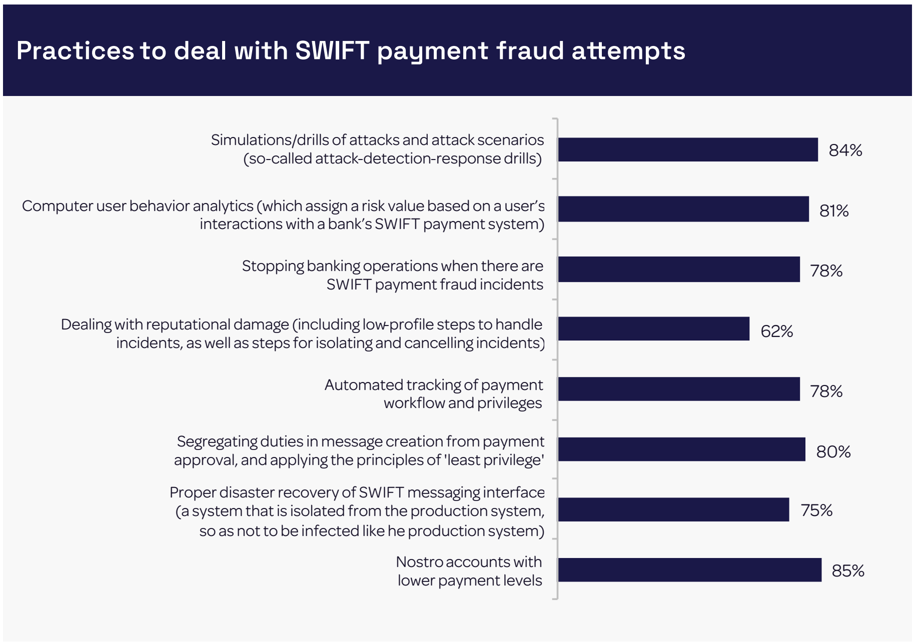


Exhibit 8

...even more banks lack fundamental practices.



In line with these simulations, banks must be prepared to handle the reputational damage that arises when losses have occurred and become publicly known. Leaders more commonly than laggards (71% vs. 56%) have procedures in place to address reputational damage and respond to attacks.

These policies include low-profile steps to handle incidents, as well as steps for isolating and cancelling fraudulent payment messages.

Educating customers about this type of fraud is also an important best practice. Interestingly, we found that leaders were more likely than lag gards to report difficulties educating customers about the risks of SWIFT fraud. This could signal that leaders place a greater emphasis on getting everyone — including customers — to fight SWIFT fraud. Banks could therefore benefit from assessing how well educated their customers are, and then improving their outreach efforts as needed.

2. Deploying Defensive IT Systems and Architecture

Banks need to institute a number of IT best practices to protect themselves from SWIFT cyber fraud, or to recover when fraud is committed. This includes having software applications that retain real-time copies of financial transactions and storing them in a separate, secure database. Fraudsters typically try to prevent detection by damaging or wiping out the system once they have sent the fraudulent messages. That makes it difficult for the bank to track where the money went, and gives the criminals time to withdraw or launder the money.

Having a backup system with copies of financial transactions gives investigators a chance to trace fraudulent activity before the money disappears. Given the pace of international transactions, speed is essential. For instance, using a real-time backup system, one of our clients was able to recover lost messages when hackers damaged its operating system. That enabled the institution to issue a cancellation before all of the money disappeared.
Establishing proper disaster recovery of the SWIFT messaging interface is also essential because it ensures business continuity.

Disaster recovery entails installing a replica system and isolating it from the production system, so that it can’t be infected by the production system. Maintaining a separate database of transactions allows banks to move all operations related to investigations, printing and extraction away from the SWIFT environment. This ensures that the security principles of need-to-know access, least privilege, and segregation of duties are applied.

Our survey found that leaders are more likely to separate such systems (90%) than the overall sample set of banks (83%).
Finally, it is also vital for banks to implement network-level controls that separate mission-critical systems and SWIFT infrastructure from other enterprise bank systems. This reduces the potential for a malicious actor to propagate across the network to reach SWIFT systems.
Again, a significant minority of banks surveyed are not using these protective measures:

- Some 16% do not collect real-time copies of payments and store them in a secure repository. That compromises their ability to trace fraudulent transactions.

- About a quarter (24%) are not prepared for disaster recovery of the SWIFT messaging interface.

- And 17% lack network-level controls that separate mission-critical systems and SWIFT infrastructure from other enterprise banking and/or IT systems.

3. Implementing Autonomous Fraud Prevention

An automated, continuous fraud-prevention system is essential to foiling criminals seeking to exploit the SWIFT messaging system. Banks handle tens or even hundreds of thousands of SWIFT-based transactions a day. Amid this torrent, criminals know they just need to sneak through a small number (or even one) nefarious money-transfer request. Manually monitoring each transaction is impractical and inefficient.

Instead, banks need an automated system that analyzes transactions and user behavior objectively, in real-time, round the clock, flagging or even deferring any activity that appears anomalous or suspicious. An analytics-based solution can expose an intruder, whose behavior does not resemble that of a typical user. The solution can identify the unusual characteristics of fraudulent transactions.

or into the integration bridge between the SWIFT application and the core banking application. As such, these transactions don't have any basis in core banking, a fact that automated solutions can readily detect before the SWIFT messages leave the bank. Again, given the high frequency of transactions, this would be impossible for human agents to monitor.

Another way that automated solutions protect banks is by verifying if the timing of the transaction is atypical. SWIFT fraud is often committed outside regular business hours, when criminals believe security personnel won't be watching.

For instance, in one case that we know of, criminals penetrated a bank's SWIFT messaging interface in the evening after it had closed, and officials were therefore not monitoring transfers. Because the bank had automatic logouts of its terminals outside banking hours, the payments were not sent.

> **“Banks need an automated system that analyzes transactions and user behavior objectively, in real-time, round the clock, flagging or even deferring any activity that appears anomalous or suspicious.”**

But the next morning, when the terminals were set to automatically log in at 7 a.m., the payment messages were released to the network before the staff arrived. This enabled the criminals to transfer millions of dollars without immediate detection. If the bank had put the appropriate systems in place, officials would have been alerted to an attempt of a large series of transfers during an unusual time.

Automated solutions also check whether a transaction is following a standard payment corridor. Just as passengers flying to a remote destination usually follow typical itineraries (for instance, Berlin to Singapore with a transfer in Dubai), banks use common corridors for transferring money.

A typical transfer from Brussels to Boston may go through a major New York bank. Because criminals lack knowledge of a bank's usual payment corridors, they will often send fraudulent requests through atypical routes. Again, these raise red flags that an automated system can instantly detect but that humans would be hard-pressed to identify given the high volume of transactions and correspondent relationships.

Finally, analytics and automated solutions can help block insiders from committing SWIFT fraud. These solutions provide objective red flags based on data, reducing the bank's reliance on employee discretion. They also identify risky behavior among employees and contractors. Given our finding that 14% of banks believe insiders were involved in SWIFT cyber fraud attempts, these solutions are critical to identifying these individuals as they plan and carry out their crimes, before it is too late.

Our survey uncovered evidence that banks' software solutions are not strong enough, or are not properly managed, to fend off SWIFT fraud. While 70% said they have software specifically developed to prevent SWIFT fraud, 82% have been subject to attacks. Sufficiently robust systems would have prevented such attacks.

4. Using Machine Learning Solutions to Track Transaction Behavior

Each bank and its clients have their own established transaction patterns. Machine learning systems are exceptionally proficient at learning these patterns and finding outliers while rendering minimal false positives. Machine learning systems can detect unusual payment corridors, as described in the previous example. Similarly, they can uncover incorrect or unusual correspondents when transferring money.

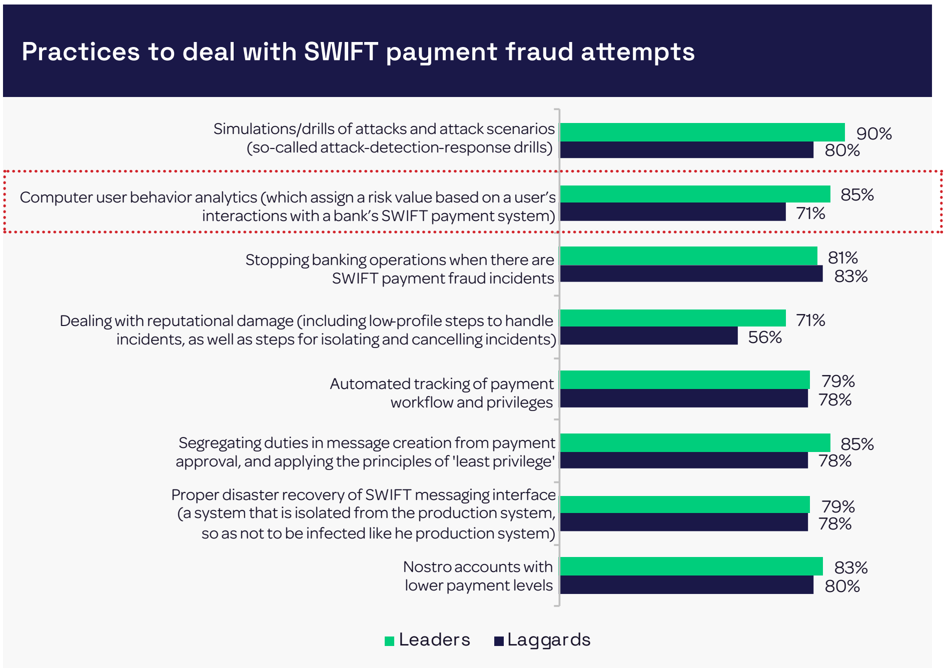
Machine learning systems are adept at understanding other nuances of transaction behavior, such as at what times during the week certain bank departments typically carry out various types of transactions. Treasury departments, for instance, tend to work late hours, weekends and public holidays to manage liquidity, cash flow and foreign transactions. Late-hour SWIFT transactions from a Treasury department, therefore, would likely be cleared. A transaction from the remittances department outside business hours, however, would be flagged as an anomaly.

While machine-learning solutions offer some of the most robust protection against SWIFT fraud, many banks have yet to take advantage

> **“In one case that we know of, criminals penetrated a bank's SWIFT messaging interface in the evening after it had closed, and officials were therefore not monitoring transfers”**

Exhibit 9

Leaders vs. laggards on IT user behavior analytics and other key practices.



of these capabilities. Some 22% of the banks surveyed didn't use automated solutions to detect payment patterns. Additionally, 19% of the banks had not implemented behavior analytics of internal computer users. Notably, more leaders (85%) were capitalizing on user behavior analytics than laggards (71%). (See Exhibit 9.)

Why the Risks of SWIFT Cyber Fraud are Likely to Increase

We believe that adopting the solutions discussed above is a business imperative for banks, and that the urgency is intensifying, largely due to changes in how the financial world operates.

Banking is becoming more convenient in a variety of ways. Transactions are occurring at an increasingly rapid speed. At the same time, other irreversible banking trends and changes in the SWIFT system are making it easier for criminals to exploit the network, and harder for financial institutions to keep them out. To remain competitive in this evolving environment, banks must be able to prevent SWIFT fraud without sacrificing speed, convenience and other modern innovations. Openness is a trend that has boosted banks' vulnerability. Financial transfer systems that were previously cordoned off within each bank's infrastructure now commonly make use of the publicly accessible networks. For instance, mobile banking and peer-to-peer money-transfer applications travel across the internet. Financial technology innovations and open banking standards are delivering major benefits to banks and their customers, but they are also creating unprecedented windows of vulnerability into the global banking infrastructure.

The growing speed and scope of global banking is also boosting vulnerability. The trend toward instant payments means that transfers are expected to be completed within a few seconds, providing very little opportunity for banks to review and verify the millions of transactions that occur daily. Moreover, while banks formerly held large institutional transfers overnight to collect interest, negative interest rates in many regions are compelling them to move money more quickly, to avoid having to pay interest on balances deposited at central banks.

The variety of institutions using the SWIFT network has also grown. Insurance and telecom companies are now on SWIFT, dramatically increasing the number and variety of users. While so far these companies are not publicly known to have been implicated in successful attacks, they don't necessarily have the same security culture frequently found in banks, and therefore could be a target for future hacks.

In all, more than 30 million transactions occur daily using the SWIFT network,[15] and there are more than 1.3 million bilateral banking relationships across the globe.[16] This means verification of payment corridors and due diligence on counterparties is a highly complex undertaking.

But perhaps the biggest reason SWIFT fraud is getting worse is that it's an effective and relatively low-risk crime for the perpetrators. Criminals have been successful in illicitly getting financial institutions to transfer large sums to accounts they control. And they can do this from afar, without risking their lives by storming a bank vault, hijacking a Brinks truck, or breaking into an automated teller machine. Building a strong defense, as described in this report, is the way that banks can simultaneously embrace the speed, openness and global nature of modern banking while keeping cyber criminals who attack payment systems at bay.

Key Challenges for Banks

Our survey found that the top challenges reported by all banks in fighting SWIFT payments cybercrime included dealing with business email compromise, educating customers about how to reduce the risk, and getting employees from different departments to collaborate. Strong interdepartmental collaboration, which is vital to every bank's SWIFT fraud defense, was particularly difficult for laggards. (See Exhibit 10.)

We identified several other challenges faced more acutely by laggards.

These include monitoring risky employee behavior, getting the proper training, and acquiring the necessary funding.
Some 59% of banks that were lagging at fighting SWIFT cyber fraud reported difficulties in monitoring risky employee behavior, compared to only 31% of leaders. This was the biggest gap between leaders and laggards on any of the challenges we asked about.

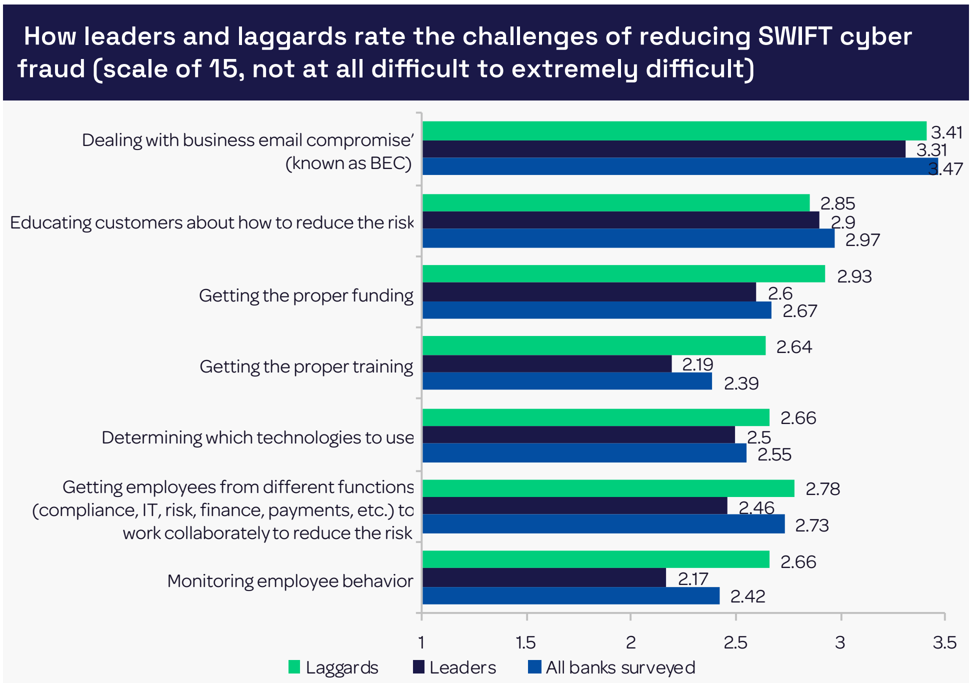
Given that insider involvement in banking fraud with SWIFT payments is not uncommon, the fact that leaders have both the means and authority to effectively monitor their employees may play a significant role in addressing the threat.
Getting proper training is a challenge reported by 59% of laggards vs. only 42% of leaders. Curiously, we found that laggards were more likely (65%) to conduct training at least quarterly for employees than leaders (54%). (See Exhibit 11.) There are several possible explanations for this.

> **“59% of laggards struggle to monitor risky employee behavior, compared to 31% of leaders.”**

[15] "SWIFT FIN Traffic & Figures" Accessed on Sept. 3, 2019 at https://www.SWIFT.com/about-us/SWIFT-fin-traffic-figures
[16] "The Decline in Access to Correspondent Banking Services in Emerging Markets" World Bank, 2018, Accessed at http://pubdocs.worldbank.org/en/786671524166274491/TheDeclineReportlow.pdf

Exhibit 10

Leaders find it easier to get the right funding, training, collaboration, and employee oversight



How leaders and laggards rate the challenges of reducing SWIFT cyber fraud (scale of 15, not at all difficult to extremely difficult)

Perhaps the training that laggards conduct is not as effective, or that they are not adequately sharing knowledge across different functions within the bank, to capitalize on enterprise knowledge rather than just departmental knowledge. It's also possible that laggards are getting inferior sults because they are depending more heavily on employees than on systems and technology.

Alternatively, this could merely be a symptom of the fact that smaller banks have higher turnover and therefore have to work harder to keep employees up to speed on the latest ways to combat SWIFT cyber fraud.

Laggards were also more likely to report difficulties getting the funding needed to mount a reliable defense. Nearly two-thirds (64%) of them struggle with this, compared to 48% of leaders. In turn, we also found that laggards spend less. As mentioned above, the average leading bank spends 75% more annually ($1.4 million) to reduce the risk of SWIFT fraud compared to laggards ($800,000).

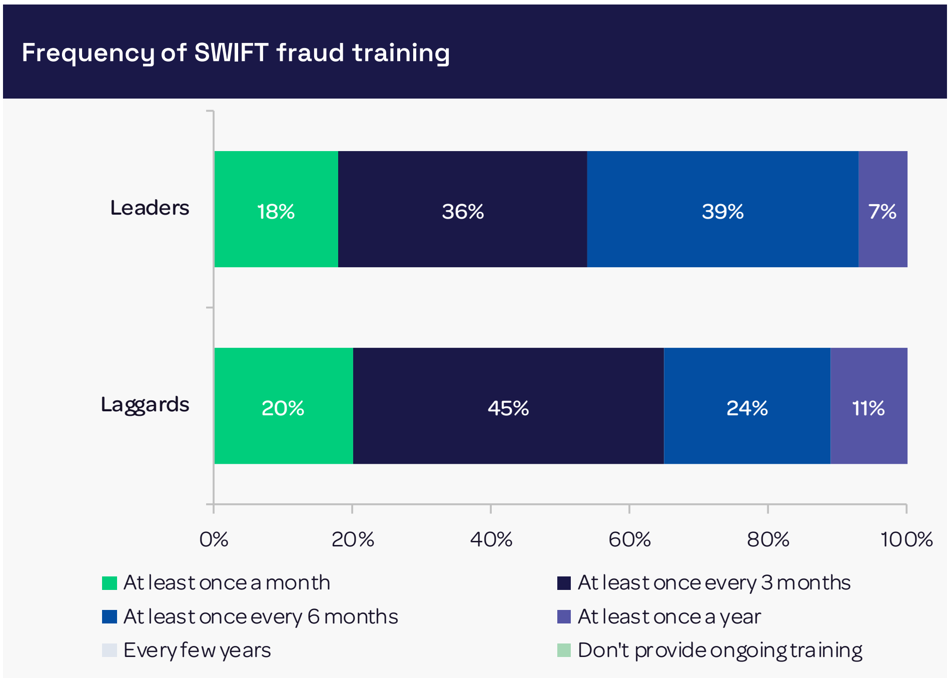
This is likely in part because the leaders we surveyed were on average larger banks than the laggards. Leaders were more likely to be banks with assets over $100 billion (54% of leaders vs. 39% of followers) while laggards were more heavily represented by banks under $50 billion in assets (27% of leaders vs. 42% of laggards).

Call to Action: Assessing Existing Policies and Practices

As mentioned previously, most of the banks surveyed see SWIFT fraud declining over the next three years. (See Exhibit 5.) However, based on what we know about SWIFT fraud, we believe this optimism reveals overconfidence and, thus, a potential for higher risks in the future.

Exhibit 11

Leaders actually train their people less frequently than laggards



The policies and practices that we surveyed in this report are essential to fighting SWIFT fraud. They are worth assessing as a next step in bolstering a bank's defenses, given that they are common to banks that reported a strong anti-SWIFT fraud performance.

As a final thought, it's worth noting that the biggest risks tend to come not from the threats that you are aware of, but instead from those that are unknown — the so-called unknown unknowns. In light of the widespread (and we believe erroneous) view that SWIFT fraud will decrease in the next three years, it is vital for banks to proactively seek to understand the hackers' next moves, rather than wait to find out after the damage has been done before building new controls.

All banks should therefore look toward technologies such as artificial intelligence and machine learning to anticipate the next threats, and deal with them before it is too late.

It's worth noting that leaders are by no means impervious to the threat. In fact, they were more likely to report that they had been targeted by SWIFT fraud attempts (88%) than laggards (80%). This signals that there was some level of cyber penetration by criminals. (It is important to note that the higher level of attacks reported by leaders may reflect a greater ability to spot intruders. Studies suggest that attackers generally linger in the target's network for about 200 days before being discovered, and many banks may lack the capacity to detect them.)

“Based on what we know about SWIFT fraud, we believe banks' optimism reveals overconfidence and a potential for higher risks in the future.”

Still, the banks reporting the greatest success in reducing SWIFT cyber fraud reported a higher level of satisfaction with their ability to address the problem. This suggests that while they were, in fact, attacked, they effectively defended their networks.

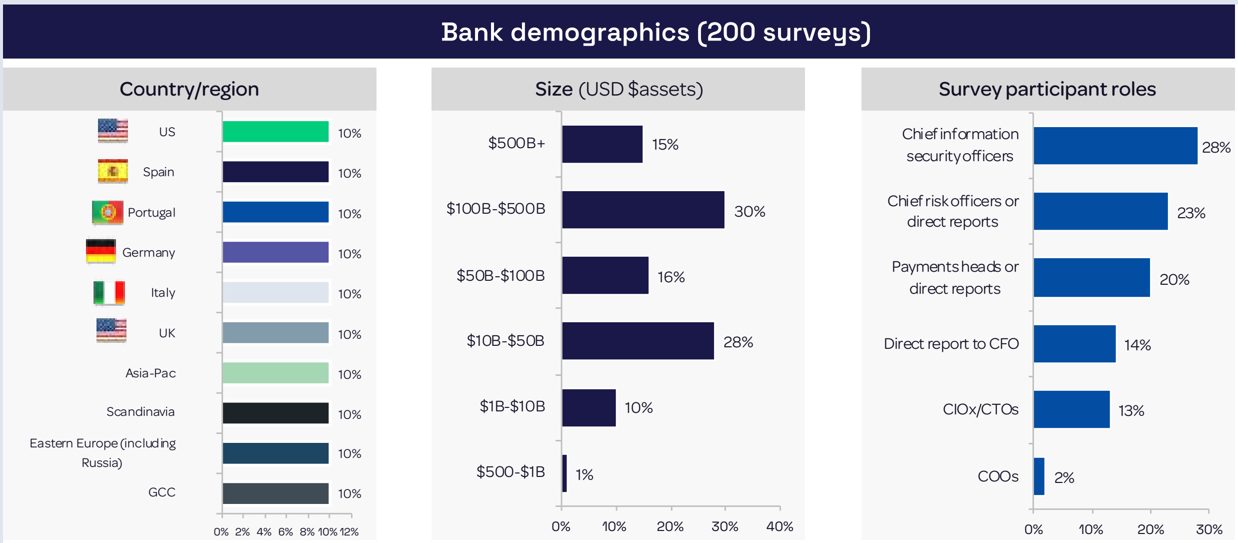
Banks seeking to bolster their defenses against SWIFT fraud would be well advised to start by reviewing their performance on the key measures that leaders more commonly emphasized, and by taking action on those measures that need improvement.

About the Study

The Eastnets study, conducted in summer of 2019, surveyed 200 banks in the U.S., Europe (Spain, Portugal, Germany, Italy), UK, Asia-Pacific, Scandinavia, GCC (Bahrain, Kuwait, Oman, Qatar, Saudia Arabia, UAE) and Eastern Europe (including Russia).
Some 45% had more than $100 billion in assets, while 44% had assets between $10 billion and $100 billion, and 10% had assets between $1 billion and $10 billion. Most of the survey participants were from the C-suite, including chief information security officers (28%), chief risk officers or direct reports (23%), chief financial officers (14%), chief information officers and chief technology officers (13%) and chief operating officers (2%). One-fifth of respondents were heads of payments of their direct reports. (See Exhibit 12.)

Exhibit 12

Survey demographics



If your organization has been impacted by the issues in this report and you'd like to discuss them with one of our experts, please contact us at marketing@eastnets.com

About the Author:
Deya Innab, Deputy CEO, Eastnets

As Deputy CEO, Ms. Innab works closely with the Chief Executive Officer to develop corporate strategy, goals, policies, short and long-term objectives for consideration, adoption, and implementation by the Board of Directors. Acts as the secondary spokesperson for the organization and is responsible for all day-to-day management decisions and for implementing the organization's long and short-term strategic objectives.

Deya has been instrumental in developing Eastnets' global growth strategy in alignment with the company's corporate vision and translating this strategy into innovative solutions and products that meet the evolving needs and the dynamic nature of the industry.

Ms. Innab has led several development initiatives for Eastnets, including the industry-leading ChainFeed™ solution — a secure real-time watchlist feed over the blockchain. Ms. Innab was also the author of the global survey report: How Banks Are Combating the Rise of Swift Cyber Fraud? and has contributed to many other thought leadership projects.
Before joining Eastnets, Ms. Innab's career encompassed working for several entrepreneurial tech firms as well as the multinational professional services network, KPMG, serving global clients.

Ms. Innab is a graduate of the University of Jordan, where she gained a degree in computer science. In addition, she has attended a number of prestigious executive development programs including INSEAD's flagship intensive Advanced Management Program in Fontainebleau France, and the Orchestrating Winning Performance management program at IMD in Lausanne, Switzerland. Ms. Innab is a certified board of directors by Jordan, Institute of Directors – IFC.

Disclaimer & Fair Use Statement
This survey may contain copyrighted material, the use of which may not have been specifically authorized by the copyright owner. This material is available in an effort to explain issues relevant to combatting Cyber-attacks on Banks SWIFT payments.
The copyrighted material contained in this survey (if any) is distributed without profit for research and information purposes.
This should constitute a 'fair use' of any such copyrighted material (referenced and provided for in; inter alia; section 107 of the US Copyright Law).
If you wish to use any copyrighted material from this survey for purposes of your own that go beyond 'fair use', you must obtain expressed permission from the copyright owner.

Disclaimer of Liability
The material and information contained in this survey is for general information purposes only. You should not rely upon the material or information on the website as a basis for making any business legal or any other decisions.
Whilst we endeavor to keep the information up to date and correct, Eastnets makes no representations or warranties of any kind express or implied about the completeness, accuracy, reliability, suitability or availability with respect to the information, products, services or related graphics contained in this survey for any purpose.
Any reliance you place on such material is therefore strictly at your own risk.
Unless explicitly stated, the views expressed in this reprot are personal and not necessarily those of Eastnets.

Copyright (c) 2020 Eastnets.

Errors and Omissions Disclaimer
The information in this survey is intended to furnish users with general information on matters that they may find to be of interest. The information contained in this survey is provided by Eastnets general guidance and is not intended to replace or serve as substitute for any audit, advisory, tax or other professional advice, consultation or service. You should consult with appropriate Eastnets professionals or other professional advisors for advice concerning specific matters before making any decision.
Certain links in this survey lead to servers maintained by individuals or organizations over which Eastnets has no control. Eastnets makes no representations or warranties regarding the accuracy or any other aspect of the information located on such servers.
Every effort has been made to offer current and accurate information to our users, but errors can occur. Eastnets assumes no liability or responsibility for any errors or omissions in the content contained in this survey. Furthermore, this survey may contain references to certain laws and regulations that may change over time and should be interpreted only in light of particular circumstances. This information is provided "as is," with no guarantees of completeness, accuracy or timeliness, and without warranties of any kind, express or implied.
In no event will Eastnets or its partners, members, agents or employees be liable to you or anyone else for any decision made or action taken in reliance on the information in this survey or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Eastnets is a global provider of compliance and payment solutions for the financial services sector. Our experience and expertise help ensure trust at 750 financial institutions across the world, including 11 of the top 50 banks.

For more than 35 years, we've worked to keep the world safe and secure from financial crime. We do it by helping our partners manage risk through screening, monitoring, analysis and reporting, plus state-of-the-art consultancy and customer support.

As specialists in end-to-end payment systems, we turn payment challenges into opportunities, helping financial Institutions operate more efficiently and cost-effectively. That includes more than 270 corporate and financial institutions who rely on us for outsourced SWIFT connectivity and compliance software solutions.

In 2019, we were awarded the ISO 27001:2013 certification for our Information Security Management System. This certification demonstrates our continued commitment to information security at every level and ensures that the security of our clients' data and information has been addressed, implemented, and properly controlled in all areas of our organization.

UAE • Jordan • Bahrain • Pakistan •
Qatar • Belgium • United Kingdom • Luxembourg •
Egypt • Hong Kong • USA •

Eastnets.com

For any questions please contact us at
marketing@eastnets.com