ACAMS® TODAY

The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field

COMBATING CYBER FRAUD in CORRESPONDENT BANKING

Cybercrime is a major concern for banks around the world. Until recently, the focus of attacks has tended to be on banks' customers through card and account detail compromises. But as criminals have become more sophisticated, they have raised their ambitions, and in a change of focus are now directly targeting banks themselves. In light of these threats, what steps can financial institutions take to protect themselves from cyberattacks, detect suspicious activity more readily, and improve their chances of recovering quickly from any cybercrime attacks?

Current context

When looking to identify current threats, the first thing to understand is that organized cybercrime can take a number of different forms, ranging from a scattergun approach to sophisticated high-end, targeted attacks.

David Ferbrache, technical director for cybersecurity at KPMG U.K., explains that fraudsters typically start with commoditized attacks, whereby organized crime groups send millions of emails containing phishing links to malware. "If clicked on, these can result in the system being compromised and the potential for money to be extorted by ransomware demands," explains Ferbrache. "Only a small number of these attacks prove successful, but it's a numbers game."

The second stage is tailored or targeted attacks. As Ferbrache explains, "The organized crime groups spend a couple of weeks researching the organization they want to compromise, and the phishing attacks they undertake are just that bit more credible, targeted and specific." One example of this is business email compromise schemes, which have already led to losses of over $3 billion, according to figures published by the FBI in June 2016.[1]

Sophisticated fraudsters are now mounting focused high-end attacks. Organized crime groups have begun directly targeting bank systems. Unlimited cash-out attacks, for example, have seen criminals compromise the networks of card-issuing banks, enabling

[1] "Business E-mail Compromise: The 3.1 Billion Dollar Scam," FBI, June 14, 2016, https://www.ic3.gov/media/2016/160614.aspx

Reprinted with permission from the June–August 2017, Vol. 16 No. 3 issue of *ACAMS Today* magazine, a publication of the Association of Certified Anti-Money Laundering Specialists

SWIFT

ACAMS® Advancing Financial Crime Professionals Worldwide®

Organized crime groups have begun directly targeting bank systems

them to modify withdrawal limits and clean out groups of ATMs in coordinated assaults.[2] Ferbrache says that one notable attack in 2013 saw a $40 million loss across 24 different countries in a single night.

In other cases, malicious software is uploaded to ATMs through banks networks, so that the machines respond to codes entered by the organized crime groups. Last year, such attacks were carried out in countries including Taiwan, Thailand, Russia, Armenia, Belorussia, Poland, Germany, Georgia, Romania, Kyrgyzstan, Estonia, Spain, the Netherlands, the U.K. and Malaysia.

Last year's attack on the Bank of Bangladesh, which resulted in the loss of $81 million, is of particular concern to correspondent banks. While the attack itself took place in early February 2016, the ultimate beneficiary accounts in the Philippines had allegedly been opened a year earlier, which is likely to have been when the attackers began their initial reconnaissance. Software on the bank's interface server was modified, not only to enter fraudulent payment requests, but also to conceal this activity so that fraudulent transactions would not appear on daily logs.

The shift from targeting banks' customers to targeting banks themselves represents a very significant change

Preventing and detecting attacks

The shift from targeting banks' customers to targeting banks themselves represents a very significant change and an increasing threat to the correspondent and the wider banking community. However, it is important to note that while compromises have taken place in banks' own environments, there is no evidence that the SWIFT network and core messaging services were compromised in any of the attacks.

The attackers are very well organized and sophisticated in terms of how they carry out back-office attacks. They follow a four-step process:

1. Compromising the customer's environment, introducing malware using techniques such as phishing or email compromise scams.
2. Capturing valid operator credentials, typically through access to password files or by putting keyloggers in place to capture password details, and thereby gaining an understanding of the payment environment and associated behaviors.
3. Using fraudulent credentials to attack the back office; for example, by sending fraudulent MT 103 payment messages.
4. Hiding transaction activity. For example, by removing payment information from local databases, modifying incoming statement information or rendering the local environments inoperable and thereby delaying the discovery of the attack and increasingly the likelihood that funds will be settled.

[2] Chris Strohm, "Most-Wanted Cybercriminal Extradited to U.S. From Germany," *Bloomberg,* June 23, 2015, https://www.bloomberg.com/politics/articles/2015-06-23/turkish-man-accused-in-global-atm-heist-extradited-to-u-s-

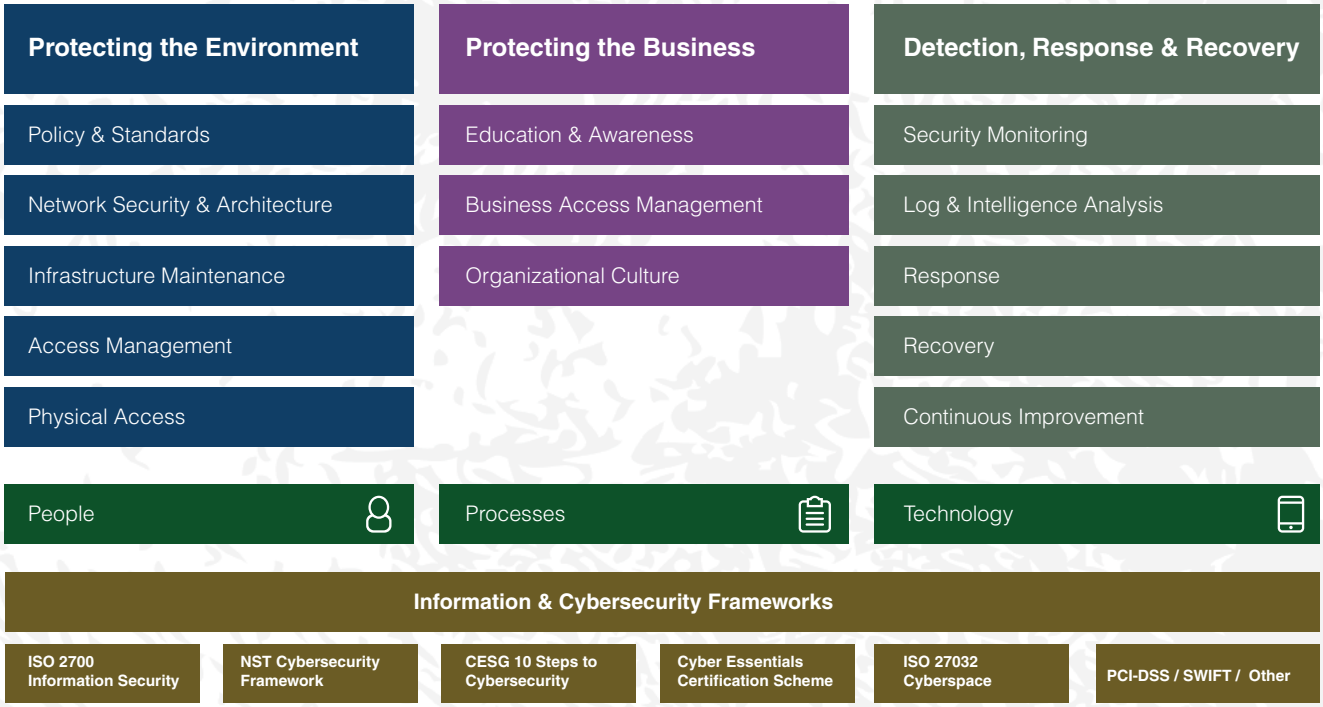


Table 1: Cybersecurity Best Practice Considerations

As attackers begin to understand banks' internal processes and infrastructure, it is clear that they are becoming more dangerous. As such, there is a greater need for financial institutions to take steps to protect their key systems and gateways.

While financial institutions would ideally be able to prevent any cyberattack from taking place, it is impossible to eliminate the threat entirely. As well as putting controls in place to prevent attacks, institutions need to be able to detect attacks when they occur, and should prepare recovery and response procedures.

From information sharing across the banking community to the adoption of appropriate market practice, there are a number of tools, techniques and initiatives that can help banks mitigate the risks, identify suspicious activity and recover from incidents.

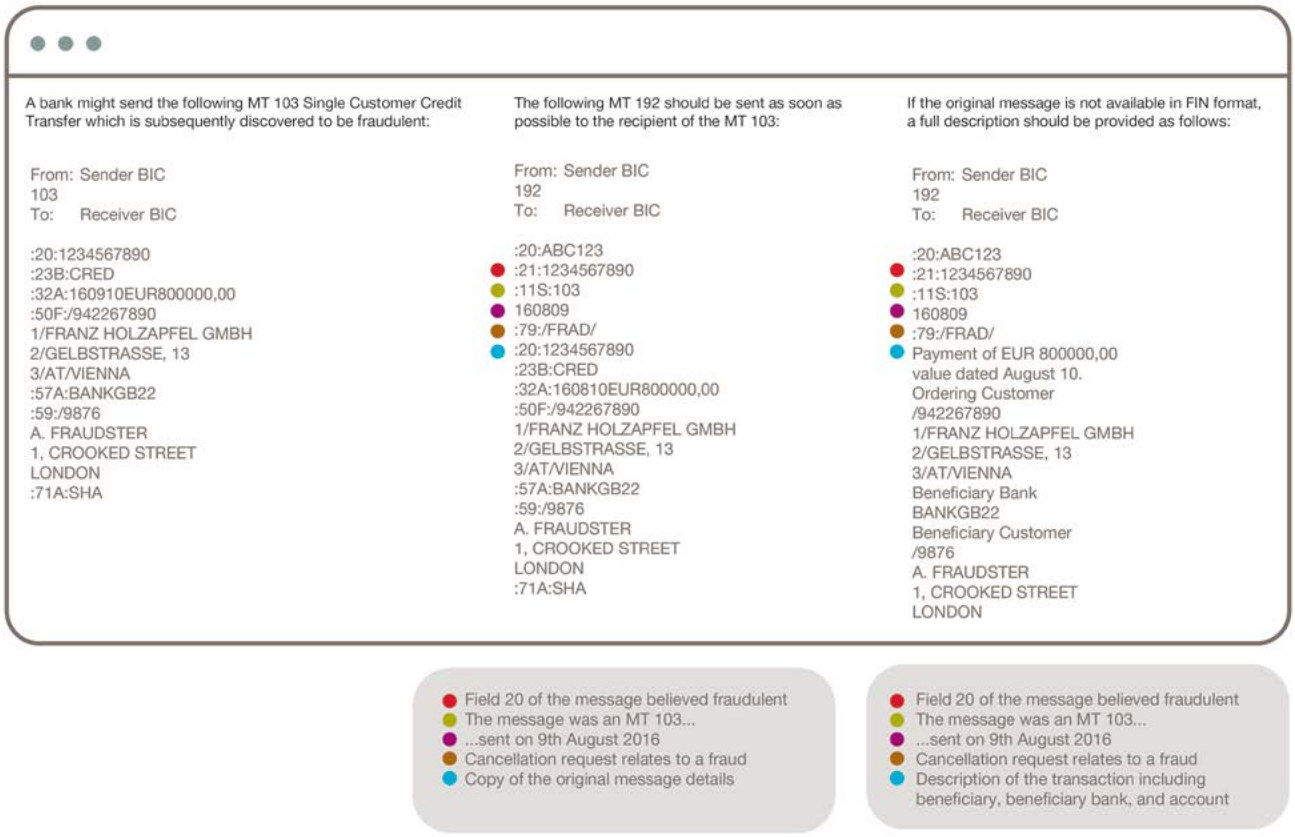
Establishing a strong foundation

As cyberattacks become more prevalent, the industry and regulators are taking steps to understand, address and mitigate the risk. In May 2016, SWIFT launched its Customer Security Programme to strengthen existing cyber controls and provide a collaborative framework for its 11,000+ member institutions to manage evolving cyber threats. The Programme focuses on the need for institutions to secure and protect their own environments and share information within the SWIFT community, as well as the importance of managing relationships with counterparts.

SWIFT's initiative comes at a time where there is also increasing scrutiny and guidance on banks' cybersecurity from regulators. For example, in September 2016, the New York State Department of Financial Services (DFS) issued a proposal building on existing guidance in relation to cybersecurity.

A common feature of all of these approaches is the need to get basic security hygiene in place. While cyberattacks are becoming more sophisticated, the importance of getting basic security right should not be underestimated. As show in Table 1, the following areas should be addressed:

- *Protecting the environment*— This includes defining and applying the appropriate policies and standards, as well as access management, and putting suitable security measures in place for the institution's network and architecture. Institutions should also apply measures such as segregating duties across key staff, dealing



Using the correct SWIFT message format can increase the likelihood of successfully canceling payment transactions when fraud is suspected.

appropriately with new and departing staff and controlling privileged access to systems.

- *Protecting the business*— In some cases, institutions may focus on cybersecurity without necessarily understanding the business context. Research has indicated that a majority of SWIFT customers see human factors as the greatest area of weakness where cyber threats are concerned. Therefore, education is critical when it comes to raising awareness of current threats. In some cases, institutions use simulated phishing messages within their organizations so that they can identify the need for reinforcement training if staff click on malicious links.
- *Detection, response and recovery*— Institutions should ensure that the required security monitoring measures are in place, such as continuous policy monitoring and the use of proper processes to monitor critical events. Specific measures should also be put in place, such as reviewing relationship management applications (RMAs) and adopting relevant market practice.

Reviewing RMAs

When it comes to managing relationships with counterparts, there are a number of steps that financial institutions can take. The first is to review the relationships covered by the RMA.

RMAs are 'digital handshakes' between financial institutions that specify whether transactions can be exchanged. Without an RMA in place, institutions cannot receive SWIFT messages from counterparts. Using RMA Plus, banks can exercise further control by specifying which particular types of messages they wish to exchange over the network and with whom. Therefore, RMA and RMA Plus enable banks to mitigate risk by avoiding the sending and receiving of unwanted messages and reducing the risk that someone within either institution initiates unauthorized transactions.

However, transaction patterns can change over time. As a result, as many as 60 percent of RMA relationships are dormant or inactive, meaning that institutions may be needlessly exposing themselves to particular corridors. Superfluous RMAs can also result in unnecessary costs, as compliance requirements will often dictate that KYC reviews are carried out on counterparts with whom open RMAs are in place. As such, institutions should regularly review the RMAs they have in place, for both cost and security reasons.

Guidance published by the Wolfsberg Group last year noted that financial institutions "should incorporate RMA due diligence standards into their Financial Crime/AML/KYC programmes," for example, by segregating RMA requests between customer

relationships and non-customer RMAs. The guidance notes that "due diligence on the RMA holder should consider the message types used by the RMA holder and the risk associated with the activity conducted."[3]

Market practice

There are other actions financial institutions can take in order to detect fraud more readily and respond more effectively to any threats. For example, it is good practice to reconcile accounts, provide payment confirmation and have policies in place around payment amendments. Institutions should also know how to cancel payments rapidly, should the need arise.

One step that institutions can take is to send—and require counterparts to send—SWIFT MT 900 and MT 910 confirmation messages. While these messages are not currently mandatory, they provide additional transparency between counterparties. By the same token, banks should also review the MT 940/MT 950 statement messages that they receive in order to check that the amounts and balances recorded on their statements match their own records of transaction activity.

As a further step, banks should avoid the use of free format messages such as MT 199 to amend or change payment instructions, as this can impede reconciliation. Instead, banks should cancel the original instructions or send payment adjustments if payment instructions need to be changed or canceled.

Monitoring transaction data

Given the growing tendency of cybercriminals to conceal their fraudulent activity, banks should also carry out activity monitoring and risk monitoring, both to prevent fraud and to detect attacks that do take place.

- *Activity monitoring*— By obtaining an aggregated record of daily activity, banks can gain a clearer understanding of their payment activity and identify any significant changes in activity.
- *Risk monitoring*— By monitoring risk in their transaction environments, banks can counteract fraudsters' efforts to hide their transaction activity, as well as identifying unusual single or aggregated transactions.

Institutions should source and store such information separately to ensure that it cannot be compromised in an attack that disables or damages their own payment systems and records.

Response and recovery

It is also important to have robust processes in place so that financial institutions can respond quickly and effectively if they detect a cyberattack. This may involve canceling fraudulent messages, or taking steps to facilitate business continuity if transactions cannot be canceled.

Canceling fraudulent transactions

In some cases, it may be possible to cancel a fraudulent instruction by sending a cancellation message. In order to cancel a payment instruction, banks should immediately send an MT n92, where 'n' refers to the category of the original message. For example, an MT 103 would require a MT 192 cancellation message, and an MT 202 would require an MT 292.

When using a cancellation message, it is also important to use the correct fraud code, as this is used to prioritize the request and improve the likelihood that the instruction will be successfully canceled. The required code is the use of the code word /FRAD/ in field 79 of the cancellation message.

Disaster recovery/business continuity

As the final stage of defense, financial institutions need to have measures in place that enable them to respond appropriately to cyberattacks and restore usual business operations as quickly as possible. This requires a strong link between cybersecurity and business continuity/disaster recovery, as well as an understanding that cybersecurity is intrinsically connected to the core business. "Cyber is not something you can separate from the core business," comments Ferbrache. "All of our businesses are digitally dependent now, and all of them deal with digital threats."

In order to have effective recovery processes in place, institutions should have worked through different scenarios and understood their consequences. Institutions need to plan how they will contain or mitigate the consequences of an attack, as well as knowing how they will deal with communications, regulatory and legal issues. They also need to have a plan in place stating how they will bring the business back online quickly and securely.

Conclusion

As cybercriminals turn their attention deeper into the banking world, it is imperative that financial institutions take appropriate steps to secure their environments. There are a number of areas in which actions can be taken both to prevent attacks, as well as to increase the likelihood of an attack being detected in time. Last but not least, institutions need to have a clear business continuity plan in place covering the steps to take in the event of a successful attack.

Tony Wicks, head of AML initiatives, SWIFT, London, U.K., tony.wicks@swift.com

[3] "Wolfsberg Guidance on SWIFT Relationship Management Application (RMA) Due Diligence," the Wolfsberg Group, http://www.wolfsberg-principles.com/pdf/standards/SWIFT-RMA-Due-Diligence.pdf