Reinforcing cybersecurity defences: a technological and human approach

By Nancy So
Head of Institutional Cash Management, APAC, Deutsche Bank

In February 2016, Bangladesh's central bank was subject to a successful malware attack that attempted to siphon US$951 million across 35 separate forged cross-border payment orders. A total capital loss of US$101 million was suffered before the remaining orders were blocked. Thus far, only US$20 million has been recovered, and only by a chance error (because the name of the recipient's account contained a spelling error).[1]

Of course, given the monumental losses – and the growing frequency of attempted attacks that occur – cybercrime has been propelled to the top of the industry's priorities, but nowhere more so than Asia, which is 80% more likely to be targeted than the rest of the world.[2]

Of particular concern are attempts to compromise correspondent banking networks, given that these systems house the world's largest remittance services providers – and, therefore, process the vast majority of the world's transactions. And when it comes to cross-border payments, ensuring that cyber-criminality prevention practices remain one step ahead of hackers is crucial to maintaining an undisrupted payment flow.

In light of this, Deutsche Bank is in the process of developing holistic payment security protocols that aim to neutralise potential threats. There are two elements to this: first, the adoption of state-of-the-art technological capabilities and, second, the construction of a "human firewall" via market collaboration and education for staff and clients. As such, the bank has established a comprehensive strategy to **help prevent, combat** and **detect potential** cyber-hacks. What remains is to ensure this strategy's wider implementation.

So: *Without employee training, even the most advanced technology is prone to fail*

Asia: a vulnerable cybercrime target

Certainly, the Bangladesh case highlights the need for urgent action. Not only were capital losses suffered, the Bangladesh central bank hack revealed the nature of the vulnerability gap. Indeed, the attack was successful due to shortcomings in the central bank's security procedures, which resulted in the fraud going undetected for some weeks prior – while it also remains unclear whether or not the malware was disseminated via an infected email sent to a staff member, as reported by *Reuters*.[3]

The Bangladesh central bank heist highlights the major challenges banks face with respect to ensuring that systems are technologically secure and staff are able to detect social engineering attempts, such as phishing – the act of inducing confidential data from an employee under the guise of a known sender.

This particular type of attack is a mounting concern, notably in Asia Pacific, where up to 90% of banks and corporates suffered a form of cyber-attack in 2016 (up from 76% on the previous year), according to LogRhythm.[4] This is partly driven by the region's institutional vulnerabilities. Indeed, the lack of regulatory standardisation across the multitude of jurisdictions can, in some instances, complicate the task of detecting threats – with compromises in Asia taking an average 520 days to be detected in 2015, compared to the 146-day worldwide average.[5]

Mitigating cyber-risk by advancing technological defences

In combating these threats, Deutsche Bank has adopted a three-pronged approach to prevention that includes sophisticated system security, industry-wide collaboration via banking networks, and sharing its expertise with both employees and financial institution clients to ensure that all parties are better prepared to combat cyber-criminal activity.

First, given the voluminous levels of automation in the cross-border payment infrastructure, service provider banks' first line of defence comprises the digitalised security

[1] http://www.reuters.com/article/us-usa-fed-bangladesh-typo-insight-idUSKCN0WC0TC
[2] http://www.bbc.co.uk/news/technology-37163076
[3] http://www.reuters.com/investigates/special-report/cyber-heist-federal/
[4] https://www.ft.com/content/38e49534-57bb-11e6-9f70-badea1b336d4
[5] http://www.bbc.co.uk/news/technology-37163076

platforms themselves. In this respect, Deutsche Bank's position as Asia's number one euro clearer and a leading USD clearer [6], affords the bank an unrivalled opportunity to leverage data mining analytics across its swathes of payment information – and thereby help to detect anomalous transactions. For instance, if a client attempts to transfer a seemingly uncharacteristic payment, the bank's proactive data analytics will flag a warning to its fraud detection team.

These advancements coincide with the bank's wider commitment to developing industry-standard, real-time solutions for both payment and banking platforms, more generally, that detect potentially fraudulent activities. Should any unexplained activity be flagged by the system, the bank will contact its client immediately – demonstrating the necessary synergy between the technological and human elements that creates a robust defence strategy. But, it's worth noting that these technological advancements, in isolation, are insufficient.

This is why the second prong to Deutsche Bank's approach is collaborating with industry peers, notably via the global financial messaging network, SWIFT. Of course, SWIFT is an attractive target for cyber-criminals in its own right, given that bank transfers worth over US$6 trillion pass through the network each day.[7]

With this in mind, Deutsche Bank believes any meaningful action to combat cybercrime must involve a critical mass of the providers involved – and the bank pursues this aim by rallying collective initiatives via SWIFT's extensive network to safeguard against cross-border payment cyber-criminality.

Among these initiatives, Deutsche Bank actively supports SWIFT's Customer Security Programme (CSP) by disseminating its expertise on preventative practices across the network. In a similar vein to SWIFT's initiatives to promote payment standardisation, the network also is planning to introduce core security standards and an associated assurance framework – including future inspections of its members' security compliance from 2018.

The human risk: upskilling employees to reduce risks

The bank has complemented its industry outreach by sharing its expertise with both employees and clients in order to mitigate cyberrisk's human elements. After all, while automated systems can detect abnormal payment patterns, not only are these systems created by employees, but many cyber-attacks, including social engineering attempts, originate from an employee's insider status – whether unintended or deliberate. Without adequate training for employees, even the most advanced cybersecurity technologies could be prone to failure.

Given the pervasive threat, Deutsche Bank believes it is crucial that every employee recognises his or her individual role in preventing cybersecurity breaches and, therefore, mandates information security training across the entire bank – to both operational and client-facing staff.

For instance, the bank's Chief Information Security Office (CISO) offers employees training that heightens awareness around how to best monitor transactions and identify any transactional anomalies. This ensures that all employees receive industry-leading advice to reinforce their respective systems – and, in effect, create a "human firewall" against potential IT risks.

More generally, the CISO is tasked with both ensuring the operational integrity of the bank's data systems and the security of client data held internally. The CISO also has a significant strategic role driving our cybersecurity strategy (both internally and externally) and seeking optimal tactics for reducing information risks and establishing the necessary standards and controls.

While Deutsche Bank has played its part in advancing the development of a robust industry-wide cybercrime prevention strategy, financial institutions are, thankfully, not working alone. Indeed, collaboration has led to a holistic effort that begins with state-of-the-art technology and runs all the way through to educating both back-end and client-facing employees on how to spot these potential threats.

Certainly, much work has yet to be done, as the Bangladesh case well illustrates. But much has already been achieved and diligent efforts are ongoing, so – be assured – Asia's financial institutions understand the gravity of the threats at hand, and are working collaboratively to safeguard their customers and close the vulnerability gap. ■

Deutsche Bank

[6] http://www.asianbankerawards.com/transactionbanking/press/2017/Best-Global-Clearing-and-International-Cash-Management-Bank-in-Asia-Pacific-Deutsche-Bank.pdf

[7] https://www.ft.com/content/e3bfdd54-21b2-11e6-aa98-db1e01fabc0c