Cyber Crime and Money Laundering – a dangerous marriage for all in finance

New York Fed to help Bangladesh Bank in $81 million cybercrime suit – Finextra Feb 04, 2019

Bangladesh Bank files lawsuit, New York Federal Reserve and SWIFT offer help – MoneyControl Feb 06, 2019

Philippines' RCBC sues 'vicious' Bangladesh Bank over heist claim – Reuters, CNBC Mar 12, 2019

Financial Services Firms Face Increasingly High Rate of Cyberattacks – biztechmagazine.com Sept 27, 2018

All Banks are acutely aware of the importance of Cyber Security and of AML defenses. Increasingly though the two are often combined by criminals aiming to benefit illegally at the cost of financial institutions. It is becoming a huge issue in not just money stolen or transferred illegally, but in cost to the global economies. A McAfee report last year estimated a $600 billion global cost.

In the case of a massive cyber heist in 2016 both threats combined resulting in $81 million being stolen. Hackers tried to transfer $1 billion from Bangladesh Banks account with the FED using the SWIFT interbank payments network. The central bank was allegedly vulnerable to the malware intrusion because it did not have a firewall and used second-hand $10 routers to network computers connected to Swift, according to an article in Finextra.

Eighty-one million dollars in fraudulent payments ended up in an account at Philippines-based Rizal Commercial Banking Corp (RCBC), before being offloaded into the hands of casinos and gambling operators in Manila. Bangladesh Bank has now filed suit against RCBC in a district court in Manhattan, and has recruited the NY Fed to provide "technical assistance" in helping the bank to recover the lost $81 million in one of the biggest cyber heists in history in 2016. The New York Federal Reserve is supporting the Bank and SWIFT has signed an agreement to rebuild its infrastructure, according to a Reuter report. RCBC has called the legal action Bangladesh Bank filed on Thursday as beyond the U.S. jurisdiction, "completely baseless" and "nothing more than a thinly veiled PR campaign" to shift blame from itself, Reuters reports.

It is unclear who should bear the blame, but it is obvious to me that all are victims of criminal activity. Because of the amounts involved it easy for all parties to blame each other, and they probably all have a reasonable argument. But the obvious lesson to learn from this is that all types of banks are at risk from money laundering activity and Cyber Crime; and all banks and financial institutions in all parts of the world need to do their utmost to protect themselves and their clients from this type of nefarious activity. Criminals no longer need to use guns and physical force which historically limited their reach geographically during any one crime, now all parts of the globe are literally within arm's length and within a few key strokes.

As usual it starts with the fundamentals –

Intuition has an excellent Cybersecurity module which prepares an institution's employees with the knowledge and skills to become part of a key defense against cyber-attacks. It provides initial training which is followed up with one year of analytics and new information on fresh cyber threats and how to deal with them.

The Intuition Know-How Library consists several tutorials related to this article:

Operational Risk Management (4 tutorials)
Other Regulation / Compliance (9 tutorials)
Transaction Banking (4 tutorials)

For Intuition blended learning related to this article, some of our popular workshops include:

- Risk Management & Measurement
- Cyber Security in Financial Services
- Disruptive Technology in Financial Services
- Blockchain Applications in Financial Services

Get the app

Get in touch with your Intuition account manager at asiainfo@intuition.com for more details.