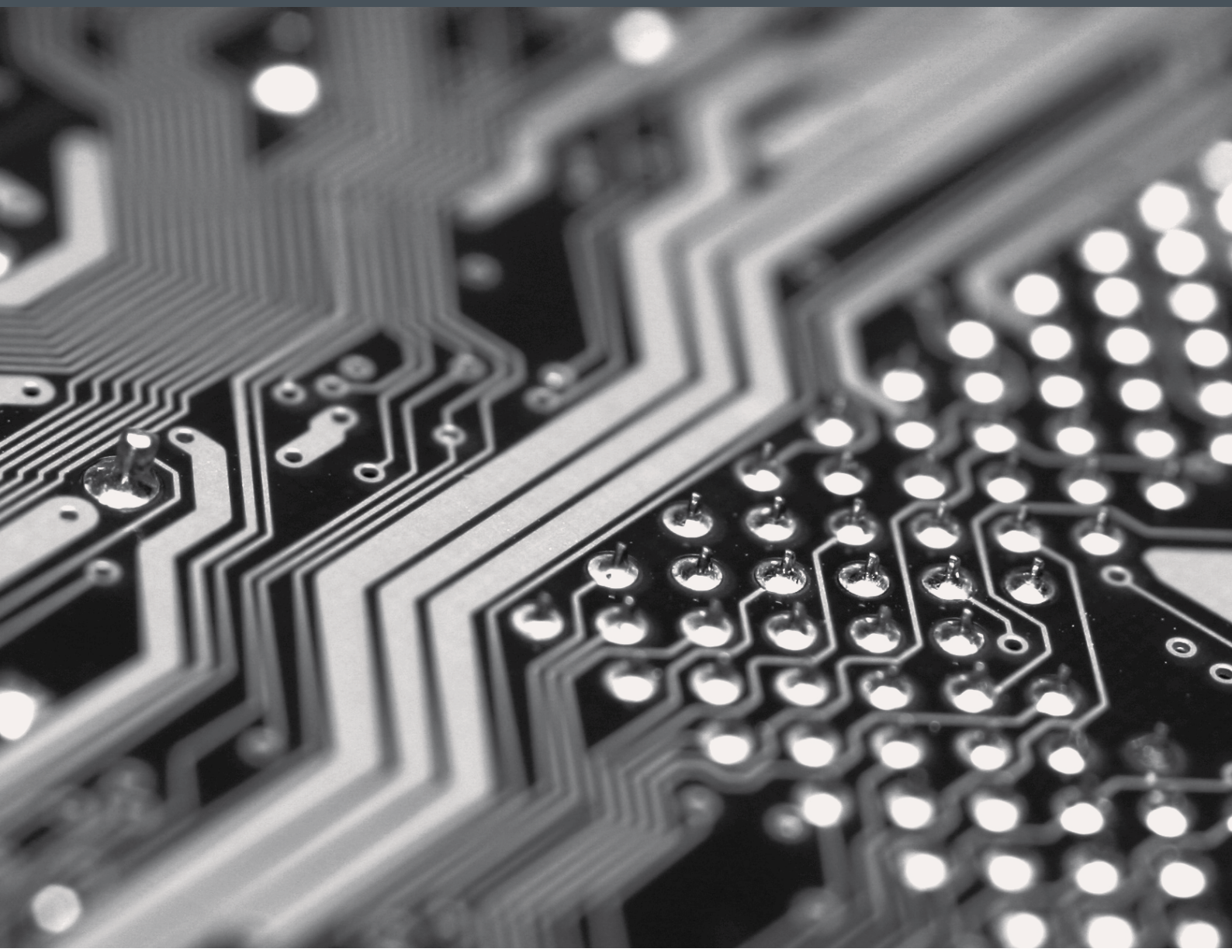
HFW

AUGUST 2019



THE RISE OF CYBERCRIME IN ASIA PACIFIC AND CONSIDERATIONS FOR ORGANISATIONS OPERATING IN THE REGION

This article was originally written for Asset Recovery Magazine

“Digital assets that are usually the subject of theft include personal information and data, trade secrets or more commonly, cryptocurrency.”

1. The Asia Pacific (APAC) region faces an increasing rate of cybercrime[1] and cases of serious digital asset theft have occurred there in recent years. This vulnerability is due to quicker digital transactions and greater internet connectivity combined with lacking cybersecurity investment and low awareness[2]. As avenues for transnational, digital payments diversify, APAC's digital economy is undergoing significant growth[3]. Asia is also a hub for the investment and trade of valuable digital assets. As cybercriminals choose to operate within APAC networks, it is unsurprising that the region is a focal point for the development of regulation, legislation and digital asset recovery mechanisms.

Defining cybercrime and its cost

2. Cybercrime can be broadly defined as computer related crime. The computer either is used as a tool to commit crime or acts as the target of a crime. A particular example is cryptojacking. This type of attack concerns the unauthorised use of a computer to mine cryptocurrencies. Cyberextortion often involves the threat of infection of a device with ransomware to coerce the recipient into submitting to a demand. Cybercriminals have also increased their capacity to launder money, steal digital assets and hijack networks. Digital assets that are usually the subject of theft include personal information and data, trade secrets or more commonly, cryptocurrency.

3. Cryptocurrency is a sought-after asset. The reported theft of the following values of cryptocurrency took place in 2019 alone[4]:

(a) 4.5 billion yen stolen from the cryptocurrency exchange Binance in Hong Kong, May 2019;

(b) US$4.3 million stolen from Bitrue in Singapore, June 2019; and

(c) 3 billion yen stolen from Bitpoint exchange in Tokyo, July 2019.

4. A study produced by the Center for Strategic and International Studies reported that the global cost of cybercrime reached US$544.5 billion in February 2018. A figure of US$171 billion is reportedly the damages cost of cybercrime to the APAC region alone[5].

Increased regulatory and legal framework

5. Governmental and regulatory bodies in APAC are recognising the need to balance technological innovation with risk management and user protection. The following countries have made progress in building the foundations of a strong regulatory and legislative framework, in which APAC's digital economy can prosper.

6. In terms of regulation in Japan, the Japan Network Security Association and Japan's Virtual Currency Exchange Association (JVCEA) are prominent bodies. The JVCEA is a self-regulatory body that applies rules to protect assets and focuses on developing anti-money laundering policy.

7. From a legislative perspective, Japan has made noteworthy developments. Japan's Parliament adopted the Cybersecurity Basic Act in 2014. The Act outlines government responsibilities and provides for the establishment of cybersecurity strategic headquarters.

1 Financial Sector Cybersecurity Requirements in the Asia-Pacific Region. William A. Carter and William D. Crumpler. April 2019. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190429_CarterCrumpler_APAC_WEB.pdf
2 Cyber Risk in Asia Pacific. The Case for Greater Transparency. Marsh & McLennan Companies. file:///C:/Users/ldr/Downloads/aprc-cyber-risk-in-asia-pacific%20(5).pdf
3 Is APAC's Desire to Lead Global Innovation in Digital Payments Working? A Tech Research Asia Report Commissioned by Temenos Group AG. https://www.temenos.com/globalassets/mi/wp/is-apac-s-desire-to-lead-global-innovation-in-digital-payments-working-.pdf
4 "Cryptocurrency thefts and fraud reach $1.2bn in Q1". Nikkei Staff Writers. 23 July 2019. https://asia.nikkei.com/Spotlight/Bitcoin-evolution/Cryptocurrency-thefts-and-fraud-reach-1.2bn-in-Q1
5 Cost of cybercrime continues to soar for Southeast Asian businesses. https://asiancorrespondent.com/2018/04/cost-of-cyber-crime-continues-to-soar-for-southeast-asian-businesses/

In October 2016, the Diet approved an amendment to the Act. The amendment increased the scope of parties which are subject to government evaluation for cybersecurity purposes. Special corporations and authorised corporations now fall within this scope.

8. In December 2016, the Hong Kong Monetary Authority launched the Cybersecurity Fortification Initiative aimed at banks and financial institutions established in Hong Kong. Three pillars form the foundation of the initiative - a Cyber Resilience Assessment Framework, a Professional Development Programme and a Cyber Intelligence Sharing Platform. Notably, the purpose of the Platform is to store information, data and intelligence on the subject of cyber-attacks. Authorised users can access this information and may find the platform useful as the initiative develops.

9. In Singapore, the Monetary Authority of Singapore provides a monitoring and regulatory function. The agency's reach expanded to include additional payment activities with the passing of the Payment Services Act in January 2019. This Act regulates payment systems and payment service providers in Singapore. Key objectives of this Act are to streamline the regulation of payment services and to mitigate the risks inherent in the payments value chain.

Mechanisms for recovery of cryptocurrency

10. Alongside an improving regulatory and legal environment, progress has been made in the realm of research and development.

11. Developments have been made in tracing stolen monies. The theft of US$534 million worth of NEM (XEM) cryptocurrency from the wallets of Japan-based exchange Coincheck is one of the largest recorded cryptocurrency thefts in history. It occurred in January 2018 and forced the exchange to consider ways of tracking the stolen coins. The NEM team developed an automated tagging system, where stolen funds could be tagged as tainted. Once stolen funds were deposited into regulated trading platforms, these deposits were verified. Accounts that received the funds were tagged and other exchanges could then be notified that they held these accounts on their platform.

12. Another mechanism for enabling the tracking and recovery of cryptocurrency is the analysis tool "The Taint Chain". This enables the tainting and tracking of stolen bitcoin. Developed by a team of researchers from the Department of Computer Science and Technology at the University of Cambridge, the tool employs an algorithm, which operates according to the FIFO (first in, first out) principle. This is based on a well-known English Chancery Court case[6]. The case considers that the first person to have paid in is the first person to be paid out where funds are withdrawn from a collective account. When applied to bitcoin wallets, the principle holds that if the first bitcoins paid into the wallet are stolen, then, (at least as a matter of English law), the first bitcoins paid out are also considered stolen.

13. Whilst digital economic activity and growth continues in the APAC region, the regulatory, technical and legal framework must keep pace with rising opportunities for cybercrime. Although rates of cybercriminal activity are high, we believe the aforementioned developments should inspire increasing confidence for organisations within APAC.

Research undertaken by Lydia Redman, Trainee.

6 Devaynes v. Noble 35 E.R. 781 (1816).

HFW has over 600 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our capabilities, please visit www.hfw.com

For further information, please contact:

DAVID HARBY
Senior Associate
T +44 (0)20 7264 8809
E david.harby@hfw.com

hfw.com

Americas | Europe | Middle East | Asia Pacific