Combating Cybercrime in Singapore

TER Kah Leng
NUS Business School, National University of Singapore

Singapore, the most globally connected country in the world, has not been spared the increasing frequency, complexity and scale of cyberattacks. These are viewed as a major business risk because of the impact on business operations and brand reputation and the exposure to legal risks. Cyberattacks will no doubt affect Singapore’s cyber connectivity and economic vibrancy. The high internet penetration rate, heavy digital reliance, ubiquity of the internet, proliferation of cybercrimes, their cross-border nature and the anonymity of the cybercriminal pose particularly challenging problems to law enforcers and other stakeholders. With these challenges in mind, this paper will evaluate the various measures that Singapore takes to combat cybercrime with particular reference to new laws that continually seek to keep pace with fast evolving cyber activities.

1. Growing cybercrime rates
The overall rise in cybercrime rates in Singapore, no doubt linked to the widespread use of the internet, social media and smartphones, underscores the need for a variety of responses. Cybercrime, the second most prevalent economic crime in Singapore, causes an estimated annual loss of $1.25 billion to 43% of companies. Not surprisingly, the number of cybercrime cases investigated has soared from 280 in 2015 to 691 in 2016. In 2016, individual victims lost $10 million through scams involving internet-banking accounts. The severity and prevalence of cybercrimes in Singapore is revealed in police statistics. In the first half of 2017, 349 cases of internet love scams caused victims a total loss of some $22.1 million, as compared to the $11.2 million lost in the same period in 2016 involving 277 reported cases. E-mail impersonation scams also rose from 124 cases in the first half of 2016 to 160 reported cases over the same period in 2017. The total amount lost increased from $17.4 million to $21.9 million in the relevant periods. Such scams involved hacking or spoofing email accounts and the transferring of funds by the victims to the scammers’ bank accounts. E-commerce scams, however, dropped to 900 cases from 1,006 cases in 2016. The victims were cheated into paying in advance for attractively priced items that were never delivered. The largest amount cheated in the first half of 2017 was $60,700.

2. A multi-pronged strategy
In view of the increase in cybercrimes, Singapore has adopted a multi-pronged approach to keep pace with the increasing sophistication of cybercriminals while seeking to become a Smart Nation. Strengthening the laws against cybercrime is essential, but the legal framework should be complemented with other measures including collaboration between the public sector and industry.

This was recognised back in 2008 when the Cybersecurity Awareness Alliance was formed to bring together Government agencies, private enterprises and professional associations to promote the adoption of essential cybersecurity practices. Under this initiative, the Singapore Computer Emergency Response Team (SingCERT) provides advisories to help businesses pre-empt cyberattacks.

In order to oversee and coordinate Singapore’s cybersecurity strategy, a central agency is needed and in 2015, the Cyber Security Agency of Singapore was formed. It is responsible for developing a robust cybersecurity industry and ecosystem by forming ties with industry and organising public outreach programmes to educate and raise awareness of cybersecurity. The Agency seeks to strengthen...

---

1 According to the McKinsey Global Institute Report 2016
2 Reported in the Straits Times, 29 August, 2017
cybersecurity in critical sectors such as energy and banking and to ensure effective coordination and deployment in responding to cyberthreats. The Agency’s “GoSafeOnline” website hosts cybersecurity tips and resources which businesses can access.

In 2016, the Ministry of Home Affairs launched the National Cybercrime Action Plan which lays down the Government’s key priorities and strategies to combat cybercrime. The Action Plan focuses on: (a) public education and outreach programmes; (b) enhancing the Government’s capability to combat cybercrime; (c) stepping up close partnerships with industry and institutes of higher learning and international engagement with foreign counterparts and (d) strengthening legislation and the criminal justice framework.

In reaching out to vulnerable groups such as the young and elderly, the Police work closely with schools and organisations such as the Media Literacy Council and with senior citizen engagement platforms such as the Infocomm Media Development Authority’s Silver IT Fest to raise cybercrime awareness among the elderly. In 2017 the Police set up public-private industry platforms to foster closer collaboration with software companies, telcos and banks on cybercrime detection and prevention as well as regularly reaching out to smaller businesses to share information on cybercrime and cybercrime prevention.

The Police are also directly involved in enhancing the Government’s capability to combat cybercrime. A key initiative was the setting up of a Cybercrime Command within the Criminal Investigation Department in 2015 to coordinate an effective response to cybercrime. It integrates police cyber-related investigations, forensics, intelligence and crime prevention capabilities. There is also a Cybercrime Response Team in every Police Land Division to assist Investigating Officers in responding to cybercrime reports through collecting and processing digital evidence. In 2016, the Police conducted five island-wide enforcement operations that targeted scams. More than 300 people were arrested in connection with scams involving some $1.8 million.

The Ministry of Defence is also involved in setting up the Defence Cyber Organisation which will take charge of developing the military’s cyber defence capabilities.

With regard to collaborating with institutes of higher learning, the Smart Nation and Digital Government Office will strengthen cross-agency coordination and collaboration with the National University of Singapore. This will provide data science training for 10,000 public servants to enable them to apply technology and use data and digital tools more effectively. The Secure Mobile Centre at the Singapore Management University aims to create a novel ICT solution to secure different layers of mobile computing systems and to assess the usability of such new technologies and solutions to conduct experiments in the real world settings so as to guard against cyberattacks in the future. Universities and Polytechnics are also offering cybersecurity programmes for those interested in pursuing cybersecurity education. Temasek Polytechnic and the Ministry of Home Affairs are developing a TALENT Lab to train students from institutes of higher learning in cybercrime investigations and forensics skills. This will be officially opened sometime in 2017.

The Government is also collaborating with industry to develop a cybersecurity workforce for Singapore. For example, under the Cyber Security Associates and Technologists programme, the Cyber Security Agency and the Infocomm Media Development Authority will work with industry and institutes of higher learning to attract new graduates and convert existing professionals from related fields.

The shortage of cybersecurity professionals is being addressed. The Cybersecurity Professional Scheme to double the existing pool of cybersecurity professionals in the public sector over the next few years was recently launched. Since many companies have highlighted the shortage of
cybersecurity professionals locally, there should be similar plans for the private sector. This is essential if cybersecurity across sectors is to be successfully implemented.

Small businesses do not invest as much in cybersecurity. Therefore, in the 2017 Budget, the “SMEs Go Digital” programme was announced to include cybersecurity and data protection. By the third quarter of 2017, the SME Digital Tech Hub will be set up by IMDA to provide technical advice to SMEs with more advanced digital needs e.g. cybersecurity and data analytics. The Hub will help to connect SMEs to ICT vendors and consultants and conduct workshops and seminars to help SMEs build their digital capabilities.

Since cybercrime cuts across national borders, there is a need to strengthen international partnerships in combating cybercrime. In 2016, the Ministry of Home Affairs, the Cyber Security Agency and the Attorney-General’s Chambers organised the first Association of South East Asian (ASEAN) Cybercrime Prosecutors’ Roundtable Meeting bringing together ASEAN cybercrime prosecutors to share their experiences and build network.

3. Strengthening the legislative framework
While the measures described above will no doubt contribute significantly to the promotion of cybersecurity and the prevention of cybercrime, they lack the legal enforcement of legislation. These measures should therefore be complemented by strengthening and updating the laws to keep pace with new and more sophisticated forms of cybercriminal activities, as well as by aggressively implementing and enforcing them.

The following examples are just the tip of the iceberg of the scale of cyberattacks and the number of victims affected. They underscore the need to update cybercrime laws.

In the first case, James Raj (calling himself “The Messiah”), hacked into various web servers including the server of Fuji Xerox and stole the statements of 647 private banking clients of Standard Chartered Bank which were stored on the server. The hacking was carried out from Malaysia. Various hacking tools were found on his computer. He was imprisoned for nearly 5 years. State prosecutors described the offences committed by Raj as "the largest, most prolific cyberattacks against IT systems in Singapore".

In the second case, James Sim, an administrative assistant, hacked into the accounts of 300 SingPass account holders and sold their personal data to a China-based syndicate involved in making sham applications for Singapore visas. The syndicate succeeded in obtaining 23 visas and enabling 20 Chinese nationals to enter Singapore.

Recently, the Ministry of Defence’s internet system was targeted in a cyberattack resulting in the theft of the personal data of 850 Singaporean national servicemen. The compromised system, however, did not contain classified or sensitive information. The computer systems of the National University of Singapore and Nanyang Technological University were also hacked into, the intention of which was to steal information related to government or research, according to the Cyber Security Agency of Singapore and the Ministry of Education. More recently, the personal data of 5400 customers of AXA Insurance were stolen in a cyberattack.

In these cases, the computer became the target of criminal conduct, if not the vehicle for the commission of offences. “Cybercrime” generally refers to two categories of crimes: first, offences that target the computer system such as hacking and denial of service and second, offences that are committed by using computers such as e-commerce scams, fraud and theft. The first category of computer crimes such as hacking or unauthorised access to or modification of computer data were first criminalised under the Computer Misuse Act 1993 (derived from the original English Computer
With changes in criminal behaviour and the need for the law to keep pace, the Act was amended between 1994 and 2012 to introduce new offences. In 2013, cybersecurity measures were introduced and the Act was renamed the Computer Misuse and Cybersecurity Act. The Act prohibits the following: unauthorised access to computer material: access with intent to commit or facilitate the commission of an offence; unauthorised modification of computer material; unauthorised interception of computer service; unauthorised obstruction of use of computer and unauthorised disclosure of access code.3

Further amendments were found to be necessary and the Computer Misuse and Cybersecurity (Amendment) Act4 was passed on 3 April 2017. The Act addresses the evolving tactics and tools of cybercriminals in carrying out elaborate attacks and the increasing scale and cross-border nature of cybercrimes. The Act also took into account the views of businesses and professionals in the internet services and cybersecurity industries to ensure that the provisions are practical and appropriately scoped. The amendments, whilst not numerous, are significant. They are a key initiative under the Government’s policies and strategies in the National Cybercrime Action Plan.

3.1 Criminalising trading in hacked personal information
This is a significant development in combating cybercrime. Personal information such as identity card numbers and residential addresses that are illegally obtained from a computer system can be misused for criminal activities. While hacking itself is a cybercrime, the new section 8A5 goes further to prevent hacked information from being misused for criminal purposes by “middlemen”, not directly involved in the hacking, from trading or dealing in the personal information if the offender knows or reasonably believes that such information has been obtained by committing a cybercrime. For example, a “middleman” may host a website to buy and sell hacked credit card information or in the case of James Sim, the China-based syndicate used the hacked information to make sham applications for Singapore visas. In certain cases it will be clear that the information could only be obtained through hacking such as credit card numbers purchased from a website that trades in hacked credit card information or an entire file of bank account passwords downloaded from such a site. However, it would be difficult for the prosecution to prove the particulars of the actual hacking offence for each of the pieces of information found on the illegal website, such as who originally hacked into the computer and when the hacking took place. For this reason, the new section 8A(6) does not require the prosecution to prove the exact details of the commission of the offence, although it still has to prove that the offender knew or had reason to believe that the personal information was obtained by the commission of a cybercrime. The particulars of the offence are fundamental issues and must be proven before a person can be convicted. However, it is apparent that the policy and legislative intent is to facilitate enforcement of and conviction under the new section 8A.

The new provision extends to obtaining or retaining hacked personal information as well as supplying, offering to supply, transmitting or making available the information. However, there are legitimate cybersecurity industry practices whereby cybersecurity professionals may deal with hacked personal information in the course of their work such as transmitting such information for the purpose of analysing a data breach or highlighting vulnerabilities in a system. Following consultation with stakeholders from the cybersecurity industry, telcos and ISPs, statutory exceptions were introduced. Section 8A does not apply where the information is obtained, retained, supplied or offered to be

---

3 Sections 3 to 8 of the Computer Misuse and Cybersecurity Act
4 Reference was made to corresponding legislation in the UK and Canada
5 The penalties are a fine not exceeding $10,000 or imprisonment not exceeding 3 years or both; for subsequent convictions, a fine not exceeding $20,000 or imprisonment not exceeding 5 years or both.
supplied, transmitted or made available for a legitimate purpose and the individual involved does not know or have reason to believe that the information will be used to commit a crime. This is intended to strike a balance between protecting the public interest and allowing the legitimate practices of the cybersecurity industry. It was asked during the second reading of the Computer Misuse and Cybersecurity (Amendment) Bill whether the exception extends to news agencies (e.g. Yahoo news, MSN news), journalists and researchers who make use of hacked information which has entered the public domain for the legitimate purposes of reporting or research. The Minister replied that while there is nothing wrong in reporting on the hacking incident or a researcher working with the hacked information for research purposes, it is another thing to publish the hacked personal information as part of the report or research findings. The latter may fall foul of the Personal Data Protection Act.

3.2 Criminalising dealing in hacking tools with criminal intent
“Hacking tools” are items that are capable of facilitating easy access to a computer. They include passwords, access codes, malware and port scanners which are readily available online. The new section 8B\(^6\) criminalises the act of obtaining or retaining such hacking tools and making, supplying or making available the hacking tools, with intent to commit or facilitate the commission of a computer crime.\(^7\) The requirement of a criminal intent is to ensure that legitimate access to such tools may be obtained by cybersecurity professionals. Hence, James Raj who had hacking tools in his computer will also be contravening section 8B.

3.3 Amalgamation of criminal charges
In view of the possibility that cybercriminals may commit multiple unauthorised acts against a computer over a period of time in preparation of an actual cyber-attack, the new section 11A allows the amalgamation as a single offence of two or more unauthorised acts against the same computer over a 12 month or shorter period. It also allows for enhanced penalties to be imposed if the combined acts result in higher aggregate damage.

3.4 Extra-territorial application of the Act with “serious harm” to Singapore.
It is apparent that a significant proportion of online commercial crimes are committed remotely by foreign syndicates. The internet is borderless and cybercrimes can be committed across geographical borders as in the case of James Raj who carried out the hacking from Malaysia. In view of this, the extra-territorial application of the Computer Misuse and Cybersecurity Act has been expanded to address the transnational nature of cybercrimes where criminals disrupt Singapore’s national security through computers located overseas. Previously, Singapore had jurisdiction only if the perpetrator or the computer, programme or data was in Singapore at the material time. This prevented enforcement actions against the perpetrator if he was overseas at the relevant time and had targeted an overseas computer, even though the act caused serious harm or risk of such harm in Singapore.

Accordingly, section 11 was amended to give Singapore extra-territorial jurisdiction over cybercrimes where the act causes or creates a significant risk of serious harm in Singapore. This will also ensure that police resources are not over-committed to pursue crimes that have little or no impact on Singapore. “Serious harm” means (a) illness, injury or death of individuals in Singapore; (b) disruption of or a serious diminution of public confidence in the provision of any essential services in Singapore; (c) disruption of or a serious diminution of public confidence in the carrying out of governmental duties and functions or (d) damage to the national security, defence or foreign relations of Singapore. Examples under (b) include publication to the public of the medical records of patients in a Singapore hospital and providing public access to the account numbers of customers of a bank in Singapore. Thus, if James Raj had published the hacked bank statements found on his laptop, he will also be contravening the amended section 11. Examples under (c) are providing public access to confidential

---

\(^6\) Similar penalties to section 8A

\(^7\) Other jurisdictions e.g. the UK have similar provisions
documents belonging to a Government Ministry and publication to the public of the access codes for a computer belonging to a statutory board.

Notwithstanding that cyberattacks pose considerable danger to the economy, the definition of “serious harm” does not include damage to the economy of Singapore, even though cyberattacks on Singapore e-commerce sites over a sustained period of time may seriously impact the businesses of Singapore companies. In responding to this concern during the second reading of the Amendment Bill, the Minister stated that the definition of essential services already takes into consideration the critical sectors that will affect the economy, should they be attacked. This paper suggests that “damage to the economy” should be specifically included, like in the UK Computer Misuse Act 1990. There, the new section 3ZA (inserted by the Serious Crime Act 2015) defines “serious damage of a material kind” to include damage to the economy. Where the unauthorised act results in serious damage to the economy, the maximum sentence is 14 years. It is also interesting to note that if the unauthorised act results in serious damage to the national security, the maximum sentence is life imprisonment. Such severe penalties appear to be justifiable in view of the wanton destruction that cybercrimes can wreak on the economy and national security.

In comparison to the UK position, no penalties, let alone enhanced penalties, are prescribed under the amended section 11 for cybercrimes that seriously harm Singapore. Section 9 of the Computer Misuse and Cybersecurity Act only prescribes enhanced punishment for offences involving protected computers, for which the penalty is a fine not exceeding $100,000 or imprisonment not exceeding 20 years or both. A “protected computer” includes one that is used directly for the security, defence or international relations of Singapore; the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services. While a cybercrime under the amended section 11 may attract enhanced penalties by virtue of section 9 if it involves protected computers, there is no additional penalty for causing “serious harm” to Singapore. This paper suggests that enhanced penalties should be specifically introduced into section 11 to prevent and deter cybercrimes that cause “serious harm” to Singapore.

While extra-territorial jurisdiction will be established in accordance with international norms and standards, the extra-territorial application of the Computer Misuse and Cybersecurity Act is likely to be complex as it will involve the laws of other jurisdictions. Furthermore, while the amended section 11 empowers investigations to be conducted against the perpetrator located overseas, there are major challenges. First, data hosted on the cloud may actually be physically stored in servers in more than one overseas location. This may affect investigation and enforcement. Second, the collaboration of foreign counterparts is essential for the purpose of conducting investigations and extraditing offenders to Singapore. Cybercrimes can be perpetrated anywhere in the world. Hence, the counterparts to extradition agreements are likely to be indeterminable. Furthermore, the inclusion of cybercrimes as extraditable offences is subject to agreement by the other contracting state. In any event, the Ministry of Home Affairs is working with the Ministry of Law to specify extraditable offences pursuant to the Act.

4. Conclusion
Cybersecurity is a collective responsibility. In order to prevent, detect and respond to cybercrime and cyberattacks, continued collaboration between industry, law enforcement agencies, institutes of higher learning and the public sector is vital to creating a safer and more secure online environment. Public education is essential and the Government has been running the Cybersecurity Awareness Campaign since 2011. The private sector should also strengthen cybersecurity awareness. After all, information or data is a valuable business asset and businesses must recognise cyber risks as an important business
risk. The private as well as public sectors should also grow cybersecurity expertise as more cybersecurity personnel are needed in both these sectors.

As technology is constantly evolving, laws have to be strengthened and new measures developed to build resilience to cybercrime. To achieve these, Singapore has implemented not only a robust legislative framework but also other measures as part of a comprehensive cybercrime and cybersecurity strategy to boost the safety and integrity of computers and data. These measures should also be implemented or enforced aggressively. However, as new forms of cyberattacks and cybersecurity threats emerge, it is recognised that a standalone cybersecurity legislation is required to complement the Computer Misuse and Cybersecurity Act. Accordingly, the Cybersecurity Bill was tabled in Parliament in 2017. The Bill is currently at public consultation stage and is expected to be enacted in 2018. Meanwhile, the Ministry of Home Affairs is reviewing other relevant legislation to deal more effectively with the evolving nature of cybercrimes.

Singapore’s policy against cybercrime is best encapsulated in the following words:

The Minister for Law stated that “to ensure Singapore remains an attractive place for investors and businesses to operate effectively and securely, computer crimes must be treated as seriously as other criminal offences…”

Similarly, the High Court observed that cybercrimes “not only undermine public and international confidence in the commercial integrity and viability of our computer systems, it also compromises Singapore’s efforts to position itself as a global e-commerce hub…IT security is a major consideration which many foreign companies take into account before deciding whether or not to develop and invest in the local IT sector…”

---

8 In the Second Reading of the Computer Misuse (Amendment) Bill on 30 June 1998.

9 PP V Muhammad Nusihan bin Kamal Luddin [2000] 1 SLLR 34