What's new with Cybersecurity in Singapore?

Abraham VERGIS & Nawaz KAMIL

With the increasing frequency of cyber-attacks, the new Cybersecurity Bill could not have come at a more pertinent time.

The worldwide WannaCry ransomware attack in May 2017 affected many companies including FedEx and Deutsche Bahn and even the United Kingdom's National Health Service. This halted services by locking data, making it inaccessible unless a ransom is paid in Bitcoin Cryptocurrency. The main goal of a cyberattack of this kind is the pay out from the ransom demands. According to A10 Networks, this type of ransomware attacks can cost up to S$1 million worth of disruption a day and also has the capacity to impair basic state infrastructure.

Another type of cyberattack that had also affected computer users in Singapore is the Advanced Persistent Threat (APT). In April 2017, it was found that the NUS and NTU computer networks were breached. APT attacks are designed to be undetectable in order to allow unauthorised access by hackers to gain confidential information, monitor usage and extract highly targeted intelligence.

Law firms value information security as breaches threaten clients' confidentiality and the firm's reputation. There has been an increase in cyber security breaches in law firms as they are seen by hackers to be the weak link in their ultimate targets' security.

In 2015, the Government established the Cyber Security Agency of Singapore (CSA) as the primary body to manage and coordinate the different areas of cybersecurity. The proposed Cybersecurity Bill creates the framework to uphold cybersecurity and on how to handle cyber threats in order to minimise the risk of disruption and harm.

According to the CSA, the Cybersecurity Bill has four objectives:

1. To provide a framework for the regulation of Critical Information Infrastructure (CII). The Bill formalises the duties that CII owners have in safeguarding the cybersecurity of the CIIs that they are responsible for.
2. To provide CSA with powers to manage and respond to cybersecurity threats and incidents.
3. To establish a scheme for the sharing of cybersecurity information with and by the CSA and for the protection of cybersecurity information. Note that this does not confer any right to the access to information subject to legal privilege.
4. To introduce a 'lighter-touch' licensing framework to regulate certain cybersecurity service providers as the Government sees it necessary that Singapore has credible cybersecurity services due to the increasing prevalence of cybersecurity risks.

With regard to protecting confidential information within the legal industry, firms must aim to use the standards set out in the Cybersecurity Bill as a minimum. The standard to which a firm is to adhere must be much higher. International disputes often involve high profile clients or controversial issues which may attract hackers whom interfere with the exchange of confidential information for various reasons like restricting access for ransom, to survey arbitration or litigation proceedings or strategies, or to expose confidential information.

When deciding on the type of cybersecurity to provide, a firm has to take the types of assets and clients into consideration. If the firm is engaged in an international dispute regarding commercially valuable assets like trade secrets or business strategies or easily monetised assets like consumer data or credit information, the firm and the client could face the risk of having this information stolen by the clients' competitors or by cybercrime organisations. It is not unheard of for a party to surveil the communication between clients and counsel

of the opposing side (as seen in *Libananco* v *Turkey*). Interferences can also come in the form of "hactivisits", these entities are mainly political activists who aim to expose certain information that may be damning to the client or firm – a recent example of this is the leak of the Panama Papers which were held under legal privilege by the law firm and corporate service provider, Mossack Fonseca.

Although the steps law firms have to take in order to ensure cyber safety for the client may go further than what the Bill requires, the Bill makes it so that other CIIs are kept safe and are protected from malware which in turn lowers the risk of cyber threats in law firms. The Bill also ensures that entities that provide cybersecurity services are credible and reliable, providing law firms with better and safer infrastructure to protect against cyber-attacks.

If you would like information on this area of law, please contact:

Abraham VERGIS
Managing Director
+65 6438 1969
abraham@providencelawasia.com

Nawaz KAMIL
Counsel
+65 6438 1969
nawaz@providencelawasia.com