GATEWAY LAW CORPORATION
Advocates and Solicitors | Notary Public | Commissioners for Oaths
Patent, Design and Trade Mark Agents

39 Robinson Road
#20 – 03
Singapore 068911
Telephone: (65) 62216360
Facsimile: (65) 62216375

Data Protection and Cybersecurity Law Update

The Cybersecurity Act 2018 and recommendations to combat cyberattacks[1]

Overview

In June 2018, Singapore's most serious breach of personal data took place, as hackers infiltrated the databases of Singhealth, Singapore's largest group of healthcare institutions, through the Integrated Health Information Systems (IHiS). IHiS runs the IT systems of all public healthcare institutions in Singapore. The targeted and meticulously planned cyberattack saw 1.5 million Singhealth's patients records assessed and copied while 160,000 of those had their outpatient dispensed medicines' records taken. Yet, it took 8 days before the cyberattack on the Integrated Health Information Systems (IHiS) was detected.

The Cybersecurity Act 2018

The Cybersecurity Act 2018 came into force on 31 August 2018, and was previously enacted in response to recent high profile attacks made on Singapore's public infrastructures. This new law creates a regulatory framework for the monitoring and reporting of cybersecurity threats to essential services in Singapore through the appointment of the Commissioner of Cybersecurity. It also creates a licensing regime that will require certain data security service providers in Singapore to be registered (generally those who are designated as an owner of a CII).

Recent Recommendations

A Committee of Inquiry (COI) was set up to investigate the cyberattack on Singhealth. On 10 January 2019, the COI put forward seven priority recommendations and nine additional recommendations to combat cybersecurity threats. These recommendations cover three broad aims: (1) to enhance the incident response plans for similar incidents; (2) to better protect SingHealth's patient database system against similar cybersecurity attacks; (3) to reduce the risk of such cybersecurity attacks on public sector IT systems which contain large databases of personal data. The recommendations are intended for SingHealth and IHiS to respectively adapt; however, all other organisations in Singapore can also adhere to it.

The first seven priority recommendations focus on improving cybersecurity policies and capabilities and embedding cybersecurity awareness into daily operations:

1. **Adoption of an enhanced security structure and readiness by IHiS and public health institutions.**

   Cyber security should be seen as a risk management issue and not just a technical issue. A multi-layered defence approach should be taken and security should not be dependent on just one line of defence.

[1] *The authors of this article would like to express their appreciation to Ms Samantha Ho, an intern at Gateway Law Corporation for her assistance and contribution to this article.*

39 Robinson Road
#20 – 03
Singapore 068911
Telephone: (65) 62216360
Facsimile: (65) 62216375

2. **Review of online security processes to assess their ability to defend and respond to advanced threats.**

   Identification and filling of gaps in the layers of security technology put in place is necessary. More importantly, application security, which encompasses measures to protect sensitive information, for email must be heightened and network security enhanced.

3. **Improvement of staff awareness on cybersecurity to better prevent, detect and respond to security incidents.**

   A security awareness programme should be implemented to educate staff on the firm's security policies and procedures, so that they know how to respond to a security breach if one occurs. IT staff must also be equipped with sufficient knowledge to recognize the signs of a security incident.

4. **Performance of regular enhanced security checks, especially on critical information infrastructure systems.**

   This involves vulnerability assessments, as well as reviewing and evaluating external vendor products. Penetration testing, red teaming (ethical hacking by an external, independent party) and threat hunting should be implemented on a regular basis.

5. **Privileged administrator accounts to be subject to tighter control and greater monitoring.**

   All administrators should use two-factor authentication (2FA) when doing administrative tasks. Instead of passwords, administrators should also use passphases which are harder to guess. This is because privileged administrator accounts are prime targets when a cyberattack occurs.

6. **Improvement of incident response processes for a more effective response to cyberattacks.**

   Early detection, proper investigation and timely reporting are key to preventing data breaches. An Advanced Security Operation Centre or Cyber Defence Centre should be established to be able to detect and respond to intrusions.

The seventh priority recommendation relates to collective security which is imperative due to the high degree of digitalisation and interconnectivity in Singapore. Partnerships between the industry and the Government can achieve a higher level of collective security when there is enhanced threat intelligence sharing and behavioural analytics is applied for collective defence.

7. **Formation of partnerships between industry and Government to achieve a higher level of collective security.**

39 Robinson Road
#20 – 03
Singapore 068911
Telephone: (65) 62216360
Facsimile: (65) 62216375

Cross-border, cross-sector partnerships should be strengthened. This includes partnerships with Internet service providers.

Collectively, these seven recommendations are priorities Singhealth and IHiS must immediately take steps to implement. However, the other nine recommendations put forward are similarly important to many organisations that are responsible for large databases of personal data.

The additional recommendations address specific issues raised in the course of the Inquiry, including technical, organisational, training, and process-related issues. They are: —

8. **Assessments of IT security risk to be carried out regularly.**

9. **Enhancement of safeguards to protect electronic medical records.**

10. **Better securement of domain controllers.**

11. **Implementation of a robust patch management process to address security vulnerabilities.**

12. **Implementation of a software upgrade policy with a focus on security.**

13. **Implementation of an internet access strategy that minimises exposure to external threats.**

14. **Incident response plans must more clearly state when and how a security incident is to be reported.**

15. **Competence of computer security incident response personnel must be significantly proved.**

16. **A post-breach independent forensic review of the system must be taken into account.**

Given that cybersecurity threats will only increase in sophistication, scale and intensity in the foreseeable future, organisations should do their part in protecting Singapore's cyberspace. Implementing the above recommendations would help improve one's cybersecurity posture and mitigate many risks concerning data protection.

GATEWAY LAW CORPORATION
Advocates and Solicitors | Notary Public | Commissioners for Oaths
Patent, Design and Trade Mark Agents

39 Robinson Road
#20 – 03
Singapore 068911
Telephone: (65) 62216360
Facsimile: (65) 62216375

Should you have any queries as to how this update may affect you or your organisation or require further information, please do not hesitate to email us.

Max Ng
Managing Director
Gateway Law Corporation

Email: max.ng@gateway-law.com

Amira Nabila Budiyano
Senior Associate
Gateway Law Corporation

Email: amira.budiyano@gateway-law.com

This article is intended to discuss the Cyber Security Act 2018 and recommendations put forward by the Community of Inquiry, and it is not intended to be comprehensive nor should it be construed as legal advice. This article is updated as at 20 January 2019.