Key lessons from the Public Report of the Committee of Inquiry (COI) on SingHealth cyber attack

February 2019

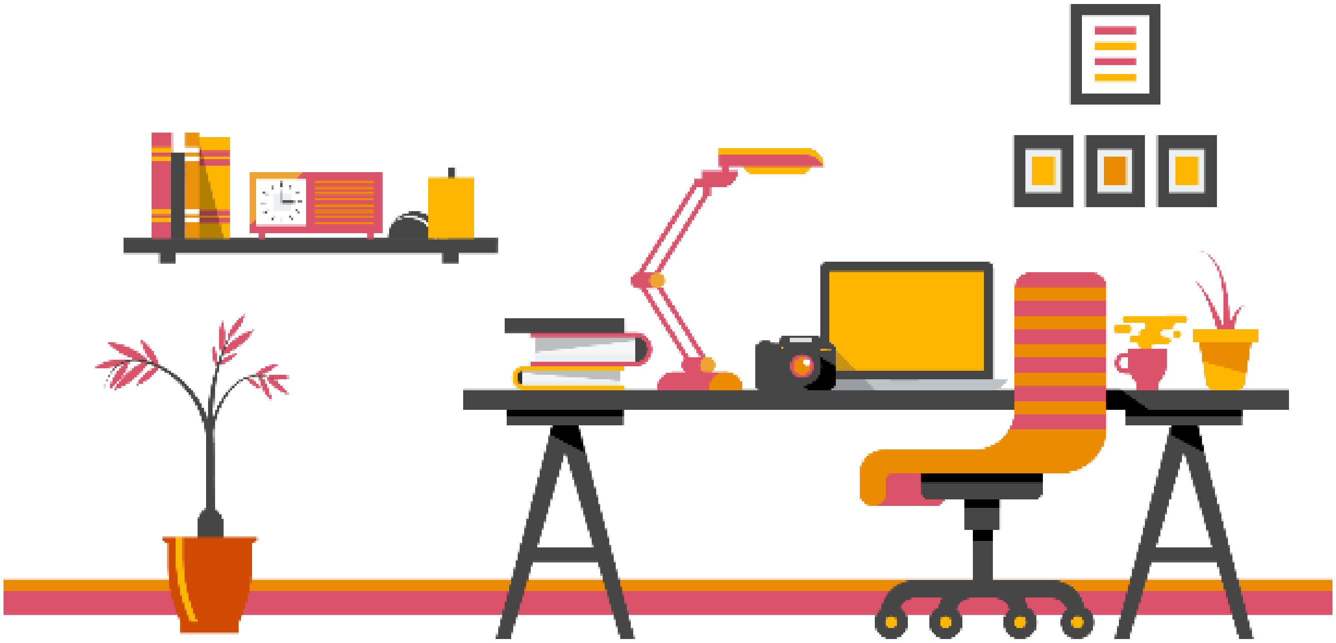
Table of Contents

Introduction

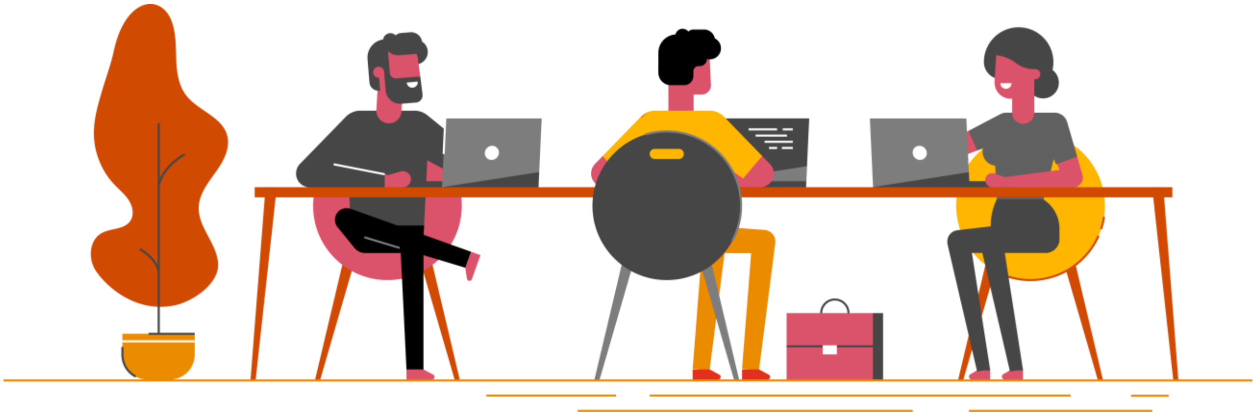
A cyberattack of unprecedented scale and sophistication in Singapore was carried out on Singapore Health Services Private Limited (SingHealth) in June-July 2018. In what is touted as Singapore's worst ever cyber data breach, hackers exfiltrated personal data and medication records of 1.5 million citizens, including that of Prime Minister Lee Hsien Loong.

The Committee of Inquiry (COI), formed to investigate the cyberattack released a 454-page report which detailed its findings and recommendations.

Here is our summary of the key takeaways from the COI's Report, our perspectives and recommendations on the immediate actions that organisations should take to lever up their cyber defence based on the lessons learnt from the SingHealth incident.



COI Report on SingHealth cyberattack



Five key findings

Employees did not have adequate levels of cybersecurity awareness, training, and resources to appreciate the security implications of their findings and to respond effectively to the attack.

Employees holding key roles in IT security incident response and reporting failed to take appropriate, effective, or timely action, resulting in missed opportunities to prevent the stealing and ex-filtrating of data in the attack.

There were a number of vulnerabilities, weaknesses, and misconfigurations in network and system that contributed to the attacker's success in obtaining and ex-filtrating the data, many of which could have been remedied before the attack.

The attacker was a skilled and sophisticated actor bearing the characteristics of an Advanced Persistent Threat group.

While cyber defences will never be impregnable, and it may be difficult to prevent an Advanced Persistent Threat from breaching the perimeter of the network, the success of the attacker in obtaining and exfiltrating the data was not inevitable.

16 Key recommendations

People

- Staff awareness on cybersecurity must be improved, to enhance capacity to prevent, detect, and respond to security incidents
- Competence of computer security incident response personnel must be significantly improved

Technology

- The cyber stack must be reviewed to assess if it is adequate to defend and respond to advanced threats
- Enhanced safeguards must be put in place to protect electronic medical records
- Domain controllers must be better secured against attack

Partnerships

- Partnerships between industry and government to achieve a higher level of collective security
- A post-breach independent forensic review of the network, all endpoints and the Sunrise Clinical Manager system should be considered

Process

- An enhanced security structure and readiness must be adopted by IHiS and Public Health Institutions
- Enhanced security checks must be performed, especially on CII systems
- Privileged administrator accounts must be subject to tighter control and greater monitoring.
- Incident response processes must be improved for more effective response to cyber attacks
- IT security risk assessments and audit processes must be treated seriously and carried out regularly
- A robust patch management process must be implemented to address security vulnerabilities
- A software upgrade policy with focus on security must be implemented to increase cyber resilience
- An internet access strategy that minimises exposure to external threats should be implemented
- Incident response plans must more clearly state when and how a security incident to be reported

PwC’s perspectives

Accountability of Senior Management

While the COI had noted the Security Incidence Response Manager (SIRM) and other middle management had erroneous interpretations of what constitute security incidences, the COI stated clearly that “one must not lose sight of the fact that the treatment of cybersecurity issues and incidents by staff and middle management is very much shaped by organisational culture”.

The responsibility to create and sustain a security culture ultimately lies with senior management. Moving forward, it may be the norm for senior management to be held personally accountable for future cyber security attacks. In an interview by Channel News Asia after the cyber attack on Singhealth was publicly revealed, CE Cyber Security Agency of Singapore (CSA), David Koh, said that CEOs and other decision-makers should be held accountable whenever a cybersecurity breach takes place. He observed that they “have not been held accountable” partly because such incidents are seen as a technical issue. It is worthwhile to note that the Cybersecurity Act 2018 holds owners of Critical Information Infrastructure liable for non-compliances, with potential penalties of fines and imprisonment.

Occurrence of a cyberattack is inevitable, but denying the attacker his objective is not inevitable

One of the COI’s key findings states that “While our cyber defences will never be impregnable, and it may be difficult to prevent an Advanced Persistent Threat from breaching the perimeter of the network, the success of the attacker in obtaining and exfiltrating the data was not inevitable.”

Similar to the physical world where police and security forces have to be right all the time in disrupting terror plots but terrorists only need to get through once, there is no 100% security in the digital world.

From a technology perspective, there are no products, software or systems without vulnerabilities. Zero-day vulnerabilities exist. Sophisticated and well-resourced attackers will take advantage of such vulnerabilities to penetrate the networks.

Even with the most technologically advanced and capable cyber defence system in place, the weakest link will still be the human element. It would not be reasonable to expect all employees to be ever vigilant and constantly updated on the latest cyber attacker modus operandi. Mistakes will happen.

[1] A zero-day vulnerability is a vulnerability in a system or device that has been disclosed but is not yet patched

PwC’s perspectives

Taking Leadership and Assuming Responsibility

Successful cyber attacks are call-to-action for companies and organisations operating in Singapore. The mindset that “it will never happen to us” has to change. Geography offers no protection, and in fact, favors the cyber attackers. In the digital world, we are all connected regardless of physical location. Our computers and networks can be reached by a hacker on the other side of the world, under a different jurisdiction and beyond the reach of our authorities. We are increasingly connected in cyberspace where the rules of engagement that we are familiar with in the real world breakdown.

The number and frequency of attacks from sophisticated and advanced hackers will continue to rise in the foreseeable future. The responsibility to protect the organisation’s cyber assets cannot rest solely on the shoulders of the Chief Information Security Officer. It is important for senior management to take collective responsibility in formulating a proactive cyber security strategy, with a pragmatic and balanced approach to minimise the impact of cyber incidents and manage the risk of cybersecurity effectively.

Our recommendations: Immediate cyber defence action plan

The five key findings and sixteen recommendations can be useful reference points for organisations and companies in Singapore. Organisations should always adopt a holistic, comprehensive and long-term approach to protect themselves from cyber threats. However, there are immediate actions that can be taken to quickly strengthen your organisations' cyber defences.

Review cyber security strategy

Recent cyber incidents provide an impetus to take stock of your cyber defence strategy and assess if your strategy is still aligned with your organisation's needs, resources and risk appetite.

Your strategy should incorporate a defence-in-depth concept. Such a defence concept would consist of deploying multiple layers of mechanisms to protect your valuable systems and data. It would prioritise more layers of protection for more important assets. Even if a single layer is compromised, there would be other protections in place to thwart the attacker.

The strategy will need to be reinforced by a strong security culture and awareness across all levels in the organisation, and not only to be reliant on the security personnel. For example, the external-facing staff are often the first to notice a security incident. From our experience working with many MNCs, in most of the cyber incidences and data breach cases, there is a social engineering component where hackers target end users to gain initial foot hold into the environment. Addressing end user security awareness is a very important, but often overlooked, part of an organisation's cyber security strategy.

In order to cultivate strong security culture, buy-in at the highest organisational level is essential. Senior management needs to recognise and believe in the criticality of cyber security and act as champions of cyber security. The strategy should involve actions by senior management to demonstrate their commitment and emphasis in this area so as to positively influence their employees' behavior toward cybersecurity.

An effective cybersecurity defence requires every individual to play a part. Cybersecurity is not the task of single department in an organisation. It only requires a weak link to undermine all the investments and effort by every other person in the organisation. A holistic cyber security strategy reinforced by a strong security culture will involve every person in the organisation.

Have full visibility over organisation's entire IT environment

Inside (Your environment) - A security hygiene feature which is often neglected is the full visibility of your IT environment by the security team. Visibility allows the security team to know which asset is the most critical, most vulnerable, and most accessible to attackers. Having visibility over data and IT assets is a basic cyber hygiene and an important advantage of the cyber security team against attackers. However, there is often a lack of visibility due to the inherently complex IT environment, operational constraints and lack of supporting technology.

Outside (The dark web) - Criminals leverage on the dark web to transact illicit information, tools and services. However, the information available can be used to assess if you are currently targeted, or worse, if you have already been compromised and your organisation's sensitive data is being sold on the dark web.

An independent assessment will provide a visibility of the existing system and an unbiased view of the level of cyber security readiness of the organisation. It will provide a firm basis to determine how best to protect your crown jewels and progress forward in meeting regulatory requirements.

Our recommendations: Immediate cyber defence action plan

Heighten Situational Awareness

In the current landscape, it is acknowledged that attackers are increasingly sophisticated and will find a way to breach your network. The security mindset will require a shift towards accepting that breaches are inevitable, and increasing focus on active monitoring of your networks to detect intrusions. To heighten your overall situational awareness of the threats, you should invest in both technology and people.

Technology - "The pace of cyber development is like the pace of computer development. Basically a computer generation is one and a half years. With cyber, it's even less. Every year to a year and a half, comes a new generation of cyber techniques," Prof. Yitzak Ben-Israel, Chairman Israel Space Agency and Israel National Council for R&D told Times of Israel in an interview on 22 June 2017.

The security solutions that have been implemented will continue to be useful. However, as the attackers evolve their techniques and tools, your cyber security defences should not remain static. There will always be emerging technological solutions that are effective against evolving threats and will be complementary to your existing portfolio of security solutions. It will be worthwhile to be updated regularly on and take a deeper look at promising technologies, and consider how they can be implemented to bring your security defences to the next level.

People - Even the best technology will be ineffective if your people are not adequately trained. Emphasis must be placed on improving your employees' cyber security awareness and knowledge of the relevant processes and procedures. Training is a not a one-off affair. Training your people should be continuous, incremental and be hard-coded into your organisation's people development system.

Besides relying on organic resources, it would be advantageous to engage independent firms to conduct periodic tests on your networks. These tests, such as threat hunting, penetration testing and network forensic, would further heighten situational awareness by identifying gaps and blindspots that may have been missed.

Improving Response Capabilities

The speed of detection and effectiveness of your response to any cyber breach will be the key determining factor of how much damage your organisation will suffer.

Process - There are many incident response plan templates, workflows, playbooks and best practices available for reference. In fact, many organisations should already have their own incident response plan. However, from our experience, organisations that exercise their cyber response drill regularly make much faster and better decisions during the crisis time and therefore manage cyber incidents much more effectively. A well-conducted cyber response drill is an effective way to raise employees' cyber security awareness as well as to train people on their decision making capability under pressure, which is critical for handling any cyber incident. The drills should be conducted not just within the IT Security team, but also at some stages involve all other stakeholders in the risk management team, crisis management team and senior management team. A drill could be carried out in multiple forms, from a table top exercise to a cyber range workshop to a red team/advisory simulation on the organisation. Depending on the organisation's resource, we recommend to use a combination of different drill forms to ensure effectiveness and sustainability.

Conclusion

Attacks of greater sophistication and by actors with greater resources will happen, or are already on-going. Singapore’s digitisation efforts through the SMART Nation initiatives will greatly benefit the population and economy, but will also increase the surface area that attackers can target.

The onus is on leaders of every organisation to be cognisant of the ever-changing cyber threats, take ownership of the strategy to address the risks and personally lead the effort to protect your organisation.

If you have any queries, please do not hesitate to call your usual PwC contacts or any of the following PwC subject matter experts:

Tan Shong Ye
Digital Trust Leader
shong.ye.tan@sg.pwc.com

Jimmy Sng
Partner, Cybersecurity
jimmy.sng@sg.pwc.com

Freddy Wee
Partner, Cybersecurity and Privacy
freddy.wee@sg.pwc.com