Health

A Case for Increased Vigilance:

How a Layered Approach to Cyber Security can help your Healthcare Organisation

This article is part of a series of articles about Telstra Health's Layered Approach to Cyber Security. You can access practical guidance on implementing a Layered Approach to Cyber Security at the People layer here, the Process layer here and the Technology layer here.

An increasing number of cyber incidents against health organisations have cast a spotlight on the role cyber security plays in healthcare. Understanding the risks of delivering digitally enabled care and protecting health information has never been more crucial for healthcare organisations. In this article, we suggest that applying a layered approach is a practical approach to increasing your healthcare organisation's cyber security maturity and helping to defend defending against increasingly complex cyber threats.

Why Cyber Security should be a Top Priority for Healthcare Organisations

Australian healthcare organisations are increasingly being targeted by cyber criminals, with data breaches occurring because of human error, system failure and malicious attack. Statistics reported by various Australian cyber security organisations all convey the same message: healthcare organisations need to do more to defend against evolving cyber threats.[1-3]

Figure 1: Indications of the Australian healthcare industry as a lucrative target for cyber criminals.

The health sector was the **highest reporting industry** for data breaches from July 2019 to December 2020, according to the Notifiable Data Breach (NOB) scheme

The healthcare industry was reported as the **most affected by ransomware** jn FY19-20, according to the Australian Cyber Security Centre (ACSC)

Only 33% of respondents complete a cyber security risk assessment annually, according to a 2017 survey conducted by HISA's Community of Practice

So why healthcare organisations? There is a high level of intrinsic and extrinsic value associated with healthcare data. Stolen healthcare data is typically worth more than records from other industries because of the high value associated with personal information. An attacker can use this data to access private health care benefits, steal and utilise credit card details, sell the data on the black market to other cyber criminals and/or use it to extort patients. Healthcare sector plays an important role in Australian society, some hostile actors may try to cripple these critical services to create social havoc.

Healthcare organisations often have a low level of cybersecurity maturity making them vulnerable to attacks. The use of legacy and/or unsupported systems with outdated security controls continue to prevail. A limited security culture and cyber awareness across healthcare organisations can lead to data breaches caused by human error. Also, accessibility to health information systems can be challenging for clinicians as they must manage a variety of credentials, adding to the complexity of maintaining rigorous cyber security controls.

Cyber security is often perceived as an IT problem that warrants an IT response. In this series of articles, we turn this common misconception on its head, and explain why cyber security is an organisational concern which requires an organisational response.

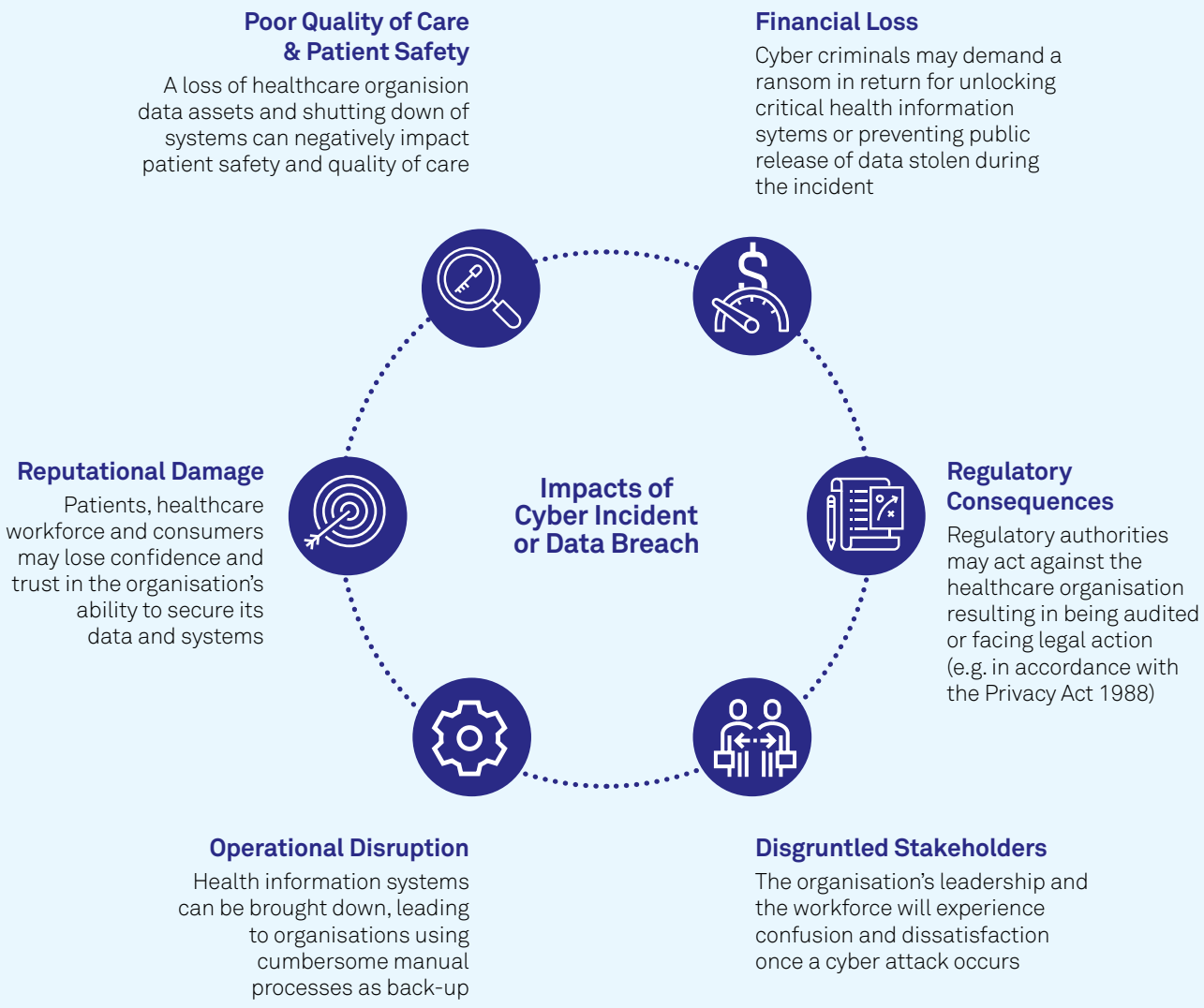
What are the Risks of Complacency?

As new and disruptive technologies become more prevalent, the volume and complexity of cyber threats is expected to escalate. An increasing demand for information sharing, and interconnectivity introduces additional attack types.

For example, the increasing interconnectedness between end user devices with Bring Your Own Device (BYOD) solutions and Medical Internet of Things (IoT) has contributed to end point complexity, which has introduced vulnerabilities that cyber criminals can exploit. Maintaining a 'wait and see' approach is no longer feasible in defending against evolving cyber threats.

The impacts of a cyber incident or data breach on a healthcare organisation can be crippling. This is illustrated below in figure 2.

Figure 2: The impacts on a healthcare organisation can be detrimental and far reaching



Recognising a Cyber Threat when you see one

Cyber criminals are highly organised and can take advantage of a rapidly changing digital health landscape. Attack tactics can be layered, aiming to exploit vulnerabilities within healthcare organisations. The following tables outline the common sources of threats and types of attacks that impact the healthcare industry.[1]

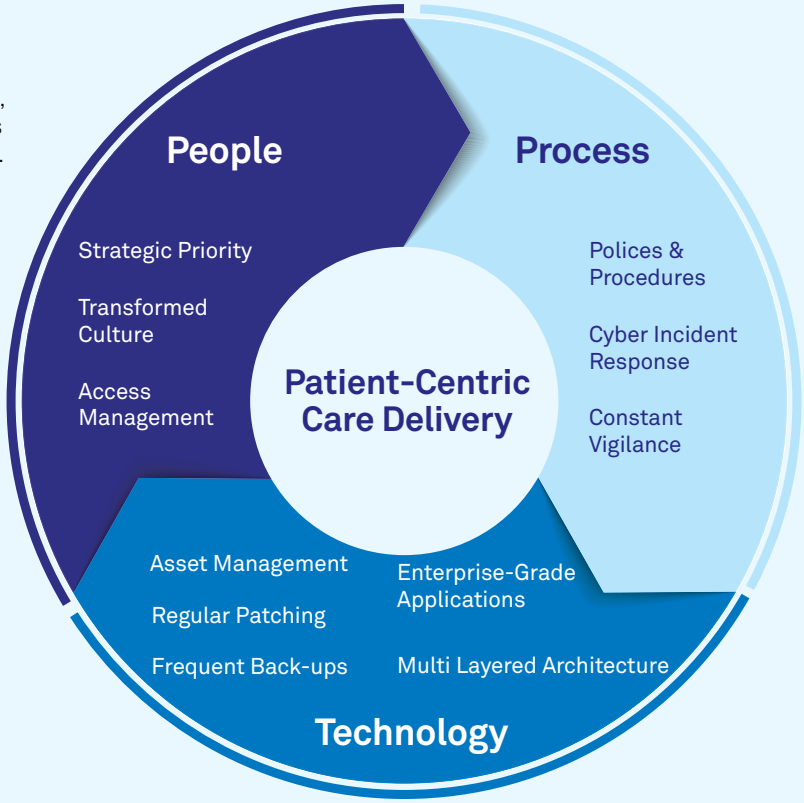
Sources of Cyber Threats	Description
Trusted insider	A 'trusted insider' is anyone who has been given access to a business's systems and physical premises. This includes past and current employees, contractors and visitors. Businesses should make sure that employees can be trusted with assets which if compromised would be of security concern.
Threat actors	Financially motivated criminal groups target the healthcare industry via ransomware attacks (described below). While medical data is typically the target of breach, trends show an increase in breaches involving personal data and credentials.[4]
Malware	Malicious software designed to harm any health information system, medical device or health organisation's network. The intention is to steal healthcare data or shut down health information systems and/or devices. There are many different forms of malware including trojan horses, viruses, ransomware, botnets and spyware.
Ransomware	This is a type of malware which can penetrate an organisation's security layer and encrypt health information systems, files or databases. The affected systems, files or databases become inaccessible and unusable, with cyber criminals often demanding ransom payment to restore normal operations. The healthcare sector was one of the top five sectors that were affected by ransomware reported to the ACSC in 2019-20 FY2.
Phishing	Phishing is a type of social engineering attack and is usually carried through emails, instant messaging or text messaging. The intent is to direct the user to enter personal, confidential, sensitive or identity management data on a fake website that feels real and use those details to access the healthcare organisation's systems.
Spear phishing	Spear phishing is similar to phishing; but it involves cyber criminals sending electronic communications targeted towards a specific individual, organisation or business. Spear-phishing attacks are personalised or modified to appeal to the target. Malicious cyber actors are capitalising on the public desire for COVID-19 related information by generating specific COVID-19 themed websites to capture personal information.[5]
Insider Threat (careless)	Security breaches can happen due to careless user errors such as sharing log-in details to a system in a clinic or ward, leaving devices unlocked or sending emails to the incorrect recipient. This is because of poor controls, processes or limited cyber awareness amongst healthcare employees. Shared workstations are the norm in healthcare organisations, and this tends to increase cybersecurity risks. Human error was one of the highest contributors for data breaches for health service providers, as outlined in the Notifiable Data Breach report for 2020.[1]
Insider Threat (malicious)	This type of threat may originate from internal, external of former employees who may have malicious intent against the healthcare organisation. They may be familiar with the organisations security policies and procedures, as well as its vulnerabilities. With the introduction of remote working, the risk of malicious insider threat has increased due to limited monitoring and visibility. For example, employees using their unsecure personal networks may erroneously download malware or use unauthorised methods to download and share data.

Adopting a Layered Approach to Cyber Security in Healthcare

Cyber criminals can use multi-layered and highly sophisticated attack tactics to target vulnerabilities in healthcare organisations. In response, healthcare organisations should apply multiple layers of defence by leveraging a well-equipped framework. This involves being proactive with cyber security, and applying controls for cyber threat identification, prevention, detection, response and recovery dimensions, across the People, Process and Technology layers.

In this series of articles, we will explain Telstra Health's Layered Approach to Cyber Security in depth and provide you with practice advice on what you can do to uplift your cyber security maturity across the People, Process and Technology layers.

Figure 3: Telstra Health's Layered Approach to Cyber Security is a holistic framework, encompassing People, Process and Technology



Not sure where to start?

We have an established Cyber Security Advisory practice which can provide you with guidance and support, wherever you are in your cyber security journey. We can help you define your cyber security strategy, build a business case for cyber security investment, review your security architecture, assess your threat profile, increase your workforce's cyber awareness and work with you to address a specific area in which you are having challenges.

Want to find out more? Let's start a conversation

This blog article is informational in nature and is not intended to be a substitute for professional advice.

References

1 Office of the Australian Information Commissioner, 2021, 'Notifiable data breaches statistics', available from: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/.

2 Australian Cyber Security Centre, 2020, 'Ransomware in Australia', available from: https://www.cyber.gov.au/sites/default/files/2020-10/Ransomware%20in%20Australia%20%28October%202020%29.pdf.

3 Health Informatics Society of Australia, 2018, 'Cybersecurity across the Australian Healthcare Sector', available from: https://www.hisa.org.au/wp-content/uploads/2018/07/HISA-Healthcare-Cybersecurity-Report_June-2018.pdf.

4 Verizon, 2020, 'Data Breach Investigation Report' available from: https://enterprise.verizon.com/en-au/resources/reports/dbir/

5 Australian Cyber Security Centre, 2020, '2020 Health Sector Snapshot' from: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/2020-health-sector-snapshot

To discuss how we can support your organisation

1800 HEALTH (1800 432 584)

Advisory@health.telstra.com

telstrahealth.com

Health