Health

A Layered Approach to Cyber Security:
How Processes Can Tip the Scale Against Cyber Threats

This article is part of a series of articles about Telstra Health's Layered Approach to Cyber Security. You can find out more about our overall approach here, and access practical guidance on the People layer here and the Technology layer here.

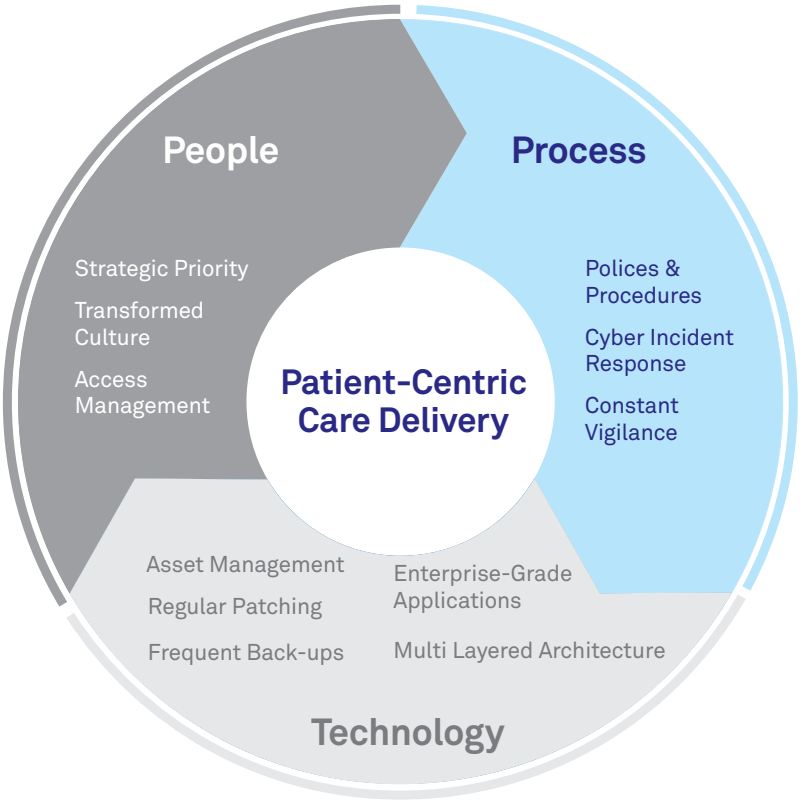
In *"A Case for Increased Vigilance: Adopting a Layered Approach to Cyber Security in Healthcare"* we covered the cyber security landscape in Australian healthcare, the types of cyber threats and the devastating impacts cyber attacks could have on healthcare organisations. We recommend a layered approach to defending against multi-faceted cyber attacks, and in this article we explain how your processes arm your workforce with the 'know-how' to manage cyber threats.

A survey conducted in 2018 by the Health Informatics Society of Australia (HISA) indicated that more than 45% of respondents were unclear on what to do in an event of a cyber incident and 35% of respondents were unaware of any cyber security processes that were in place1. When your organisation experiences a cyber attack, your IT professionals, clinicians, healthcare administrators and operational teams need to be aligned, informed and ready to minimise the negative impacts. Your cyber security activities are most effective when your processes enable your workforce to be proactive instead of reactive.

In Telstra Health's Layered Approach to Cyber Security, the process layer defines the activities and documentation which inform your healthcare workforce on how to identify, manage and respond to cyber incidents. The process layer is underpinned by policies and procedures, cyber incident response plans and a regular cadence of threat detection and reporting.

Figure 1: Unpacking the Process layer in a layered approach to cyber security

Telstra Health's Layered Approach to Cyber Security



We understand it's challenging to get your process layer defined and working effectively. Here are three practical tips to help you build your process layer defences:

01. Get the basics right: keep your cyber security policies and procedures simple and educate your staff

Your cyber security policies and procedures are documents that detail how you will implement your cybersecurity strategy at a practical level, and outline the activities and expectations for your workforce. For busy healthcare employees who are focused on delivering care, your policies and procedures won't be read if they can't be easily consumed. Communicating regularly about policy and procedure updates keeps your workforce engaged and reminded of their role in securing the organisation. In an agile workforce environment, consider supplementing your formalised policies and procedures with regular updates at team meetings, electronic dashboards, posters in staff rooms or organisation wide communication applications.

To inform the development of your policies and procedures, we recommend that you leverage external legislation documents such as the My Health Records Act and Privacy Act (the My Health Records Rules and Regulation), Australian Privacy Act 1988, and the Data Privacy Amendment, Notifiable Data Breaches Act 2017. Legislative documents can help you understand government-directed cyber security guidelines, key focus areas for reporting and the potential consequences of experiencing a cyber incident.

02. Have a plan: define, communicate and test your cyber security incident response plan

- A cyber security incident response plan contains repeatable procedures, which can be actioned in the event of a cyber security incident. As a minimum your response plan should:
- Include clearly defined communication pathways and responsibilities
- Detail an incident response team which brings together multiple functions to respond to the incident.
- A schedule for regular review and updates to the plan by the Incident Response Team
- Describe how you will regularly test your cyber incident plan at every level. You can do this by running 'cyber security simulations' which allow you to identify gaps in your plan and understand how your healthcare organisation react toa cyber threat.
- Detail how it is aligned to the organisation's wider business continuity plan

A business continuity plan aims to maintain business functions or quickly resume them in the event of a major disruption, whether caused by a fire, flood, cyberattack or terrorist attacks. Both plans need to be regularly tested and updated to defend against evolving threat landscapes.

Figure 2 explains how the cyber incident response plan is developed and applied across four key phases of incident response management:

03. Be vigilant: maintain an effective cyber risk assessment and mitigation process

Risk management plays a big part in cyber security. Being proactive and adopting an effective risk assessment and mitigation approach is crucial for getting ahead of cyber criminals. This means driving a regular cadence of threat detection, analysis and reporting that can help your organisation surface trends and identify vulnerabilities in your defences. It's also important to be aware of the regulatory landscape and your reporting/compliance requirements, and to comply with them appropriately.

Define clear cyber security measures that will supplement your reporting process, which should be driven by your leadership across your healthcare organisation. Not only does it measure the effectiveness of the organisation's cyber security policies and procedures, it can also lead to developing more effective controls.

Figure 2: Four focus areas your cyber incident response plan should address

Preparing the Cyber Incident Response Plan

When defining a cyber incident response plan:

- Outline your workforce's roles and responsibilities
- Outline secure communication guidelines in the event of a cyber incident
- Define the cyber incident response process, including how the incident is identified, assessed and treated, and how the business recovers
- Seek the input of key stakeholders such as your executive leadership team, clinicians, HR, legal, risk, IT and third party vendors supporting your health information systems

Responding and Recovering

During and after a cyber incident, you should refer to your cyber incident response plan for guidance on how to:

- Identify, contain and recover from the cyber incident
- Analyse the cyber incident, investigate the root cause and understand the impacts across your healthcare organisation
- Execute recovery activities such as restoring data or systems and enable business as usual activities
- Communicate internally, and externally if required (e.g. public communications, regulatory authorities etc.)

Understanding the Lessons Learnt

Your cyber incident response plan should incorporate any lessons learnt by:

- Reviewing the cyber security incident, and reporting on what happened
- Engaging an expert to review your cyber security defenses
- Updating your policies, procedures and cyber incident response plan
- Educating your workforce on the cyber incident and how it can be prevented in the future

Not sure where to start?

Our Cyber Security Advisory practice provides cyber security services to healthcare organisations across Australia. We offer services in cyber security audit and compliance management, cyber security risk assessment, cyber security policy and procedure development and implementation, cyber security analytics and reporting, and cyber security incident response planning.

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. Health Informatics Society of Australia, 2018, 'Security Check of Australia's Healthcare Information (Final Report)', available from: https://www.hisa.org.au/wp-content/uploads/2018/07/HISA-Healthcare-Cybersecurity-Report_June-2018.pdf.

To discuss how we can support your organisation

1800 HEALTH (1800 432 584)

Advisory@health.telstra.com

telstrahealth.com

Health