Health

A Layered Approach to Cyber Security:
Why People are your Most Valuable Asset

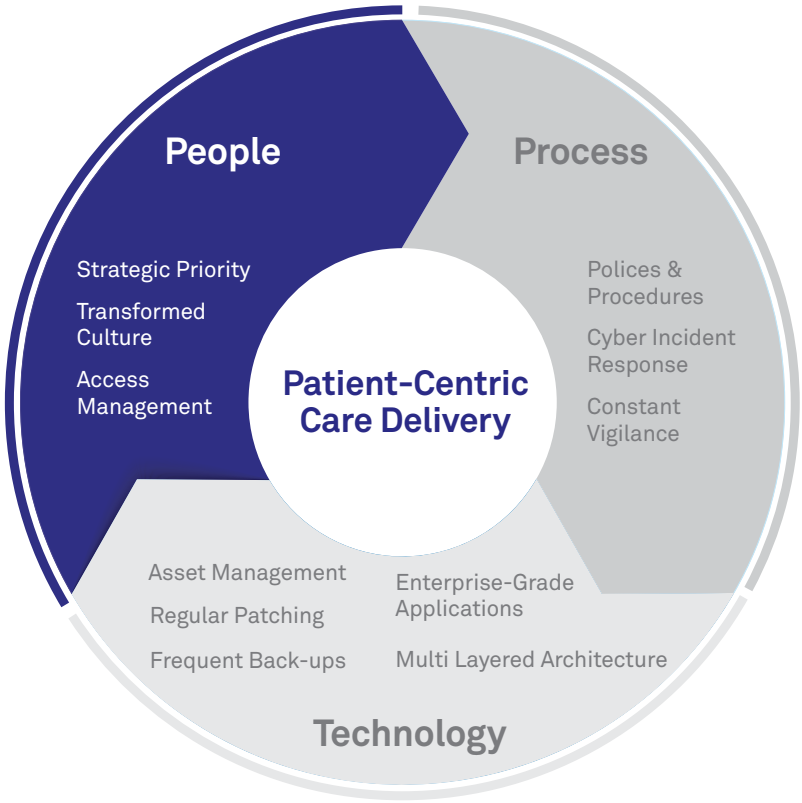
This article is part of a series of articles about Telstra Health's Layered Approach to Cyber Security. You can find out more about our overall approach here, and access practical guidance on the Process layer here and the Technology layer here.

In *"A Case for Increased Vigilance: How a Layered Approach to Cyber Security can help your Healthcare Organisation"* we explored the escalating importance of cyber security for healthcare organisations, and the value of applying a layered approach to cyber security. In this article we explain the role people play in defending your organisation against cyber attacks, and provide practical advice for bolstering your people defences.

According to the Office of the Australian Information Commissioner (OAIC), human error was the most common source of data breaches within healthcare in 2020, accounting for 57% of total data breaches reported by the sector1. The threat posed by people, whether it be through lack of knowledge, human error or malicious intent, can be significant to the cyber security of healthcare providers. Yet, when educated and empowered, people can serve as your most powerful line of defence to a cyber attack. In Telstra Health's Layered Approach to Cyber Security, an organisation's leadership and staff prioritise and take responsibility for cyber security, and appropriately embed it into the organisational culture. But getting to this point takes time, investment and effort across all levels of the organisation.

Figure 1: Focusing in on the People layer in a layered approach to cyber security

Telstra Health's Layered Approach to Cyber Security



So, where should you start? Here are three practical tips to help you transform your healthcare workforce into your most valuable defence against a cyber security attack:

01. Change starts from the top: make cyber security a strategic priority with executive level support

Send a message to your workforce, stakeholders and patients by transforming cyber security from a technology issue into a strategic one. As an executive team, recognise the important role cyber security plays in enabling your organisational strategy and ensuring the delivery of high-quality patient care.

Robust cyber security requires effective governance and decision making. If you are a relatively large organisation, consider creating a dedicated role at the executive level – the Chief Information Security Officer or CISO – to drive accountability for uplifting your cyber security capability and overseeing the smooth function of cyber security operations. Alternatively, if you are a smaller organisation, you should embed information security responsibilities into the role of the Chief Information Officer (CIO). By driving change at the top, you will create the foundation required for a patient-centred culture of security.

02. Transform your culture: create a patient-centred culture of security

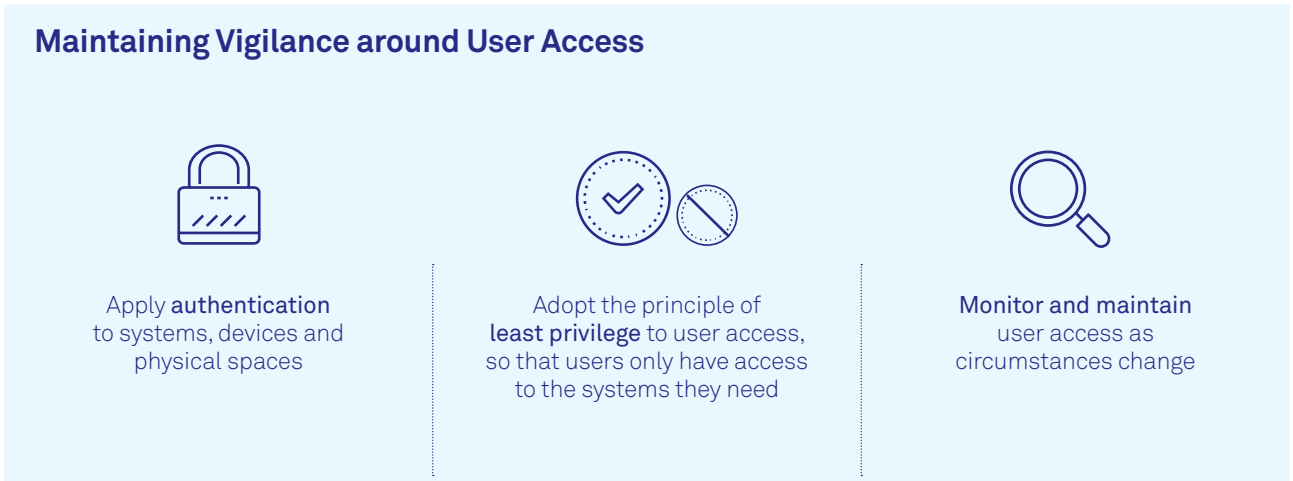
When trained effectively, your workforce can be your most effective defence to a cyber security attack. Build a culture in which the security of patient data and organisational systems, devices and facilities is regarded as everyone's shared responsibility. While transforming organisational culture can be a slow and complex undertaking, there are several steps you can take to kick-start the process. We recommend the following:

- **Start by selling the benefits** of a patient-centred security culture to your staff through an effective communication campaign, focusing on the role they can play to protect themselves and their patients
- **Adjust staff behaviours** by defining and promoting 'good' security behaviours, such as locking your computer before you leave it, and communicating and discouraging 'poor' security behaviours, such as sharing log-in details. Leaders should look to provide actionable feedback, praising staff who demonstrate consistently 'good' behaviours and holding staff accountable when they engage in 'poor' security behaviours
- **Educate staff in cyber security policies and practices** in a way that is engaging and relevant to their roles. For example, some healthcare providers simulate phishing attacks on a regular basis to raise awareness and educate staff on how best to respond. Remember, staff education isn't a one-off event; just as the nature of cyber-attacks changes, so too must the content and approach of cyber security education and training.
- **Consider embedding cyber security responsibilities** into the job descriptions of all employees, to create accountability and drive long-lasting changes in behaviours.

03. Maintain vigilance: manage internal access to systems, devices and physical space with precision

Whether by human error or malicious intent, a security breach cannot occur if a person does not have access to the applicable system, device or space. Prevent future security breaches by practicing vigilance around access to systems, devices and physical space. At the technology level, we recommend that you apply authentication mechanisms to all assets, granting user access in line with the principle of least privilege and carefully monitoring and maintaining user access in line with staff roles. For your people, it will be important to embed vigilance into your organisational culture. In line with a patient-centred culture of security, this should involve encouraging staff to work collectively to prevent unauthorised access to assets, including patient data.

Figure 2: Key components of maintaining vigilance around user access



Not sure where to start?

Our Cyber Security Advisory practice has the skills and experience to help you drive sustainable change in your people layer. We offer services in cyber security strategy and planning, cyber security leadership training, operating model design, culture transformation, change management, communications and training, and user access management design.

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/.

To discuss how we can support your organisation

1800 HEALTH (1800 432 584)

Advisory@health.telstra.com

telstrahealth.com

Health