Health

A Layered Approach to Cyber Security:

Using Technology to Beat Cyber Attackers at their Own Game

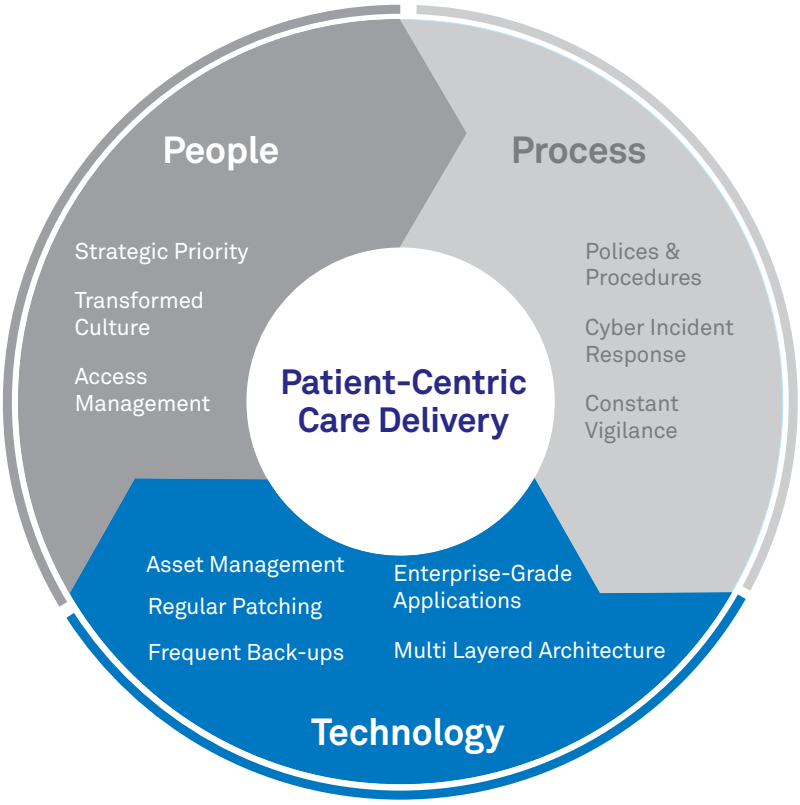
This article is part of a series of articles about Telstra Health's Layered Approach to Cyber Security. You can find out more about our overall approach here, and access practical guidance on the People layer here and the Process layer here.

In the previous articles in this series, we highlighted the rising tide of cyber threats in the healthcare landscape and explained how people and process could be optimised to improve your cybersecurity maturity. In this article, we explore the final piece in the layered approach puzzle, technology, and provide practical guidance on how you can use technology to form a highly effective line of defence against cyber threats.

According to the Australian Cyber Security Centre, Healthcare remains the most targeted industry for cyber attacks in Australia, and the threat is accelerating[1]. As cyber criminals become more sophisticated in their predatory techniques and technologies, so too must healthcare providers in their defences. Technology is a critical component of the layered approach to cyber security and when deployed and managed well, it can be highly effective in preventing, detecting and addressing cyber threats. In Telstra Health's layered approach to cyber security, multiple components, ranging from technology-enabled asset management through to a frequent back-up regime intersect to deliver a robust line of defence.

Figure 1: Exploring the Technology layer in a layered approach to cyber security

Telstra Health's Layered Approach to Cyber Security



To bolster your technology defences, we have compiled a set of practical suggestions for you to consider. Whatever your level of cyber security maturity, we believe that all healthcare organisations stand to benefit from uplifting cyber controls across the technology layer.

01. Know what you need to protect: start with technology-enabled asset management

It's important to understand what your assets are before determining how you will protect them. Start by identifying, cataloguing and prioritising your information assets in a digital system, such as a configuration management data base (CMDB). This will help you understand the scope of the assets requiring cyber protection. Ensure that this information is kept up to date and that it directly informs your cyber security strategy and approach. Remember, as a healthcare organisation, data is one of your most valuable assets and it must be adequately understood for it to be sufficiently protected.

02. Layers within layers: build a robust multi-layered security architecture

There are a wide variety of tools and technologies which can be applied to help secure assets against cyber threats. We suggest applying a suite of tools and approaches which meet the unique security requirements of your organisation. This might include one or more of the following:

- Leveraging **proven prevention technologies**, including firewalls, endpoint protections, and secure email gateways, which seek to stop cyber attackers in their tracks
- Adopting **automated monitoring tooling** to monitor and detect cyber threats as they arise, apply automated controls and escalate to the appropriate people
- Building **redundancy into your architecture** to enable system functions or components to continue to operate when others have been compromised
- Deploy **deception technologies**, or 'honeypots', which are dynamic decoys strategically placed through the technology environment that distract cyber attackers from real assets
- Applying **network segmentation**, which separates assets into sub-networks with different levels of security, limiting an organisation's exposure in a security breach.

Achieving the right balance in tooling and selecting secure and dependable products and vendors is key. If you need assistance in mapping out your target architecture, seek out a trusted advisor to provide you with the right guidance and support.

03. Don't get left behind: keep all technology patched and up to date

With funding constraints and multiple competing priorities, many healthcare organisations adopt the mantra of "if it ain't broke, don't fix it". This is particularly the case for technology, with healthcare organisations often continuing to operate legacy systems which are end of life. Without vendor support and utilising ageing technologies, these systems are inherently vulnerable to cyber attack and can expose your organisation to significant risk. Maintaining an up-to-date and appropriately patched technology architecture is essential to keeping cyber criminals out. In order to do so, it's important for healthcare organisations to view investment in system upgrades as investment in remediating high priority organisational risks.

04. Don't compromise on security: ensure all staff use enterprise-grade applications

With the onset of the COVID-19 pandemic in early 2021, many healthcare organisations found themselves having to pivot quickly, adapting technology, operations and ways of working. Telehealth in particular became a key priority as healthcare organisations navigated the challenges of lock-down and worked to shield their staff from unnecessary exposure to the virus. Many organisations devised workarounds utilising widely available consumer technologies for videoconferencing and document sharing. The challenge with this, however, is that these technologies often do not offer the strength of security controls delivered through enterprise-grade applications, such as encryption and the ability to configure security settings.

Healthcare organisations should look to limit, and ultimately eliminate, the use of consumer applications for work purposes. In order to do so, technology functions must seek to understand the requirements of the organisation's staff and ensure that appropriate enterprise solutions are in place to fulfil them. One way of achieving this is by embedding business relationship management capabilities and responsibilities within technology, so that technology teams actively engage business stakeholders, understand their needs and ensure that the technology architecture is aligned with business requirements. Equally, technology policies provide clarity on the appropriate use of enterprise systems and should be appropriately communicated and enforced. When not told otherwise, staff might not be aware of the security implications of their technology use and may continue to jeopardise patient and organisational data.

05. Back it up: maintain a frequent back-up and testing regime, and effective supplier security risk management

The frequency and effectiveness of your back-up regime is a key determinant in your ability as a healthcare organisation to recover swiftly from a cyber-attack. Maintaining frequent and reliable back-ups of data, including patient and service data, is an essential component of your technology defence system. It is equally important to regularly test your back-up and restoration process to ensure that the process works and can be relied upon in the event of a cyber-attack.

With the proliferation of cloud infrastructure and applications, it has become increasingly important to maintain effective supplier security risk management. This should involve undertaking due diligence when initially engaging a technology supplier, to ensure that they have effective controls in place to mitigate the impact of security incidents and support a smooth recovery, and regularly monitoring and auditing suppliers, to confirm
that they are continuing to apply security controls effectively. Together, a frequent back-up and testing regime, and effective monitoring of technology vendors, helps to mitigate cyber security risk and improve incident recovery.

Not sure where to start?

Our Cyber Security Advisory practice has the technical capability and experience to help you bolster your cyber security technology. We offer services in cyber security strategy, technology analysis, configuration and implementation, and cyber security architecture design and optimisation.

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. Australian Cyber Security Centre, 2020, '2020 Health Sector Snapshot', available 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