Briefing Paper

Patching for IT Professionals

Protecting healthcare information by updating systems and software

A briefing for IT professionals

This document has been prepared for information technology (IT) teams in small to large organisations within the health sector. It provides guidance on maintaining systems and software applications, including actions that can be taken to proactively apply patches to core and interconnected systems, applications, and devices to help protect the information they hold.

This document provides general guidance on updating of systems and software and is not intended to be comprehensive.

Summary

Protecting sensitive healthcare and corporate information is essential in the delivery of healthcare services. One of the most effective ways to reduce the risk of unauthorised information access, is to ensure that all devices, systems, software applications, and digital medical equipment are running supported and up to date version of software.

Applying patches helps address known security vulnerabilities in operating systems and software applications. Automating patching where possible can further reduce an organisation's exposure to these vulnerabilities.

Keeping systems and software up to date reduces the likelihood of cyber incidents that could disrupt access to healthcare records and other critical business systems. This type of incident has the potential to compromise sensitive healthcare information, cause operational disruption, result in financial loss, reputational damage and potentially have a flow on effect to patient care.

Impact

Protecting the wellbeing of healthcare consumers extends beyond their physical care. It also includes safeguarding their privacy and keeping their sensitive personal information secure.

As the use of digital health records, connected systems and internet-enabled medical devices become increasingly central to healthcare delivery, healthcare organisations have an increasing responsibility to protect the information they hold from unauthorised access, disclosure, alteration or loss. Using older versions of systems and software, or failing to apply security patches, can increase the risk of a cyber security incident. Any network connected system could be affected, including desktop and laptop computers; clinical, personnel or financial information systems; databases containing sensitive digital health records and images; mobile devices; and medical equipment.

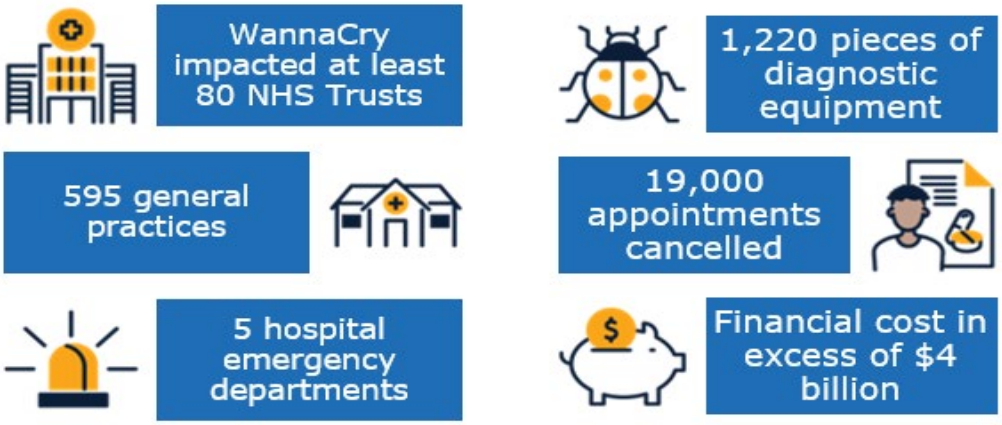
"Healthcare records are a particularly attractive target for cybercriminals, since they hold almost all of the information required for identity theft, social engineering, financial fraud, tax fraud, insurance fraud and medical fraud."

Malicious actors often use known security vulnerabilities to access systems that hold sensitive information. Patching is one of the most effective lines of defence against this type of attack.

When evaluating security patches, a robust risk assessment framework is required to determine the priority for applying specific patches in your IT structure. The case study of a cyber security incident that affected healthcare organisations and hospitals worldwide demonstrates the importance of applying security patches and being aware of the way they can impact other systems.

Protect healthcare information being compromised by a cyber attack

In 2017, the United Kingdom National Health Service (NHS) experienced significant interruption, with WannaCry ransomware attack[1]. The attack targeted computers running the Microsoft Windows operating system and was successful in infecting systems running older versions that were no longer supported. Two months prior, Microsoft had released a patch which addressed the security vulnerability that was exploited in the WannaCry incident.



Healthcare providers are operating in an environment where consumers expect streamlined processes that leverage digital technologies. If healthcare information is breached, the reputation of the organisation can be severely impacted

Approaches to patching systems and software

Data loss is inconvenient - it can disrupt operations, damage trust, and create lasting financial and reputational impacts.

Industry best practice is to apply security patches for critical or extreme risk operating system or application vulnerabilities within two days of release. This is because once a vulnerability becomes publicly known, malicious actors will often attempt to exploit it within the first 48 hours.

You can increase your awareness of potential security threats by subscribing to vendor and Government alerts and prioritising the application of emergency patches for high-risk systems and software.[2]

Cyber incidents such as ransomware make backups even more critical. In the event of an attack, a secure and recent backup can allow systems and data to be restored quickly. Backups are a fundamental part of cyber resilience and business continuity. They ensure that when incidents occur, recovery is possible, and disruption is minimised.

[1] lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf
[2] Strategies to mitigate cyber security incidents | Cyber.gov.au

A successful patch management solution needs to factor in the risks of the change causing an interruption to services. For example, an Australian healthcare organisation experienced issues with users logging onto certain applications to access medical records after applying the security patches to prevent a WannaCry attack.[3] It can be difficult to test legacy systems, in-house applications and some medical devices as they often run on proprietary operating systems and firmware. In some situations, you may not be able to apply a patch immediately. Where this occurs, you should implement other controls to reduce the risk until patching can be completed. These controls may include anti-virus and anti-malware protections, network segmentation, encryption, firewalls and multi-factor authentication.[4]

An incremental roll out of patches to smaller groups of users is advisable to minimise the risk of interrupting services. To assist you in determining the risks associated with the timing of applying a patch you can consult vendor bulletins or use standards such as the Common Vulnerability Scoring System (CVSS).[5] The same process can be applied to temporary workarounds that may be implemented if there are no patches available.

"All NHS organisations infected by WannaCry had unpatched or unsupported Windows operating systems so were susceptible to the ransomware." [4]

When developing a patch management process, you should consider:

- Maintaining an up-to-date inventory of all IT assets, including operating systems, software and version
- Using an asset register or vulnerability management tool to help identify and prioritise patching activities.
- Prioritising patches based on the criticality of the affected system or asset.
- Understanding how systems and devices interact and assessing whether patching could affect functionality or interoperability.
- Establishing regular patching schedules aligned with recognised cyber security guidance and business requirements Patching applications and operating systems | Cyber.gov.au
- Maintaining a test environment so patches can be assessed before they are deployed to production systems.
- Ensuring backup processes are in place and regularly tested so systems can be restored if a patch needs to be rolled back.
- Clearly assigning patching responsibilities to internal IT teams or service providers.

You may also wish to consider an automated patch management solution, which can reduce the time and expense involved in applying patches. This can be included as a requirement when tendering for new IT services or outsourcing support.[6]

A holistic cyber security plan that facilitates collaboration between users, providers, consumers and IT security staff is the key to implementing any cyber security measure.

[3] Services Interrupted As Hospitals Push Fixes For WannaCry Ransomware Exploit
[4] Mitigating cyber security incidents | Cyber.gov.au
[5] What is CVSS - Common Vulnerability Scoring System | SANS Institute
[6] Guidelines for procurement and outsourcing | Cyber.gov.au

Start a conversation about patch management in your organisation

Patch management performs a critical role in reducing the risk of sensitive personal and corporate information being compromised. The need for timely patching of high priority security vulnerabilities has increased, as has the complexity of systems and software that require patching. Consequently, a coordinated effort is required by IT and business teams across healthcare organisations to protect sensitive information.[18]

Business leaders and members of the IT and cyber security team may benefit from discussing the following questions:

- How are we currently registering, assessing and prioritising risks, to support the scheduling of security and non-security patches in our organisation?
- What is the average monthly volume of patch installations and the time and resources required to maintain this level of work?
- Are we considering adding new IT assets to our environment that may require changes to our systems and software patching schedule? What other security measures have been explored to manage these and our existing environment?
- What proportion of patching applications is automated and is there an opportunity to increase automation?
- Is the current structure and resourcing for our IT team sufficient to achieve a patch management schedule that meets our business security risks? Are there other ways we could manage this to better protect our healthcare and corporate information?
- Do we have specialised systems or devices that cannot be patched due to technical limitations? How are we mitigating the risks associated with these instances?

Reviewing your approach to patch management can provide benefits beyond streamlining processes. There may be an opportunity to enhance the capture of data used for reporting. In addition, improving the security of your systems and software through patch management can strengthen the trusted relationships with consumers by demonstrating you are committed to keeping their information secure.

Further information

The Australian Digital Health Agency offers resources to assist healthcare providers to enhance their security practices. Visit the Agency's website for additional guides and information on enhancing the security of your healthcare practice*: www.digitalhealth.gov.au/about-the-agency/ digital-health-cyber-security-centre*

Other organisations you could contact for more information or specific advice include:

Australian Cyber Security Centre	Australian Cyber Security Centre
Office of the Australian Information Commissioner	Office of the Australian Information Commissioner
ScamWatch	ScamWatch