Australian Government
Australian Digital Health Agency

PATCHING:

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 to provide advice about maintaining systems and software applications. The document outlines the actions you can take to proactively apply patches to core and interconnected systems and software applications, to keep the information they hold safe.

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

Summary

Protecting sensitive healthcare and corporate information is essential in the provision of healthcare services. One way to mitigate the risk of information being accessed is to ensure supported versions of systems and software applications are being used on all devices, including digital medical equipment. Applying patches addresses known security vulnerabilities in operating systems and software applications. Automating the process for applying patches can further reduce an organisation's exposure to the risk of a known security vulnerability being exploited.[1]

Keeping systems and software up to date reduces the risk of an incident that could prevent access to healthcare records and other corporate systems. This type of incident has the potential to compromise healthcare information, cause reputational damage, result in financial loss, and have flow on effects to patient care.

Impact

Taking care of the wellbeing of healthcare consumers extends past their physical needs, to protecting their privacy and keeping their sensitive personal information secure. As the use of digital health records and internet-enabled medical devices increases, healthcare organisations have an increasing responsibility to prevent data being compromised.

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."* [2]

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.

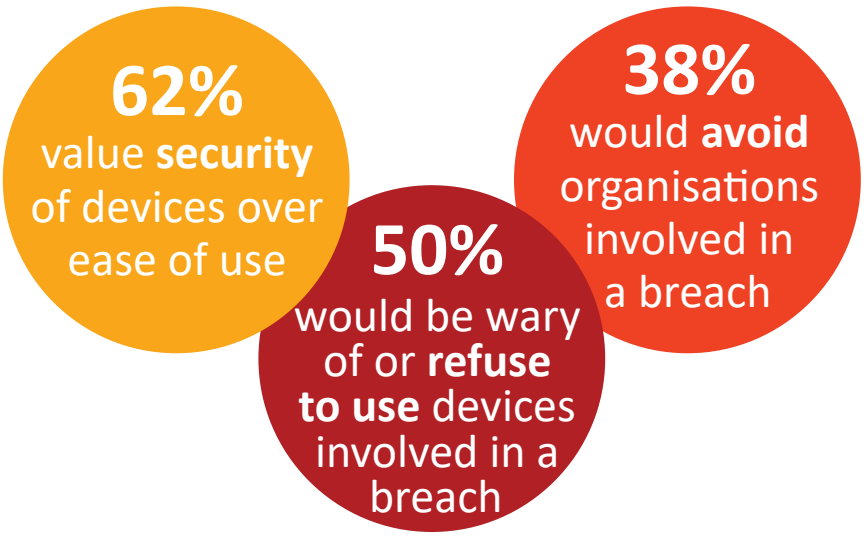
Protect healthcare information being compromised by a cyber attack

On Friday 12 May 2017, over 230,000 computers in 150 countries were impacted by the Wannacry ransomware attack. The United Kingdom National Health Service (NHS) experienced significant interruption, with WannaCry impacting at least 80 NHS Trusts, 595 general practices, five hospital emergency departments and 1,220 pieces of diagnostic equipment. 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. It is estimated that 19,000 appointments were cancelled and the financial cost of the incident was in excess of $4 billion.[3] [4] [5]

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. The impact of a breach associated with medical devices, due to their direct interaction with consumers, can be even greater.[6]

Surveys following the Wannacry incident outlined above, revealed that 38 per cent of consumers would leave or avoid using a health organisation or hospital that had experienced an incident where healthcare information was accessed. If consumers were aware a medical device had been involved with a breach of healthcare information, then 50 per cent would be wary of, or refuse to use the device. Further, 62 per cent of consumers valued the level of security a device could offer, over ease of use.[7]

Changes to consumer confidence after a security incident [7]



Source: Top health industry issues of 2016:
Thriving in the New Health Economy, PwC Health Research Institute

Approaches to patching systems and software

Industry best practice for security patches that address vulnerabilities with extreme risk is to apply patches to operating systems and applications within a two-day timeframe. This is because, once vulnerabilities in an operating system or application are made public, you can expect new malware to be developed by malicious actors within 48 hours.[8] 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.[9]

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.[10] 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.[11] In some cases, given the unique challenges of healthcare organisations, security measures other than patching could be implemented to address the vulnerability. This could involve a combination of anti-virus and anti-malware protection, network segmentation, encryption, firewalls and multi-factor authentication.[12]

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).[8] The same process can be applied to temporary workarounds that may be implemented if there are no patches available.

A Health Informatics Society of Australia survey of healthcare providers found that 40.2% of respondents were implementing high priority security patches within 48 hours.[13] This indicates that while many organisations are finding ways to apply patches without impacting services, there is still work to be done within the health sector, to ensure patches are applied in a timely manner.

Stay ahead of the game - proactive patch management

Taking a proactive approach to applying system and software patches is one of the best preventative measures you can take to keep your healthcare and corporate information secure. The dynamic nature of the IT environment means relying on antivirus and anti-malware alone to defend against current and future threats is not sufficient. Recent events such as the one described in the case study show that patches can limit attacks that exploit known vulnerabilities but need to be applied in context to the organisation's IT environment.

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

The first step is to ensure that you have an up to date listing of your IT assets and level of compliance in running the most current system or software versions.[14] You can then use this asset register to create a database of the patches that are required. The register can also be reviewed to assess the priorities for applying patches, and for determining other security measures for items where patching may impact functionality or where patches are unavailable.

Generally, the minimum schedule for patching is monthly, with patches your organisation defines as high vulnerability security patches, applied within 48 hours of receiving a security

alert. A comprehensive patch management plan factors in time to test lower priority patches in a test environment and establish processes for a remediation if you need to rollback a patch. Ensuring a backup of the data is completed prior to marking any changes to the environment will assist in facilitating a rollback, if required. The structure of the team or service provider that manages IT in your organisation will determine the way you delegate tasks associated with controls for patching systems and software.[15]

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.[16]

"Patching is the most significant characteristic of firms that were not breached in the last two years." [17]

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.

Start a conversation about the opportunities for 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:

1. How are we currently registering, assessing and prioritising risks, to support the scheduling of security and non-security patches in our organisation?
2. What is the average monthly volume of patch installations and the time and resources required to maintain this level of work?
3. 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?
4. What proportion of patch application is automated and is there an opportunity to increase automation?
5. 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 we manage this to better protect our healthcare and corporate information?
6. 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?

There is an opportunity when reviewing your approach to patch management to benefit from more than simply 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:

Table 1. Australian Cyber Security Organisations

Organisation	***Role***
Australian Cyber Security Centre	The Australian Cyber Security Centre (ACSC) provides advice and assistance to help businesses, individuals and governments to protect information from cyber threats, respond to incidents and develop information security strategies.
Stay Smart Online	Stay Smart Online provides simple, easy to understand advice on how to protect yourself online as well as up-to-date information on the latest online threats and how to respond.
Australian Cybercrime Online Reporting Network	The Australian Cybercrime Online Reporting Network (ACORN) provides a national online system for reporting cyber incidents and obtaining advice about cyber security.
Office of the Australian Information Commissioner	The Office of the Australian Information Commissioner (OAIC) provides advice and resources in relation to privacy of health and personal information, including a guide to securing personal information.

References

1 Strategies to Mitigate Cyber Security Incidents - Mitigation Details. Available from: https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents-mitigation-details

2 Protecting Data in the Healthcare Industry. An Osterman Research White Paper Published July 2017. Available from: https://www.ostermanresearch.com/home/white-papers/

3 Lessons learned review of the WannaCry Ransomware Cyber Attack. Available from: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

4 Investigation: WannaCry cyber attack and the NHS. Available from: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

5 WannaCry: Lessons Learned 1 Year Later. Available from: https://www.symantec.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later

6 2017 Mid-year Horizon Report – The state of cyber security in healthcare. Available from: https://www.fortifiedhealthsecurity.com/wp-content/uploads/2017/07/Fortified-Health-Mid-Year-Horizon-Report.pdf

7 PwC Top healthcare issues of 2016: Thriving in the new health economy. Available from: https://www.pwchk.com/en/people-and-organisation/hc-top-issues-dec2015.pdf

8 Assessing Security Vulnerabilities and Applying Patches. Available from: https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches

9 Stay Smart Online Alert Service: Available from: https://www.staysmartonline.gov.au/alert-service

10 Services Interrupted as Hospitals Push Fixes for WannaCry Ransomware Exploit. Available from: www.forbes.com/sites/leemathews/2017/05/25/services-interrupted-as-hospitals-push-fixes-for-wannacry-ransomware-exploit

11 Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives. Available from: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-networked-medical-device.pdf

12 Tips for Risk Assessment in Healthcare IT Security. Available from: https://electronichealthreporter.com/tips-for-risk-assessment-in-healthcare-it-security/

13 Health Informatics Society of Australia (HISA) Cyber Security Community of Practice Survey Report 2017. Available from: https://www.hisa.org.au/blog/hisas-cybersecurity-community-of-practice-survey-report

14 10 keys to successful patch management. Available from: https://www.techrepublic.com/blog/10-things/10-keys-to-successful-patch-management/

15 Australian Government Information Security Manual. Available from: https://www.cyber.gov.au/ism

16 Introduction to automated enterprise patch management software. Available from: https://searchsecurity.techtarget.com/feature/Introduction-to-automated-patch-management-products-in-the-enterprise

17 Ponemon Institute: Patch work demands attention. Available from: https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ar-ponemon-financial-report.pdf

18 Combating Patch Fatigue. Available from: https://www.tripwire.com/misc/combating-patch-fatigue-register

Publication date: March 2019 - second edition.

Contact for enquiries

Telephone: 1300 901 001 or **email:** help@digitalhealth.gov.au

Acknowledgements

Council of Australian Governments
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Australian Government

Australian Digital Health Agency

digitalhealth.gov.au