



**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 and communication technology (ICT) teams in small to large organisations within the health sector to provide advice about maintaining system 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 the latest versions of systems and software applications are being used on all devices, including digital medical equipment. Applying patches fixes known security vulnerabilities in operating systems and software applications.<sup>[1]</sup> Automating the process for applying updates can further reduce an organisation's exposure to the risk of a known security vulnerability being exploited.<sup>[2]</sup>

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 and result in financial loss.

## **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; or mobile and medical devices.

*“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<sup>[3]</sup>.”*

Malicious actors often use known security vulnerabilities to access systems that hold sensitive information. In 2016, 96% of attacks used known vulnerabilities to exploit networks and compromise data. Patching is one of the most effective lines of defence against these types of attacks.<sup>[4]</sup>

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

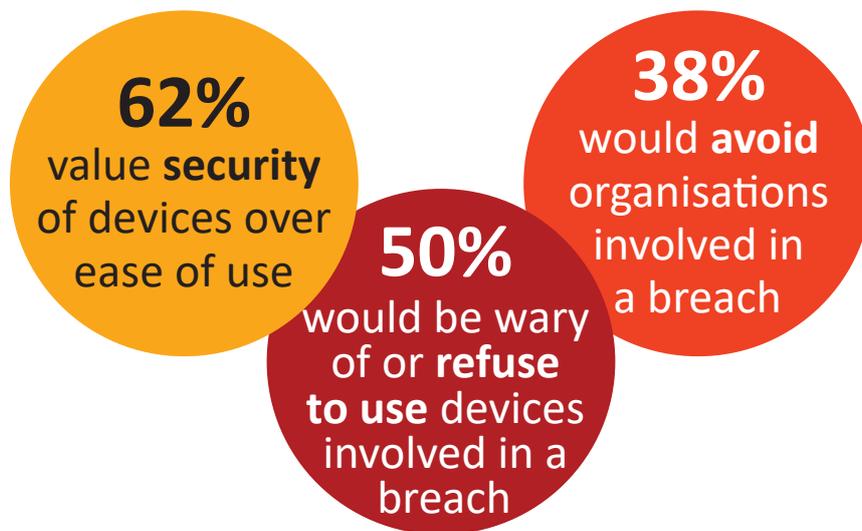
### **Protect your organisation's healthcare information being compromised by a cyber attack**

On Friday 12 May 2017, over 230,000 computers in 150 countries were impacted by the Wannacry ransomware attack. It also impacted over 70,000 devices connected to operating systems including mobile devices and medical equipment. At least 81 healthcare organisations, 595 general practices, five hospital emergency departments and 1,220 medical devices used by the National Health Service in the United Kingdom.<sup>[5]</sup> 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 that 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.<sup>[6]</sup>

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.<sup>[7]</sup>

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.<sup>[8]</sup>

### Changes to consumer confidence after a security incident



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 serious vulnerabilities is to apply patches to operating systems and applications, within a two-day timeframe.<sup>[9]</sup> Once vulnerabilities in an operating system or application are made public, you can expect malware to be developed within 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.<sup>[10]</sup>

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.<sup>[11]</sup> 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.<sup>[12]</sup> 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.<sup>[13]</sup>

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).<sup>[14]</sup> The same process can be applied to temporary workarounds that may be implemented if there are no patches available.

## Stay ahead of the game - proactive patch management tips

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 ICT environment means relying on antivirus and anti-malware alone to defend against current and future threats is not sufficient.<sup>[15]</sup> 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 ICT environment.

The first step is to ensure that you have an up to date listing of your ICT assets and level of compliance in running the most current system or software versions.<sup>[16]</sup> You can then use this asset register to create a database of the patches that are required.<sup>[17]</sup> The register is also reviewed to assess the priorities for applying patches and determining other security measures for items where patching may impact functionality or be 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 making any changes to the environment will assist in facilitating a rollback, if required. The structure of the team or service provider that manages ICT in your organisation will determine the way you delegate tasks associated with controls for patching systems and software.<sup>[18]</sup>

*“All NHS organisations infected by WannaCry had unpatched or unsupported Windows operating systems so were susceptible to the ransomware.”<sup>[19]</sup>*

An automated patch management solution can reduce the time and expense involved in applying patches. This can be included as a requirement when tendering for new ICT services or outsourcing support. It's mutually beneficial to work in partnership with your vendors and providers, as the loss of intellectual property suffered as a result of a cyber security attack can also have long term financial impacts on the ICT provider.<sup>[20]</sup> The evaluation of solutions starts with understanding organisational and individual requirements, budget and implementation timeframes. Future requirements such as introducing the use of wearable devices for home monitoring of consumers, needs to be factored into the selection of a patching solution.<sup>[21]</sup>

You may consider taking your plan a step further and sourcing an endpoint protection tool. This can help mitigate unpatched vulnerabilities that may expose an end user when opening phishing emails, clicking links or downloading unverified software.<sup>[22]</sup> A holistic cyber security plan that facilitates collaboration between users, providers, consumers and the cybersecurity team 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.<sup>[23]</sup> The complexity of systems and software that require patching can create an increasing volume of work for ICT teams in healthcare organisations.<sup>[24]</sup>

Business leaders and members of the ICT 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 ICT 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 ICT 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 automating application processes.<sup>[25]</sup> There may be an opportunity to enhance the capture of data used for reporting associated with regulatory compliance and privacy obligations. 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.<sup>[26]</sup>

*“Applying patches to operating systems, applications and devices is critical to ensuring the security of systems.”<sup>[27]</sup>*

## Additional information

The Australian Digital Health Agency (the 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.

In addition, the table below outlines other organisations you could contact for more information or specific advice.

Organisation	Role
Australian Cyber Security Centre	The Australian Cyber Security Centre (ACSC) brings cyber security capabilities from across the Australian Government together into a single location. The ACSC website provides advice to individuals, businesses and government on cyber security and has an online cyber incident reporting facility.
Australian Signals Directorate	The Australian Signals Directorate (ASD) provides public sector organisations with advice and assistance relating to information security. ASD undertakes operational responses to cyber incidents of national importance. It also publishes the Information Security Manual (ISM) and strategies to mitigate cyber security incidents.
Computer Emergency Response Team (CERT) Australia	Provides the private sector with information and assistance to help them protect their Information and Communications Technology (ICT) infrastructure from cyber threats and vulnerabilities. CERT Australia also provides a coordination role during a serious cyber incident. Stay Smart Online is a CERT Australia initiative to provide advice and tools to protect individuals and businesses from cyber incidents.

## References

1. Strategies to mitigate cyber security incidents – Top 4 mitigation strategies to protect you ICT system. Available from: [https://www.asd.gov.au/publications/protect/top\\_4\\_mitigations.htm](https://www.asd.gov.au/publications/protect/top_4_mitigations.htm)
2. Stay Smart Online Small Business Guide - Protect your business in 5 minutes. Available from: <https://www.staysmartonline.gov.au/get-involved/guides/smallbusinessguide>
3. Protecting Data in the Healthcare Industry. An Osterman Research White Paper Published July 2017. Available from: [http://www.bitpipe.com/data/document.do?asrc=SS\\_OCTT\\_450417492-shealthit&res\\_id=1502995795\\_829](http://www.bitpipe.com/data/document.do?asrc=SS_OCTT_450417492-shealthit&res_id=1502995795_829)
4. *Exploits: How great is the threat?* Available from: <https://securelist.com/exploits-how-great-is-the-threat/78125>
5. 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>
6. Patch Management Remains A Struggle For Healthcare Industry. Available from: <https://one.comodo.com/blog/patch-management/patch-management-remains-a-struggle-for-healthcare.php>
7. 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>
8. 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>
9. General advice for mitigating cyber incidents. Available from: <https://www.cert.gov.au/advice>
10. Stay Smart Online alert service. Available from: <https://www.staysmartonline.gov.au/alert-service>
11. Services Interrupted As Hospitals Push Fixes For WannaCry Ransomware Exploit. Available from: <https://www.forbes.com/sites/leemathews/2017/05/25/services-interrupted-as-hospitals-push-fixes-for-wannacry-ransomware-exploit/>
12. 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>
13. Tips for Risk Assessment in Healthcare IT Security. Available from: <http://electronichealthreporter.com/tips-for-risk-assessment-in-healthcare-it-security/>
14. Assessing Security Vulnerabilities and Applying Patches, April 2016. Available from: [https://www.asd.gov.au/publications/protect/assessing\\_security\\_vulnerabilities\\_and\\_patches.htm](https://www.asd.gov.au/publications/protect/assessing_security_vulnerabilities_and_patches.htm)
15. Update management process, Microsoft library. Available from: <https://technet.microsoft.com/library/cc700845.aspx>
16. 10 keys to successful patch management. Available from: <http://www.techrepublic.com/blog/10-things/10-keys-to-successful-patch-management/>
17. Eight Steps to Better Security with Patch Management Automation. Available from: <http://blog.kaseya.com/blog/2015/12/08/eight-steps-to-better-security-with-patch-management-automation/>
18. Controls 2016 Information Security Manual. Available from: [https://www.asd.gov.au/publications/Information\\_Security\\_Manual\\_2016\\_Controls.pdf](https://www.asd.gov.au/publications/Information_Security_Manual_2016_Controls.pdf)
19. Investigation: WannaCry cyber attack and the NHS. [Internet]. Available from: <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>

20. Select the best patch management software for your company. Available from: <http://searchsecurity.techtarget.com/buyersguide/Select-the-best-patch-management-software-for-your-company>
21. 2016 Cyber Security Survey. Available from: <https://www.bdo.com.au/en-au/2016-cybersecurity-survey-results>
22. Patch Management Software Buyer's Guide. Available from: <http://www.esecurityplanet.com/network-security/patch-management-software-buyers-guide.html>
23. Accenture Technology Vision 2017 Survey, Technology for the People: The Era of the Intelligent Enterprise. Available from: [www.accenture.com/technologyvision](http://www.accenture.com/technologyvision)
24. Combating Patch Fatigue. Available from: <https://www.tripwire.com/misc/combating-patch-fatigue-register/>
25. The Realities of Patch Management Best Practices. Available from: <https://cipher.com/blog/2017/07/18/the-realities-of-patch-management-best-practices/>
26. Deloitte 2016 Global health care outlook - Battling costs while improving care. Available from: <https://www2.deloitte.com/au/en/pages/life-sciences-and-healthcare/articles/global-health-care-sector-outlook.html>
27. Australian Cyber Security Centre Threat Report 2017. Available from: [https://www.acsc.gov.au/publications/ACSC\\_Threat\\_Report\\_2017.pdf](https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf)

**Publication date:** December 2017

### **Contact for enquiries**

**Telephone:** 1300 901 001 or **email:** [help@digitalhealth.gov.au](mailto:help@digitalhealth.gov.au)

### **Disclaimer**

The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

### **Document control**

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

### **Copyright © 2017 Australian Digital Health Agency**

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the permission of the Australian Digital Health Agency. All copies of this document must include the copyright and other information contained on this page.

### **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**

[www.digitalhealth.gov.au](http://www.digitalhealth.gov.au)