



Australian Government
Australian Digital Health Agency

PATCHING:

*Protecting healthcare information
by updating systems
and software*



*A briefing for
senior managers*



This guide has been prepared for senior managers in the healthcare sector who are responsible for managing the risk of systems or software being inaccessible or compromised due to exploitation of a known security vulnerability. A companion document has been prepared for information technology (IT) teams to provide further information on the approach to applying patches that fix known security vulnerabilities.

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 use the supported versions of systems and software applications on all devices, including digital medical equipment.

Using unsupported versions of systems and software or failing to apply security patches, can increase the risk of a cyber security incident. A sensible risk assessment approach is required to determine the best approach and timing for the installation of specific patches in your IT structure.

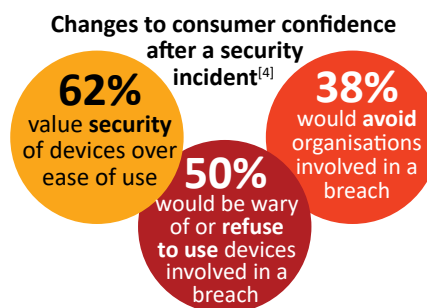
Malicious actors often use known security vulnerabilities to access systems that hold sensitive information. In 2016, 96% of attacks used known vulnerabilities to exploit networks and compromise data. Patching is one of the most effective lines of defence against these types of attacks.^[1]

Cyber security incidents may disrupt service delivery to consumers and could lead to clinical and administrative errors due to lack of access to vital records. An incident can result in compromised consumer privacy, and reputational, financial and individual loss as outlined in the case study below.

Protect your organisation's healthcare information from 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.^[2] 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.^[3]

Surveys following the Wannacry incident revealed that 38 per cent of consumers would leave or avoid using a health organisation that had experienced a security incident where healthcare information was accessed. If consumers were aware a medical device had been involved with a breach of healthcare information, 50 per cent would be wary of or refuse to use the device; and 62 per cent of consumers value the level of security a device offers, over ease of use.^[4]



Key Points

- 1 Given the financial and non-financial impacts associated with the risk of using unsupported versions of systems or software applications, it is important that senior managers understand their organisation's risk exposure and appropriate mitigations. Suggested questions to ask your IT team include:
 - Are all our operating systems the most current versions available? If not, do we have a plan in place to update them?
 - Are the software applications running on physical and virtual machines, mobile devices and other digital equipment the most current versions available? If not when are we planning to update them?
 - How do we receive, evaluate and action bulletins about security and non-security patches for our systems and software? How do we assess patches in the context of our network structure? What is the time frame we take to apply a security patch that has been evaluated as a high priority for our ICT environment? (Industry best practice is to apply high priority security patches within 48 hours).
 - Are our patch management processes automated? Does the IT team need additional support or resources to better manage this process and mitigate security risks? Are there additional mitigation strategies or solutions, such as those outlined in the companion document, Patching for IT Professionals, which could be implemented?

- 2** There are a number of information security frameworks and standards that organisations in the health sector can use to improve the security and resilience of their digital health systems and help meet their professional and legal obligations to protect health information.
- 3** If your organisation doesn't have the resources or expertise to assess its risks or to implement adequate security measures, it is recommended that you seek professional advice from a reputable IT service provider or information security consultant.

If your systems or software are compromised, please note the following:

- Under the *Privacy Act 1988* (Cth), healthcare organisations must report data breaches under the Notifiable Data Breaches scheme. Refer to advice from the Office of the Australian Information Commissioner (OAIC) for details of these requirements: www.oaic.gov.au.^[5]
- For any event or situation where there is a suspected or actual breach of the My Health Record system, organisations are required to notify the Australian Digital Health Agency (the System Operator).^[6] In addition, organisations in the private sector are required to notify the OAIC.
- In the event of a cyber security incident, or to seek more information or specific advice, you can contact the Australian Cyber Security Centre: www.acsc.gov.au
- Additional information about how to protect your systems and software is available on the Stay Smart Online website: www.staysmartonline.gov.au

References

- 1 *Exploits: How great is the threat?* Available from: <https://securelist.com/exploits-how-great-is-the-threat/78125>
- 2 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>
- 3 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>
- 4 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>
- 5 Notifiable Data Breaches scheme. Available from: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>
- 6 My Health Record data breaches. Available from: <https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/manage-data-breach>

Publication date: March 2019 - second edition.

Contact for enquiries

Telephone: 1300 901 001 or **email:** 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 © 2019 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

digitalhealth.gov.au