Fact sheet

Patching: For senior managers

Protecting health information by updating systems and software

Summary

Protecting sensitive health and corporate information is essential in the provision of healthcare services. One way to reduce the risk of unauthorised information access, 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 infrastructure.

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 these types of attacks.[1]

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

Case study

On 12 May 2017 over 230,000 computers in 150 countries were being impacted by the WannaCry ransomware attack. It also impacted over 700,000 devices connected to operating systems including mobile devices and medical equipment. At least 81 healthcare organisations, 595 general practices, 5 hospital emergency departments and 1,220 medical devices used by the National Health Service (NHS) 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]

Fact sheet

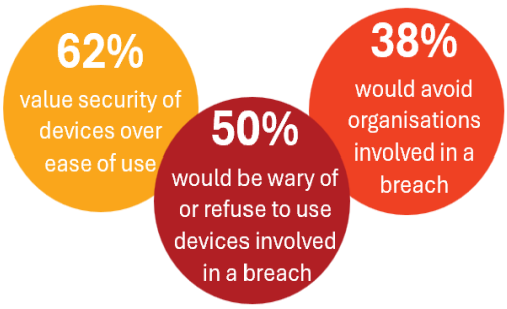
Patching: For senior managers

Protecting health information by updating systems and software

Surveys following the WannaCry incident revealed that 38 per cent of patients would leave or avoid using a healthcare organisation that had experienced a security incident where health information was accessed.

If a medical device had been involved with a breach of health information, 50 per cent of patients would be wa of or refuse to use the device; and 62 per cent would value the level of security a device offers, over ease of use.[4]

Changes to confidence after a security incident.



Key points

1. Given the financial, operational and reputational impacts associated with unsupported systems and software, it is important that senior managers understand their organisation's risk exposure and the measures in place to manage those risks.

   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 with 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 infrastructure? How quickly do we apply high-priority security patches once they have been assessed? (Industry best practice is to apply critical 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 does not have the resources or expertise to assess risks or implement appropriate security measures, consider seeking advice from a reputable IT service provider or cyber security specialist.

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

   - Under the *Privacy Act 1988,* 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.cyber.gov.au
   - Additional information about how to protect your systems and software is available on the Australian Cyber Security Centre website: www.cyber.gov.au

References

1 Essential Eight Explained: Essential Eight explained | Cyber.gov.au

2 15 of biggest ransomware attacks in history: 15 of the Biggest Ransomware Attacks in History

3 Investigation: WannaCry cyber attack and the NHS. Available from: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/

4 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

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