Australian Government
Australian Digital Health Agency

Risk Mitigation Advice

Ransomware – a briefing for senior managers

2 May 2017 v1.0
Approved for external information

This document has been prepared for senior managers in the health sector to help increase understanding and facilitate better management of the risks posed by ransomware. A companion document, Preventing and recovering from ransomware*, has been prepared for information, communication and technology (ICT) teams which provides further information and outlines security measures and practices that will help healthcare organisations prevent and recover from a ransomware attack.*

Summary

Ransomware is a type of malicious software that denies access to computers and files and demands that affected organisations make a payment to regain access to their information. CryptoLocker is a particularly virulent and widely known form of ransomware that encrypts all files located within the infected computer, its shared network drives, and any attached storage.

A ransomware attack on a healthcare organisation can potentially cause significant financial, reputational, health and safety harm. Any network connected system could be affected, such as: desktop computers; clinical, personnel or financial information systems; databases containing digital health records; or medical devices.

Ransomware, which has become increasingly common within the health sector,[1] may pose a significant risk to the security and privacy of individual health information and impede organisations' ability to deliver healthcare services.[2] Depending on the access obtained, an attacker could also read, modify, export or publicly release digital health records.[3]

It is vital that organisations in the health sector understand their risks and ensure they are prepared to prevent and respond to ransomware attacks.

Key points

1 Given that organisations in the health sector have professional and legal obligations to protect individual health information,[4] it is important that accountable senior managers understand how the risk posed by ransomware is being managed within their organisation

[1] *Healthcare held to ransom.* [Internet]. Available from: http://www.cso.com.au/article/597125/healthcare-held-ransom-how-protect-australian-healthcare-systems-patients-from-cybercrime/.
[2] *Ransomware and recent variants.* [Internet]. Available from: https://www.us-cert.gov/ncas/alerts/TA16-091A.
[3] *Webcast: Prepare and respond to healthcare ransomware.* [Internet]. Available from: http://healthitsecurity.com/resources/webcasts/prepare-and-respond-to-healthcare-ransomware-attacks.
[4] *Privacy and security of digital health.* [Internet]. Available from: http://www.digitalhealth.gov.au/using-the-my-health-record-system/maintaining-digital-health-in-your-practice/privacy-and-security.

and determine if the risk mitigation is acceptable. Suggested questions to ask your ICT team include:

- Have existing security controls within the organisation been reviewed in light of the risk posed by ransomware? If so, what was the outcome? What is the level of risk and is it acceptable?
- How are backups of critical systems managed and secured? Will this approach prevent backups being compromised by ransomware?
- When was the backup process last tested and what was the outcome?
- Does the ICT team need additional support or resources to better manage and mitigate the organisation's risks? Are there additional mitigation strategies, such as those listed in the *Preventing and recovering from ransomware* document, that should be implemented?

2 Ideally, the risks posed by ransomware and other malware should be managed as part of a comprehensive information security framework or in accordance with an appropriate information security standard. There are a range of information security frameworks and standards, including those applicable to state jurisdictions, which 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 individual 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.

4 If ransomware does compromise your organisational systems, please note the following.

- Paying attackers is not recommended as this will encourage further attacks and does not guarantee that organisations will be able to recover affected files or avoid a data breach. It is suggested that you seek legal advice if paying the ransom is considered necessary.
- Government agencies and businesses covered by the *Privacy Act 1988* (Cth) will need to report individual health information breaches under recently introduced amendments to the Privacy Act. Refer to advice from the Office of the Australian Information Commissioner (OAIC) for details.[5]
- If systems used to access or update the My Health Record system are compromised, it is possible that the security or integrity of the My Health Record system has also been compromised. For any event or situation where there is a suspected or actual data breach of the My Health Record system, organisations are required to notify us, the Australian Digital Health Agency, (the System Operator).[6] In addition, organisations in the private sector are required to notify the OAIC.[7]

[5] *Mandatory data breach notification.* [Internet]. Available from: https://www.oaic.gov.au/media-and-speeches/statements/mandatory-data-breach-notification.
[6] *Notifications of data breaches.* [Internet]. Available from: https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/notifications-of-data-breaches.
[7] *Guide to mandatory data breach notification in the PCEHR system.* [Internet]. Available from: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-mandatory-dbn-in-pcehr-system.

Publication date: 2 May 2017

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.

Acknowledgements

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