



Australian Government
Australian Digital Health Agency

Preventing and recovering from
RANSOMWARE



A briefing for
IT professionals



This document has been prepared for information technology (IT) teams in medium to large organisations within the health sector to help increase understanding and facilitate better management of the risks posed by ransomware. The document outlines security measures and practices to help prevent and recover from a ransomware attack.

This document provides general guidance in relation to the risks posed by ransomware and is not intended to be comprehensive.

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. Ransomware has become increasingly common within the health sector ^[1] and may pose a significant risk to the security and privacy of health information and impede organisations' ability to deliver healthcare services.^[2]

The WannaCry ransomware attack in May 2017, demonstrates the impact this type of incident can have on the delivery of healthcare. Computers and devices were affected in 81 healthcare organisations, 595 General Practices and five hospital emergency departments across the National Health Service (NHS) in the United Kingdom.^[3] This ransomware leveraged a known security vulnerability, which shows the importance of applying patches to reduce the likelihood of ransomware attacks which exploit known security vulnerabilities.

Given that healthcare providers have professional and legal obligations to protect health information ^[4], it is recommended that ICT teams review and assess the adequacy of security measures in place to mitigate the risks posed by ransomware.

Impact

A ransomware attack on a healthcare provider can potentially cause significant reputational damage, clinical safety risks, financial harm, and may impact continuity of business operations. The level of harm depends on the effectiveness of existing security measures and the number and criticality of affected systems. Any network connected system could be affected, such as: desktop computers; clinical, personnel or financial information systems; databases containing sensitive digital health records; or medical devices. Depending on the nature of the attack, the impact could range from minor to severe, with the potential to disrupt a healthcare facility's ability to deliver effective healthcare services.



While ransomware attacks generally seek to deny access to an organisation's files and systems, depending on the access obtained, an attacker could also read, modify, export or publicly release digital health records. In the USA, health records have a high value on the black market and provide attackers an additional revenue stream to supplement ransom payments.^[5] Some attackers may threaten to publicly release sensitive data if a ransom is not paid.^[6]

Attack vectors and vulnerabilities

Generally, attackers initiate ransomware attacks by exploiting vulnerabilities in browsers or other applications such as email clients and PDF readers. Others use techniques to convince users to open an email with an infected attachment, or follow a link to a site that deploys the malicious software.

Keeping software and systems updated and patched will reduce the potential that known security vulnerabilities are exploited to gain unauthorised access to health, personal and other sensitive information. For example, organisations with up-to-date software were likely to avoid being affected by the WannaCry ransomware attack, as Microsoft had released a patch prior to the attack, to address the vulnerability that was exploited by the WannaCry incident ^[3]. It is also important to use versions of software that are supported by the software provider, as security patches are generally not available for unsupported software.

“Ransomware has become mainstream and will play a prominent role in future attacks.”⁷

The importance of taking steps to prevent and recover from ransomware attacks is highlighted by research that shows the healthcare sector is one of the most targeted industries.^[7]

The comparative prevalence of ransomware in the health sector was highlighted in the Office of the Australian Information Commissioner's Notifiable Data Breaches Quarterly Statistics Report for the period October to December 2018. This report shows that the percentage of ransomware-related data breaches reported for the health sector was twice that of other organisation types. It is vital that organisations in the health sector understand their risks and ensure they are prepared to prevent and respond to ransomware attacks.^[8]

Depending on the variant, ransomware may install itself on a single computer, or propagate and compromise many computers.^[9] Once it has installed itself, most variants will encrypt files on the infected computer and files that are connected to, or accessible by, the compromised computer, such as network shares, external hard drives, synchronised cloud storage, and potentially some cloud applications.^[10]

Ransomware variants differ in how they encrypt files. Some variants, such as CryptoLocker, use public key encryption and delete Shadow Volume Copy in Windows, which means the only way to recover encrypted files is by restoring them from backups. Some variants target web application servers and encrypt data as it is written to the database and decrypt it when the data is read through the web application. Later, when the attacker removes the decryption key, any content that was previously encrypted becomes unreadable. The longer an attacker is able to delay detection, the more difficult it is to recover data following the initial compromise due to the contamination of backups.^[11]

Typically, attackers tweak and test their ransomware to ensure the variant has a low rate of detection by anti-virus software when first distributed. Hence there is a lag between the release of a new ransomware variant and the ability for anti-virus signatures to detect and prevent the ransomware executing. A new form of all-in-one malware combines ransomware, cryptocurrency mining and self-propagating capabilities similar to WannaCry.^[12] It is possible to protect users by implementing preventative measures to minimise ransomware attacks.

Preventing and recovering from an attack

Preventative measures

Controls to help prevent ransomware attacks include:

- 1** Segment and segregate the network to ensure that valuable data, systems and storage are only readable and writable by authorised, authenticated users.^[13] Deploy network level authentication via 802.1x or network access control, or both, to ensure only authorised devices connect to your network.
- 2** Once you control the devices on your network, it is easier to manage the security of software on your network. Ensure that only fully supported and up-to-date operating systems and applications (including web browsers and email clients) are allowed to operate within your network.^[14]
- 3** Implement an application whitelisting solution for servers and desktops.^[15] For example, AppLocker is built into Microsoft Windows (version 7 onward) and Windows Server (2008 R2 and later versions). Software Restriction Policies are available for earlier versions of Windows.^[16]
- 4** Configure hardware and software to be secure,^[17] including mobile devices.^[18] Disable pop-ups and plugins in browsers and disable or control the use of macros in Microsoft Office and Windows and workstations.^[19] Configure desktops and servers so they do not auto-run content from removable media such as USBs, DVDs and mounted network shares.
- 5** Reduce the use of administrative privileges.^[20] Ensure all users operate from a limited user account when accessing email and the web and that privileged accounts (administrator or root) are restricted to staff who need them and only use them when required.
- 6** Deploy up-to-date anti-virus and spam filter protection on mail gateways, desktops and servers. Configure anti-virus protection to automatically conduct a malware scan of removable media when inserted.
- 7** Implement an authenticated web proxy server for outbound connections to the internet and to block access to known malicious URLs, domains or IP addresses.
- 8** Educate users about the security risks associated with social media ^[21] and socially engineered messages that direct users to click on links or open attachments from unknown sources to reveal account credentials and other sensitive information.^[22] The Australian Government's Stay Smart Online and ScamWatch sites provide useful resources to help raise user awareness of online threats.

Prepare to recover

If prevention fails, having backups that are not contaminated by the ransomware will significantly mitigate the impact of a ransomware attack.

- 1** Develop an Incident Response Plan that outlines the procedure for reporting and handling incidents.^[23] The plan should detail who is responsible for coordinating the response to the incident, and the internal and external contacts, including cloud application vendors (if applicable). Once developed, all staff should be made aware of the content of the plan so that they understand their responsibility to report incidents in a timely manner, and know how to do so.
- 2** Develop and implement a backup plan that identifies critical data sources and backup processes. Ensure that at least one backup destination is not continuously connected and is separate from its source systems. This is important as backup files stored on a continuously

connected USB external drive, accessible from a connected network drive, or copied and synchronised to a cloud destination, for example, are at risk of being contaminated by ransomware. The plan should include verification that scheduled backups complete successfully.

- 3** Maintain pre-prepared, up-to-date, securely configured images (operating system and applications) to re-image affected desktops and servers if required.
- 4** For critical cloud hosted applications, such as clinical information systems, contact the vendor to determine what protection they provide to prevent a malware infection, and what recovery assistance they will provide if ransomware either infects the cloud application or encrypts cloud data.
- 5** Document the system recovery process (system and data) and practise restoring backup data at least quarterly. This will help identify and address any problems with the backup and recovery process.

Corrective actions after an attack

- 1** Disconnect affected systems from the network as quickly as possible to prevent the ransomware encrypting connected file shares or propagating further.
- 2** Identify systems compromised, including accessible data sources.
- 3** Attempt to identify the ransomware variant as this may inform your mitigation and recovery options and help assess the impact of the attack.^[24]
- 4** Follow your procedures to re-image the infected systems and restore data from backups.
- 5** Review the adequacy of existing security measures to help prevent further attacks.

Additional advice

- 1** Paying attackers is not recommended as this will encourage further attacks and does not guarantee you will be able to recover affected files or avoid a data breach.^[25] It is suggested that you seek legal advice if paying the ransom is considered necessary.
- 2** 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 relating to the My Health Record system, organisations are required to notify the Australian Digital Health Agency (the System Operator) and the Office of the Australian Information Commissioner (OAIC).^[26]
- 3** Government agencies and businesses covered by the *Privacy Act 1988* (Cth) will also need to report health information breaches under the Notifiable Data Breaches Scheme. Refer to advice from the Office of the Australian Information Commissioner (OAIC) for details.^[27]
- 4** If your organisation doesn't have the resources or expertise to implement effective mitigation strategies, it is recommended that you seek professional advice from a reputable IT service provider or consultant.

There are a number of information security standards and frameworks which healthcare providers 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.

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.

References

- 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/>
- Ransomware and recent variants. [Internet]. Available from: <https://www.us-cert.gov/ncas/alerts/TA16-091A>.
- 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>
- Recognise your privacy and security obligations. Available from: <https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/recognise-your-privacy-and-security-obligations>
- 2018 Trustwave Global Security Report. Available from: <https://www2.trustwave.com/GlobalSecurityReport.html>
- Webcast: Prepare and respond to healthcare ransomware. [Internet]. Available from: <http://healthitsecurity.com/resources/webcasts/prepare-and-respond-to-healthcare-ransomware-attacks>
- Cylance 2017 Threat Report. Available from: <https://www.cylance.com/content/dam/cylance/pdfs/reports/CylanceThreatReport2017.pdf>
- Office of the Australian Information Commissioner, Notifiable Data Breaches Quarterly Statistics Report 1 October - 31 December 2018. Available from: <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-quarterly-statistics-report-1-october-31-december-2018>
- Microsoft warns of a new self-propagating malware. Available from: <https://www.scmagazine.com/new-ransomware-has-worm-like-ability/article/528210/>
- Ransomware a threat to cloud services too. Available from: <https://krebsonsecurity.com/2016/01/ransomware-a-threat-to-cloud-services-too/>
- Ransomware: Current Trends, Challenges, and Research Directions. Available from: https://www.researchgate.net/publication/320346114_Ransomware_Current_Trend_Challenges_and_Research_Directions
- New Malware Combines Ransomware, Coin Mining and Botnet Features in One. Available from: <https://thehackernews.com/2018/09/ransomware-coinmining-botnet.html>
- Network segmentation and segregation. Available from: <https://www.cyber.gov.au/publications/network-segmentation-and-segregation>
- Assessing security vulnerabilities and applying patches. Available from: <https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches>

- 15 Implementing application whitelisting. Available from:
<https://www.cyber.gov.au/publications/implementing-application-whitelisting>
- 16 Applocker. Available from: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview>
- 17 Essential Eight Explained. Available from: <https://www.cyber.gov.au/publications/essential-eight-explained>
- 18 iOS Hardening Configuration Guide. Available from:
<https://www.cyber.gov.au/publications/os-hardening-configuration-guide>
- 19 Microsoft Office Macro Security. Available from:
<https://www.cyber.gov.au/publications/microsoft-office-macro-security>
- 20 Restricting Administrative Privileges. Available from:
<https://www.cyber.gov.au/publications/restricting-administrative-privileges>
- 21 Security Tips for Social Media. Available from:
<https://www.cyber.gov.au/publications/security-tips-for-social-media>
- 22 Detecting Socially Engineered Messages. Available from:
<https://www.cyber.gov.au/publications/detecting-socially-engineered-messages>
- 23 Australian Government Information Security Manual, updated January 2019. Available from:
<https://www.cyber.gov.au/ism>
- 24 Attacks on computer systems. Available from:
<https://www.acorn.gov.au/learn-about-cybercrime/attacks-computer-systems>
- 25 Ransomware. Available from: <https://www.us-cert.gov/Ransomware>
- 26 Data breach notification - steps to follow. Available from:
<https://www.myhealthrecord.gov.au/for-healthcare-professionals/data-breach-notification-steps>
- 27 Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth). Available from: <https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response>

Publication date: February 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