Risk Alert

DECEMBER 2021

ansvar
RISK

The Care Sector and Cyber Risks

RANSOMWARE ATTACK: CEO SHARES EXPERIENCE AND ADVICE

This Risk Alert shares the experience of one care provider who suffered a ransomware attack, the impact of the attack on their business and what they did to resume operations. It also provides essential advice on what you should do if you suffer a cyber-attack.

The Australian Cyber Security Centre has issued a “critical” warning that ransomware known as “Maze” is targeting health and aged care sector around Australia.

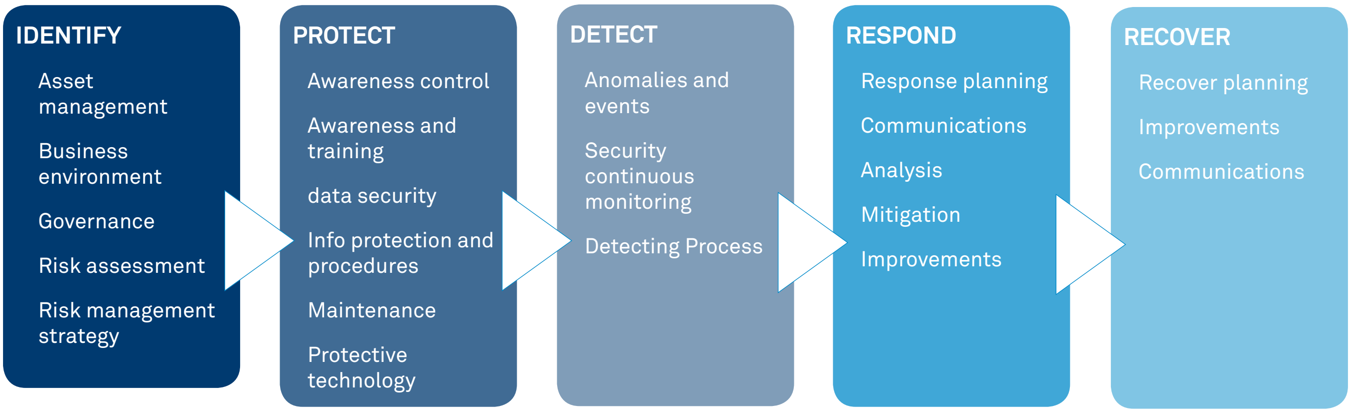
These sectors are targeted due to the sensitive personal and medical information they maintain in order to care for their patients and residents/ customers.

Effective risk management has been demonstrated to help organisations improve their ability to manage cyber risks and cyber resilience by:

- Identifying cyber risks and vulnerabilities
- Developing detection and protection measures
- Establishing contingency plans
- Having respond and recovery plans

A Risk Based Approach to Cyber Security

The reality is, it is nearly impossible to detect and respond to every cyber-threat, so it's better to protect business assets and mitigate risk by detecting and responding quickly to any potential breach.



IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Awareness control
- Awareness and training
- data security
- Info protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detecting Process

RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recover planning
- Improvements
- Communications

Using a framework such as the one below, you can start to understand your current position on cyber activity.

Identify

What are the organisation's cyber-security risk to systems, assets, data and capabilities.

Protect

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect

Develop and implement the apropriate activities to ***identify*** the occurrence of a cyber-security event.

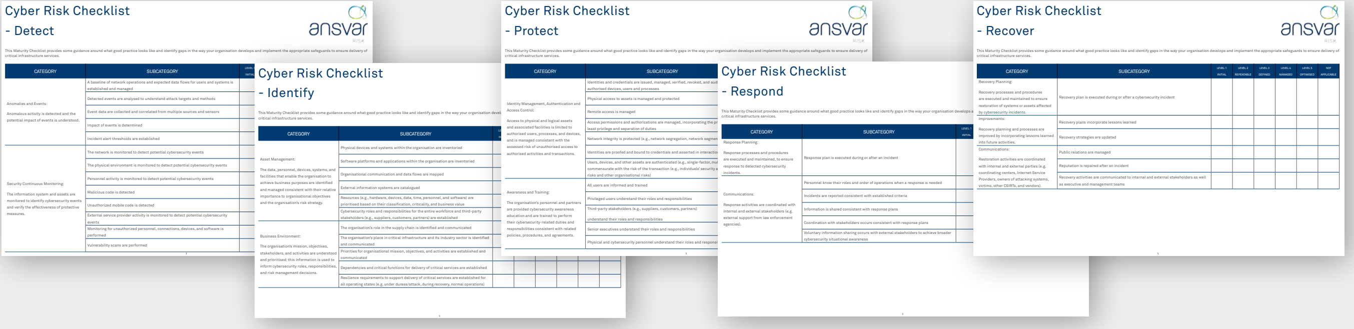
Respond

Develop and implement the appropriate activities to ***take action*** to a detected cyber-security event.

Recover

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-security event.

Working with Australian Managed Service Security Provider, Interactive, Ansvar Risk has developed a Cyber Risk Assessment Tool to provide guidance around what best practice looks like in terms of risk management and help identify any gaps in the way your organisation manages cyber security risks. Click here to download.



Cyber Risk Checklist - Detect

Cyber Risk Checklist - Identify

Cyber Risk Checklist - Protect

Cyber Risk Checklist - Respond

Cyber Risk Checklist - Recover

A CEO’s Experience

A number of Aged Care Providers have recently suffered cyber-attacks, leaving them without access to files and clinical records. A recently reported attack on Aged Care Provider resulted in the release of sensitive personal data.

Ansvar Risk recently interviewed a CEO of a large Aged Care organisation, following a recent ransomware attack in their business. Their insights and advice are valuable to all care sector organisations.

WHAT HAPPENED

The care provider’s IT service provider identified an issue at 6.00 am and found a breach had occurred at 9.30pm the previous day. By 6.00am the care provider had been locked out of some of its servers.

The IT service provider shut down the servers to stop further damage and started its investigation, identifying it as a ransomware attack. They located a ransom note demanding money to release the service – there was no reference to taking or leaking data.

HOW DID THEY RESPOND

The CEO was advised at 6.30am. Knowing they didn’t have the capability to manage the incident, the CEO sought advice from their professional network. The advice was simple - don’t react immediately, take a breath and develop a recovery action plan.

The incident was managed by the CEO and CFO, leaving others on the executive team to manage operations. The CEO focused on the recovery plan, while the CFO worked with the IT Service provider.

Since February 2020 any breach of personal data affecting organisations with revenues of $3 million and over, or holding healthcare records must be reported to the Office of the Australian Information Commissioner within 30 days of the breach being identified.

The organisation’s recovery process involved six steps:

Step One:
They contacted their insurance broker and insurer to understand their cyber insurance coverage and how the insurer could help. The broker liaised with the insurer who approved engagement of a Cyber Incident Manager to help with recovery and a lawyer for potential data breach.

Step Two:
Identifying the Impact. The IT Service provider identified the impacted servers, controlled emails and operational hard drives impacting the administrative functions.

As the organisation was implementing its IT strategy, it had moved its Clinical data to cloud storage, minimising impact on clinical programs and, allowing clinical staff to continue operations.

The focus was risk assessing potential data breaches and recovering email access, as email is the main form of communication to and from residents’ families.

Step Three:
Recover. The Cyber Incident Manager coordinating with the IT Service Provider, worked to recover access to the servers.

Step Four:
Keep staff informed. The staff WhatsApp group became the main form of staff communication to inform and update staff until the servers were restored.

Step Five:
Identify data breaches. Working with the lawyer, a forensic review was undertaken to determine if any data had been removed and if there had been any legislative breaches. Any data breach must be reported to the Office of the Australian Information Commissioner within 30 days after the breach.

Step Six:
Resumption with full access to the servers was achieved within 5 days.

Learnings

The CEO noted that there were many learnings from this incident. The main ones were:

- Make sure your organisation or its IT provider has a response and containment plan.
  - Take a breath – don’t react immediately or make rash decisions to get the business back up. Investigatethe impacts and develop a recovery plan.
- Speak to your broker and insurer about what your policy covers and how they can help.
- Bring in expertise to help manage recovery.
- Keep your Board and staff informed: determine your messaging platform and if you don’t have one,
- consider a WhatsApp group for all employees.

GUARDING AGAINST CYBER FRAUD

The No More Ransom Project, (an initiative of the Netherlands' police, Europol's European Cybercrime Centre, Kaspersky and McAfee) suggest the following risk mitigation strategies:

☑ Back-up regularly. Have a recovery system in place so data isn't lost forever.

☑ Use antivirus software to protect systems.

☑ Keep all software up to date.

☑ Ensure staff are aware not to open attachments in emails from people or organisations they don't know.

☑ Enable the 'Show file extensions' option in the Windows settings. Making it easier to spot potentially malicious files.

☑ Ensure staff delete files with extensions like '.exe', '.vbs' and '.scr'.

☑ If an unknown process or file is identified, disconnect device immediately from the internet or other network connections.

Types of Cyber Attacks

Phishing & Social Engineering:
Fraudulent communication to trick you into sharing private information or downloading viruses.

Malware:
Various forms of harmful software that hackers use to wreak havoc on your computer or network.

Ransomware
A form of malware that holds your data captive with the threat to publish or destroy it unless their ransom is paid.

Denial of Service Attacks

When a website is maliciously flooded with more visitors than it's equipped to handle, causing it to crash.

Data breach
Unauthorised access to sensitive or personally identifiable information.

Strategies to mitigate cyber security incidents must be a prioritised list to assist protecting systems and should be customised based on each organisation's risk profile.

ACSC
Australian
Cyber Security
Centre

The Australian Signals Directorate's Essential Eight Guidelines provides a series of mitigation strategies useful for care providers to protect themselves from cyberattacks or data breaches.

https://www.cyber.gov.au/acsc/view-all-content/essential-eight

What do you do it you have a breach?

Implement your Cyber incident plan. The plan should include 4 key four key steps to consider when responding to a breach or suspected breach.

Step One: Contain the breach

The following may help you identify strategies to contain a cyber-incident:

- How did the breach occur?
- What was the impact - Is data being shared, disclosed or lost without authorisation?
- Who has access to the personal information?
- What can be done to secure information, or stop the unauthorised access or disclosure?

Step Two: Assess the risks associated with the incident

Gather and evaluate as much information about the breach as possible to understand the impact, and identify and take all appropriate steps to limit the impact of the data breach.

In your assessment of a data breach, consider:

- The type of types of personal information involved
- The circumstances of the data breach, including its cause and extent
- The nature of the harm, and if this harm can be removed

Step Three: Consider breach notification

- Who should be notified
  - Your insurance broker and insurer for direction and advice
  - Your IT Service provider
- Does the incident trigger reporting obligations to other organisations such as Office of the Australian Information Commissioner

Step Four: Review the incident and take action to prevent future breaches

This might involve:

- A review including a root cause analysis of the breach
- A prevention plan for similar future incidents
- Prevent plan is implemented with audit programs
- A review of policies and procedures to reflect lessons learned
- Changes to employee selection and training practices
- A review of service delivery partners that were involved in the breach

The response team should ideally undertake steps 1, 2 and 3, simultaneously or in quick succession. At all times, the response team should consider whether corrective action can be taken to reduce impact or harm to the organisation.

The Telstra Security Report 2019 identified the number one risk to IT security is human error – often caused by inadequate business processes and employees not adequately understanding their organisation's security position.

Ansvar has recently responded to a number of phishing (social engineering) and third party fraudulent activity claims under its Management Liability policies.

Organisations need appropriate safeguards for requests for sharing or amending private information such as changes to a supplier's or creditor's banking details, or purchasing of transferable e-tickets or vouchers purportedly requested by a senior employee. A simple practice is to double check with the supplier or employee, particularly where the request seems unusual or is from a different email address.

Cyber Risk Insurance

Cyber insurance may give you piece of mind. Speak to your broker to determine how you can ensure you have the right insurance that covers your cyber risks.

References

The following resources can provide you with more guidance to help you protect your systems, data and personal information.

The Australian Signals Directorate's Essential Eight guidelines

https://www.cyber.gov.au/acsc/view-all-content/essential-eight

Victorian Government Incident Response Plan Template

https://www.vic.gov.au/prepare-cyber-incident

National Cyber Security Centre United Kingdom Government

https://www.ncsc.gov.uk/section/information-for/public-sector

How to organize your security team: The evolution of cybersecurity roles and responsibilities (Microsoft)

https://www.microsoft.com/security/blog/2020/08/06/organize-security-team-evolution-cybersecurityroles-responsibilities/

Take Action Now - We Can Support You

Ansvar Risk is encouraging clients to be floor and storm ready. Ansvar Risk provides a range of consultancy services to assist clients to review and enhance their systems, processes and practices and the time to act is now.

For further advice, email us at info@ansvarrisk.com.au

Anthony Black

SENIOR RISK CONSULTANT - ERM & NATIONAL CARE PRACTICE LEADER

0402 239 149

ablack@ansvarrisk.com.au

As our National Care Sector Leader, Anthony works with organisations throughout Australia to support governance and risk management capability; supporting boards, senior managers and staff to implement effective approaches to support decision making, improve performance, optimise objectives and prevent harm.

Ansvar Risk is a division of Ansvar Insurance Limited, ABN 21 007 216 506 AFSL No 237826 ("Ansvar"), Level 5, 1 Southbank Boulevard, Southbank VIC 3006. This information is general in nature and does not constitute legal, financial or personal advice. Before using this information, you should consider the appropriateness of it having regard to your own business objectives, needs and individual circumstances. While every care has been taken in preparing this document, Ansvar makes no representations and gives no warranties of whatever nature in respect of the accuracy or completeness of the information contained therein.