

An aerial photograph of a coastal defense structure. The left side shows turbulent blue water with white foam. A vertical concrete wall runs down the center, covered in a dense layer of interlocking concrete armor units (Tetrapods). To the right of the wall is a beach made of small, light-colored stones. The sky is not visible.

Ransomware Defence

Recommended Practices

It's time for defence in depth

Overview

Ransomware: It's time for defence in depth	1
The nature of ransomware is changing	2
Insurers reach a tipping point	3
Assessing ransomware risks	4
Recommended practices:	
Leveraging the appropriate controls across people, process and technology	5
1. Identify – Understanding and assessing the risks ransomware poses to your organisation	6
2. Protect – Developing protective safeguards to prevent ransomware threats	7
Manage risk through identity controls	7
Privilege Access Management (PAM)	7
Multi-Factor Authentication (MFA)	7
Training & Awareness	8
Phishing Simulation	8
Incident Response Preparedness	8
Incident Response Plan	8
Testing the Incident Response Plan	8
3. Detect – Identifying and discovering cyber security events and incidents prior to response	9
Monitor for vulnerabilities	9
Utilise threat intelligence to stay ahead	9
4. Respond – Taking action to respond in the event of a ransomware incident	10
Leverage Endpoint Detection & Response (EDR) to contain, analyse, mitigate and improve in real-time	10
5. Recover – Returning to business operations and minimising the impacts of a cyber incident	11
Engage in Business Continuity and Disaster Recovery (BCDR) planning	11
What is your organisation's Ransomware Defence Maturity Level?	12
Complete Aon's Ransomware Defence Checklist	13

Ransomware:

It's time for defence in depth

Ransomware is rapidly becoming the dominant tool for cyber criminals intent on extracting significant value from their victims via the dual threat of paralysing business systems and the use of stolen confidential data in order to extort ever growing ransom payments. But are organisations doing enough to combat the threat? According to Aon's 2021 Cyber Security Report, only 31% report having adequate business resilience measures in place to deal with ransomware.¹

Ransomware is a critical risk for modern businesses, with the frequency, sophistication and business impacts of ransomware attacks increasing significantly over recent years. Ransomware cannot be underestimated for its ability to inflict significant financial, business interruption and reputational damage. The methods used by threat actors do not stand still and neither should the defences that organisations use to nullify their activities. A defence in depth approach is required to manage ransomware and should be regularly considered based on industry advancements. This is not confined to technical measures: ransomware-related losses have also impacted the cyber insurance market.

Introducing Aon's Ransomware Defence Recommended Practices

Developed with the purposes of helping organisations understand the controls needed to manage their cyber defences against ransomware; these recommended practices identify the common and accessible ways to protect businesses from suffering an attack and what to do in the event a cyber incident occurs.

Proactive engagement by executive or technical teams with these recommendations can help manage and mitigate the risk of ransomware and in so doing, improve their risk profile in an increasingly challenging market for securing cyber insurance cover.

Whilst these controls regularly align with risk and technology capabilities, resilience cannot be achieved through deploying these controls alone and each

defensive measure should form part of a wider cyber security strategy encompassing governance, technical controls, risk and financial mechanisms that are all based on an understanding of the relative cyber risk.

These recommendations have been developed based on practical experience of delivering 20+ years of cyber solutions and through leveraging industry practices and frameworks. The intention of this guidance is to consolidate the controls which can positively impact the cyber defences of an organisation required to manage ransomware threats. Each of the recommended practices align with the categories defined by the National Institute of Standards and Technology (NIST) Cyber Security Framework: [Identify](#), [Protect](#), [Detect](#), [Respond](#) and [Recover](#).

Mitigating the ransomware threat

Resilience requires a multi-function combined approach and strength in one domain does not make up for a deficiency in another, there is also no true one size fits all solution. Aon's end-to-end approach to managing the threat of ransomware comprises three key phases: Assessment, Mitigation and Transfer – the controls outlined in this document align to the Mitigation phase of this process.

To help understand the maturity of defences within your organisation, [Aon's Ransomware Defence Checklist](#) considers current capabilities on a maturity scale of 'Initial' to 'Advanced'. An indication of overall ransomware defence maturity can be achieved by completing the checklist, which will also highlight key improvement areas.

In support of enhancements needed and aligning to these recommendations, Aon have consolidated critical experience, capabilities and these key recommendations to develop a Ransomware Defence Bundle designed to help enhance the protective controls needed to establish a defence in depth approach when managing the risk of ransomware. To learn more get in touch with your local Aon contact.

1. Aon's 2021 Cyber Security Risk Report <https://www.aon.com/2021-cyber-security-risk-report/>

The nature of ransomware is changing

As the fastest growing type of cybercrime facing organisations in 2021, global ransomware damage costs are predicted to reach US\$20 billion in 2021, a **more than 50 times increase** from 5 years ago.²

The increase in ransomware attacks is exponential. With the rise of Ransomware-as-a-Service, staying out of the attack path is even harder for organisations as criminals share hacking tools and sell malware between groups. The total damage costs associated to ransomware are likely even higher than reported as victims often remain silent and pay ransoms discreetly, while attackers do not always publish data from compromised networks.

Neither the public sector nor private organisations, regardless of size or industry, are immune and many organisations on the attack path still only have basic levels of cyber hygiene and defence. As attackers move on from ‘spray and pray’ tactics to target practice and big-game hunting, proactive defence has become urgent. The threat to organisations is not only around encryption and business interruption, but also the possibility of hackers releasing stolen sensitive and confidential data.

Myth of the zero-day attack

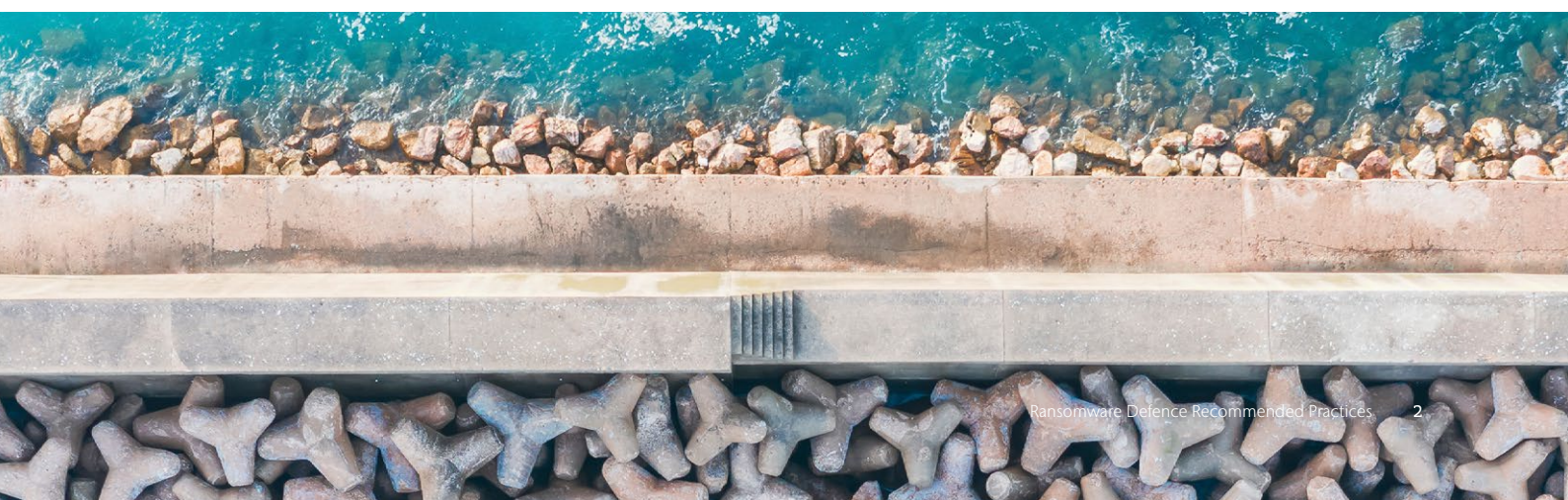
It’s a fallacy to assume attackers focus on zero-day vulnerabilities and only access the network at the time their attack is launched. Attackers are likely to have accessed the network much earlier using that time to carry out reconnaissance and the creation of admin accounts to escalate their privileges. To gain ongoing access when launching their attack, they disable firewall rules, activate remote server access, and even set up a persistent backdoor into the network, bypassing normal authentication or encryption. Before the attack even happens, often they will already have exfiltrated data both to prove that they have access and to threaten exposure.

Extortion on the rise

The emergence of double extortion tactics explodes another myth that secure back-ups can be relied upon to deal with ransomware demands. Increasingly attackers focus on targets not only because they can easily exploit known vulnerabilities to demand ransom payments, but because they sense a bigger payday through data leaks.

Even where back-ups have not been compromised and used to restore services, attackers can still apply pressure on the victim to pay the ransom by selectively publishing sensitive data as extortion leverage. Complying with the ransom payment demand to gain access to decryption keys is no guarantee against subsequent data leaks, and there are cases of payments being made and criminals later monetising exfiltrated data by auctioning it on the dark web.

²<https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/>



Insurers reach a tipping point

Insurance is a key weapon in the armoury for organisations to use in the fight against ransomware, but a dramatic increase in the **frequency and severity of ransomware-related losses** has impacted the cyber insurance market.

Insurers are demanding increased levels of underwriting information from organisations to ensure they can demonstrate their preparedness for a ransomware attack and have appropriate levels of security control maturity.

In the same way that property insurance cover demands adequate fire safety measures, cyber insurance is also often predicated on the implementation of corresponding cyber 'hygiene' measures. Demonstrating proactive risk mitigation strategies, such as assessment and testing, is now critical to better position a risk with an insurer and in helping to secure cyber insurance.

Insurers are reviewing ransomware exposure via specific supplemental questionnaires and use of scanning technology. Their focus is now on business continuity and disaster recovery planning, privileged access controls, multi-factor authentication, proactive scanning/testing, and overall incident response readiness.

In addition, insurers are continually adjusting their underwriting approach, reviewing terms and conditions of coverage, and re-evaluating capacity deployment. Specific examples of coverage considerations that insureds will need to navigate are included in Aon's 2021 Cyber Insurance Snapshot,³ but the conclusion for organisations is that a strategic risk-based broking approach is critical in a hard cyber insurance market.

Careful preparation of an organisation's underwriting submission is vital in order to differentiate themselves in the market and to maintain access to insurers' capital. Insurers are continually raising the bar in terms of the risks they'll accept. What might pass scrutiny this year, won't necessarily pass next year.

To keep ahead of the threat and remain an attractive risk for insurers, organisations must continuously improve their cyber security posture and be prepared to tell their story to underwriters, while also helping to facilitate the possibility of long-term market partnerships which can make all the difference in a hard market. Cyber insurance is an important risk mitigation measure for the corporate balance sheet which means that correct levels of transparency with insurance partners from the enterprise (and vice-versa) must be fostered, maintained and developed.

3. Aon's 2021 Cyber Insurance Snapshot
<https://www.aon.com/cyber-solutions/thinking/aons-cyber-insurance-snapshot-emea/>

With insurers seeing both an increase in frequency and severity of ransomware-related losses, **organisations should be prepared to showcase their preparedness** for a ransomware attack.

Assessing ransomware risks

Risk management programmes must be **based on a data-driven approach** that assesses potential vulnerabilities at both system and human factor levels.

Many organisations will have existing investments in cyber risk management programmes, and it is important to consider if and how this can align accordingly. Industry frameworks such as the NIST Cyber Security Framework provides specific profiles which can be used to assess, mitigate and manage the risks posed by ransomware, and shows the importance of systematically identifying enterprise-wide risks prior to taking actions to remediate and protect against these issues.

As an ever-expanding threat, a cyclical approach to assessment will enhance an organisation's view of mission critical assets, but also allow it to easily demonstrate weaknesses in the programme. This provides the blueprint to make better decisions, whether for vulnerability prioritisation, patching frequency, or new technology investment to achieve the risk reduction goals. Another challenge for many organisations is creating a sustainable methodology to facilitate a process that can incorporate several workstreams. For example, it does not make sense that cyber security assessments remain separate from insurance underwriting submissions or ransomware supplemental question sets.

Organisations must adapt processes to save time and maximise output. The insurance policy needs to be a natural complement to the security strategy. That means, if it doesn't fit alongside and work in parallel to IT and information security then perhaps it doesn't fit at all. Further still, alignment with corporate risk registers and creating executive level understanding of the strategic security investment programme, will enhance the overall governance protocols associated with ongoing improvement and business resilience.

“There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again.”⁴

Robert Mueller
Former Federal Bureau of Investigation

4. <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>

Recommended practices

Preparedness for a ransomware attack requires a mature and considered approach, **leveraging the appropriate controls across people, process and technology.** Many control domains may be technical by nature, but require alignment with governance, risk and business owners to achieve resilience.

Equally, controls should not be reviewed as stand-alone capabilities and rather seen as integral measures forming part of a wider enterprise defence to cyber threats, and specifically considered regarding ransomware.

These recommendations reflect a combination of practical experience, industry best-practices and feedback from leading cyber security and insurance partners, however, they also align with the *NIST Cybersecurity Framework Profile for Ransomware Risk Management*. The intention of these recommendations is not to mirror those controls outlined in this standard, but consolidate and reflect on Aon's 20+ years of developing cyber solutions to provide organisations with clear and practical guidance they can take to safeguard their businesses against ransomware.

These recommendations consider cyber control areas which can be a useful tool to understand the preparedness of an organisation not just to respond, but also to deliver an end-to-end cyber risk management framework: **Identify, Protect, Detect, Respond, and Recover.**



Identify

Understanding and assessing the risks ransomware poses to your organisation.



Protect

Developing protective safeguards to prevent ransomware threats.



Detect

Identifying and discovering cyber security events and incidents prior to response.



Respond

Taking action to respond in the event of a cyber incident.



Recover

Returning to business operations and minimising the impacts of a cyber incident.

Identify

Understanding and assessing the risks ransomware poses to your organisation.

Controls to consider:

Do you understand your organisation's attack profile and have you reviewed governance, controls, roles and responsibilities?

Have you tested your defences by reviewing the defensive security controls of key systems?

The **Identify** function represents the understanding and assessment of the risks ransomware poses to an organisation. This can mean understanding the technology estate within an organisation, roles and responsibilities and security of key business systems. These insights help to form a foundation required to build and manage the appropriate protective mechanisms needed to mitigate the risk of ransomware. As part of an assessment, organisations should look at how data is backed up and whether the organisation could re-create the data if the systems that store the data were to be attacked. In order to defend against ransomware, it is critical that organisations understand their attack profile and test the controls of their systems.

Understand the organisation's attack profile: Review governance, controls, roles and responsibilities

In order to manage a risk, it is important to first understand it. Moving beyond a general cyber risk assessment (which is recommended as part of good security hygiene and provides a useful assessment of cyber risk), Aon recommends that organisations understand their attack profile as it may relate to a ransomware incident. This means assessing the systems and data that the organisation relies on to do business, the attack surface of the technology estate and the maturity of associated protective controls specifically to a potential ransomware attack.

Taking a framework such as NIST which has a specific profile for ransomware, Aon recommends that organisations undertake a review of governance relating to cyber security, and consider who is responsible, accountable, consulted

and informed (RACI) for the management of ransomware risk. This will help not only with protective/defensive controls, but also with planning and recovery following a cyber incident. A risk assessment should also consider asset management, risk governance and the implications third-parties may have on the organisation's attack surface. Through understanding the existing maturity of such control mechanisms this can help guide and influence the investments made into the required security domains.

Test defences: Review the defensive security controls of key systems

Further to assessing the maturity of controls and gaining a greater understanding of the organisation's attack surface, Aon recommends the security testing of key business systems to identify vulnerabilities within the estate and validate the likelihood of a potential ransomware attack against them. This can be achieved in part through ongoing vulnerability scanning and management, however, it can be furthered through targeted security testing activities. Whilst the exact target of such testing will be dependent on the systems within the organisation and the associated criticality, typical recommended systems for assessment include Active Directory, Office 365, corporate email systems and the testing of a corporate build or 'endpoint'. These recommendations are provided due to the way ransomware spreads (often triggered through a phishing email/compromised endpoint) and the systems associated. Given that protective controls within these targets will provide an initial line of defence, Aon recommends assessing the efficacy of them before an attacker does.

Protect

Developing protective safeguards to prevent ransomware threats.

Controls to consider:

Have you deployed Privilege Access Management (PAM) and are Multi-Factor Authentication (MFA) controls in place?

Are you continually strengthening employee cyber security awareness, for example, through Phishing simulations?

Do you have an adequate Incident Response plan in place, and have you recently tested it?

The **Protect** function focusses on developing the appropriate protective safeguards needed to manage the risks outlined in Identify. Specifically, this means protecting the people, technology and data within the business, deploying critical security tools and preparing for incident response.

Manage risk through identity controls

Business users are often the first point of attack for ransomware criminals and therefore protecting against initial account compromise can be the first line of defence. The capability of Identity and Access Management (IDAM) focusses on providing the right users access to the right systems for the right reasons and in the right way – securely. As ransomware spreads by following the access of an infected user/endpoint and encrypting associated files and business systems, managing user access and authentication can be essential in prevention as well as in response should a ransomware attack strike.

Privilege Access Management (PAM)

PAM solutions work through granting access to systems only when needed, with the right reasons and for a limited amount of time, with mature solutions offering features such as session monitoring for investigative and audit purposes, or automated password management/rotation services to prevent ‘password spraying’ techniques. To deploy and utilise PAM, it is important to understand which employees have access to which systems. Only provide access to data or systems on a ‘needs must’ basis – otherwise referred to in the industry

as ‘the Principle of Least Privilege’ (PoLP). Prior to deploying any solutions Aon recommends first analysing current users and access rights across the organisation and defining an access management policy needed to drive a technology plan – identifying who should have access and when, and how this will be managed. Once a policy is in-place, Aon recommends deploying a PAM solution for the management of administrator access and ongoing enforcement and audit against this policy. In the UK the National Cyber Security Centre (NCSC) recommends utilising a Privileged Access Management solution “removing the need for administrators to directly access high-value backup systems” and minimising this risk.⁵

Multi-Factor Authentication (MFA)

Many digital transformation strategies increase the number and type of business systems provided to business users, meaning multiple authentications may be needed. Authentication points provide an opportunity for compromise by attackers using ‘password spraying’, ‘brute force’, or ‘credential stuffing’ techniques. A control which can help mitigate this risk is Multi-factor Authentication (MFA), which is a way of authenticating users requiring more than two forms of authentication to gain system access with examples of additional verification steps including biometrics, SMS verification, and secret question/answers. Through adding an additional layer of verification, businesses can reduce the likelihood – or ease – of account compromise techniques which can be a first stage of a ransomware threat actor.

5. <https://www.ncsc.gov.uk/collection/secure-system-administration/use-privileged-access-management>

When considering MFA Aon recommends first analysing the objectives specifically to the business estate and defining the success criteria, critical user groups, critical assets, number of users and overall management process. Once the objectives and processes have been defined, consider deploying or adopting the appropriate tooling needed which will depend on the business estate and existing technologies. Organisations should consider the deployment options available (cloud-based vs on premise), types of functionality, and integrations to other key functions (such as PAM or Security Operations Centre requirements). The UK National Cyber Security Centre states that “Multi-factor Authentication (MFA) should be enabled, and the MFA method should not be installed on the same device that is used for the administration of backups.”⁶

Training & Awareness

Ransomware attackers will often seek to exploit unsuspecting business users to launch an attack. At times of business disruption technology change attackers seek to take advantage of unsuspecting business users, performing reconnaissance on their targets before attempting to exploit. Training staff to defend against attack techniques becomes a critical capability when managing ransomware risk. A lack of knowledge is almost never the fault of the user, but should be addressed by the organisation in the form of a structured Training & Awareness campaign designed to ensure end-users have the knowledge and skills they require to keep themselves and the business secure.

Phishing Simulation

One way of identifying gaps in staff security awareness is to run a phishing simulation. One of the most common methods of attack is through phishing emails designed to trick people into handing over sensitive data, which can be used to access protected data, networks and systems. In the early weeks of the COVID-19 pandemic phishing attempts rose by over 600% in the early weeks alone.⁷ A phishing attack has the potential to lead to critical business impacts and it is crucial that organisations help employees to understand “what is phishing?” and how to spot and report phishing attempts. A well-designed campaign simulates real-world phishing attacks to assess employee security awareness, highlight gaps in knowledge and improve the education of users to help recognise the threats that these attacks can pose.

Incident Response Preparedness

In the event of a cyber incident rapid detection and response can be critical to minimising impact. It is vital to prepare the organisation to respond to cyber incidents such as ransomware across people, process and technology domains. This includes the core capabilities outlined below to develop and test plans and Incident Response (IR) functions.

Incident Response Plan

An initial place to begin incident response preparedness is the IR Plan. A comprehensive plan that is stress-tested regularly helps to ensure that a business can activate the right resources, at the right times throughout the incident lifecycle, providing a streamlined process to bring the matter to a close. It should outline the key steps to follow in the event of an incident (organisations commonly build from the NIST Incident Response Framework of Preparation, Detection & Analysis, Containment, Eradication & Recovery) and align to wider business security and crisis management policies. A key factor is pre-agreeing roles and responsibilities in the event of a cyber incident – consider legal, PR, HR, IT, C-Suite etc. and who is responsible, accountable, consulted and informed throughout. Clear lines of communication, governance and escalation should be identified for each phase of an IR process and specific to ransomware organisations should consider a playbook to identify business impacts and the associated preventative, containment and recovery measures to follow should an incident occur. Consideration should also be made in how to access the plan, who should have access and how regularly to test it.

Testing the Incident Response Plan

To assess the completeness of IR capabilities during a potential ransomware event, Aon suggests a targeted Cyber Threat Simulation Exercise. Testing of the Incident Response Plan should be conducted at both a technical and leadership level to assess the appropriateness, completeness and efficacy of the controls in place to mitigate and manage a ransomware response. The testing should include careful scenario scoping and align to realistic scenarios and be tailored to the risks facing the organisation. Organisations should capture lessons learned to identify key strengths, gaps, risks and recommended improvements to the plan.

6. <https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services>

7. <https://www.accenture.com/us-en/blogs/business-functions-blog/the-human-aspect-of-cyber-security-in-a-covid-19-world>

Detect

Identifying and discovering cyber security events and incidents prior to response.

Controls to consider:

Do you employ continuous network vulnerability scanning?

Are you proactively utilising threat intelligence to monitor for the tactics, techniques and procedures (TTP's) of cyber attackers?

The **Detect** function considers the development of controls and measures to enable the identification and discovery of cyber security events and incidents prior to response. Going beyond the deployment of software that performs anti-virus scanning (which should be considered an implicit requirement), many organisations invest in protective monitoring capabilities to provide visibility across the estate. Detection capabilities such as a Security Operations Centre (SOC), Security Information Event Monitoring (SIEM), or Endpoint Detection & Response (EDR) can be critical enablers for finding and triaging security events/incidents and should leverage a risk-based approach to the detection rules employed.

Many of these capabilities can offer both detection and response capabilities ([see EDR](#)). Aon recommends enabling the tooling and processes needed to proactively provide visibility of events across a technology estate through protective security monitoring and utilising capabilities such as threat intelligence to detect external threat actors and get ahead of cyber incidents before they happen.

Monitor for vulnerabilities

One of the key elements within the detection phase is the ability to detect known vulnerabilities and malicious code within the target environment. In order to find and fix vulnerabilities before they become incidents, Aon recommends employing continuous network vulnerability scanning. For critical systems or those connected to the internet, the ability to continuously review for vulnerabilities can provide immediate focus on those occurring as a result of activities such as configuration and management system updates. Organisations should

give careful consideration to the tooling and services able to deliver this, with a critical output being the reporting. The goal is to provide an IT team with the tools needed to identify security vulnerabilities in the network infrastructure, applications and APIs (either on the internet or internally), and then track and manage remediation of identified issues before they can be taken advantage of by an attacker.

Utilise threat intelligence to stay ahead

In addition to network-level protective monitoring capabilities, the use of threat intelligence can be critical to proactively identify threats (insider and external) in addition to compromised credentials, threat actors and otherwise. Tooling-based security solutions provide a solid foundation for detecting live security events and can be augmented by the use of proactive threat intelligence which monitors for the tactics, techniques and procedures (TTPs) of adversaries which can be used to defend against specific strategies.

Aon recommends considering the threat profile of the organisation and developing a series of key search criteria to determine the focus of a threat intelligence function. A mature threat intelligence function should have the ability to monitor across industries, geographies, languages and a variety of information sources (e.g. deep/dark web, hacking forums etc.) and correlate information to determine the likelihood and extent of threats facing the organisation. Typically, threat intelligence can be performed either as a one-off exercise (e.g. with a focus on a specific threat or event) or as an ongoing capability supporting the information security function. Aon recommends utilising an ongoing proactive threat intelligence function based on key threats and assessing directly at times of business or technology change.

Respond

Taking action to respond in the event of a ransomware incident.

Controls to consider:

Do you leverage Endpoint Detection and Response (EDR) as a cyber defence?

The **Respond** function considers the criticality of taking appropriate action to respond effectively in the event of a major cyber incident. As outlined elsewhere in these recommendations, planning and rehearsing incident response plans are key, equally, in a response scenario having the right tools at an organisation's disposal can make all the difference when managing impacts.

For consideration, the NIST Cyber Incident Response Lifecycle comprises four key phases:

- Preparation
- Detection & Analysis
- Containment, Eradication & Recovery
- Post-incident Activity

Having – and regularly testing – a tailored incident response plan is a critical factor in an organisation's ability to respond to cyber incidents when they occur. Through gaining proactive visibility via detection, scanning and threat intelligence capabilities, it can be possible to capture events earlier in the kill-chain to prevent and minimise impact. In addition to those factors, Aon recommends engaging the appropriate tools capable of Containment, Eradication & Recovery real-time in a way that enables organisations to reduce the spread, scale and impact of an incident.

Leverage EDR to contain, analyse, mitigate and improve in real-time

Like many cyber security attacks, the initial entry point for ransomware threat actors is often through phishing or spear-phishing via the opening of an infected phishing email attachment, or compromising a machine setup for remote access. Many ransomware threat actors can infect the machines and networks and bypass traditional cyber security defences such as Anti-Virus (AV).

Given the initial infected target device or 'endpoint' is the first entry point for the attackers into the corporate network, one of the most critical tools within cyber defence is an Endpoint Protection Platform (EPP) and specifically, Endpoint Detection & Response (EDR). Modern EDR capabilities provide organisations with visibility (see Detect) to attacks happening on devices (endpoints) across their technology estate to provide the context and remediation controls needed to respond to ransomware incidents in real-time. Through establishing a mature EDR capability within an organisation's cyber defence operation, it is possible to proactively contain and respond to the threats in real-time once initial compromise has occurred.

Aon recommends utilising an EDR capability which can leverage threat intelligence and data modelling techniques to analyse real-time activity to proactively isolate activity recognised – or indicative – of a ransomware threat and interrogate, mitigate or respond prior to traffic expanding elsewhere. Leading EDR capabilities complement this through the ability to isolate, investigate and respond to suspicious files and software which can provide further critical information to get ahead of the attackers and proactively update the rest of an organisation's endpoint protection controls in real-time.

Building response capabilities using EDR is more than just deploying a tool and requires a combination of process, governance and tooling which should first be established in order to run effectively. Once the requirements and support model are understood, Aon recommends investing in appropriate EDR tooling capable of being deployed across the entire estate, utilising threat intelligence and technologies to analyse Indicators of Compromise (IOCs) and Indicators of Behaviours (IOBs) in real-time to proactively block ransomware threats traditional Anti-Virus capabilities may have missed.

Recover

Returning to business operations and minimising the impacts of a ransomware incident.

Controls to consider:

Do your Business Continuity and Disaster Recovery (BCDR) plans take account of and regularly test for Ransomware threats?

Ransomware risk is **ever-changing and evolving**, and to manage it appropriately requires a combined strategy – not simply of cyber security, risk and insurance – but of the detailed controls outlined in these recommendations.

The **Recover** function focusses on the recoverability of an organisation following a ransomware incident, and the preparedness to be able to return to business operations. This is through developing and leveraging tried and tested plans in order to minimise ransomware impacts such as downtime, loss of production and/or lost productivity. This section of the recommendations specifically addresses the need to engage in business continuity planning which is aligned to incident response plans/playbooks relating to ransomware and tested regularly within the business.

Engage in Business Continuity and Disaster Recovery (BCDR) planning
Aligned to a cyber IR plan, a specific BCDR plan should be established which is specific to ransomware risk/loss scenarios. Business continuity planning is common in most enterprises, however, many organisations have not adapted existing practices to reflect an evolving organisation and are not dynamic enough to reflect a changing risk environment. This includes ransomware-related BCDR planning such as ensuring backups are carried out regularly and protected appropriately.

Aon recommends preparing for an incident by developing BCDR plans connected to incident response processes and then testing and updating those plans through an iterative process. This will help enable both a continuous improvement approach to BCDR relating to ransomware, but also provide organisations with the opportunity to improve through ‘lessons learned’.

PHASE ONE	PHASE TWO	PHASE THREE
Review the current ransomware risk landscape (see Identify): understand the key ransomware scenarios which could affect an organisation and review the potential impacts which require a BCDR plan	Review existing BCDR strategy: analyse the existing BCDR strategy of an organisation to ensure cyber/ ransomware specific scenarios align accordingly	Align BCDR plans to ransomware scenarios: develop and align specific BCDR plans to an organisation which can be leveraged when facing a ransomware event

As with each of the recommendations outlined in this document, no single control can provide a comprehensive defensive capability, nor does strength in one make up for another. Implementing and continually testing the effectiveness of these controls is critical given that attackers constantly evolve their attack methods and with those attacks becoming more frequent, targeted, sophisticated and costly.

What is your organisation's Ransomware Defence Maturity Level?

Understanding strengths, weaknesses and improvement areas is a critical first step towards ransomware defence preparedness. Organisations can gain an initial understanding of maturity by completing Aon's Ransomware Defence Checklist.

What is your organisation's ransomware defence maturity level?

Complete the checklist and refer to the score values below to help determine your organisation's overall Ransomware Defence Maturity Level.

Ransomware Defence Maturity Level	Score Value
Initial preparedness	10-14
Basic preparedness	15-24
Managed controls established	25-34
Advanced controls in place	35+

Aon's Ransomware Defence Checklist reflects our recommended practices and can help provide a quick and simple indication of your organisation's level of maturity and preparedness. This insight can provide initial critical visibility of ransomware preparedness and prioritise improvements and investments needed to remain secure.

Steps to complete checklist

Step 1

To start, work through the 10 Ransomware Defence Control questions

Step 2

Assign yourself a maturity score and record this in the correct box on the grid. For example; If you score a maturity score of 'Initial' on question 1, place a score of 1 in the corresponding box

Step 3






Once completed add up your score total for each of the five Ransomware Defence Control areas (*Identify, Protect, Detect, Respond & Recover*)

Step 4

To finish, add up your total scores for each Ransomware Defence Control area to determine your final score value and indicate your organisation's overall Ransomware Defence maturity level

> Aon welcomes the opportunity to help understand your current maturity, prioritise enhancements and discuss next steps.

Aon's Ransomware Defence Checklist

Ransomware Defence Control	Maturity Score				Score
	Initial = 1 Ransomware control is not performed or does not currently exist	Basic = 2 Ransomware control is managed in an ad-hoc or non-formalised manner	Managed = 3 Ransomware control is established across the majority of the organisation	Advanced = 4 An organisation-wide approach to managing the ransomware controls	
Identify  Do you understand your organisation's attack profile and have you reviewed governance, controls, roles and responsibilities?					
Have you tested your defences by reviewing the defensive security controls of key systems?					
Protect  Have you deployed Privilege Access Management (PAM)?					
Are Multi-Factor Authentication (MFA) controls in place?					
Are you continually strengthening employee cyber security awareness, for example, through phishing simulations?					
Do you have an adequate Incident Response plan in place, and have you recently tested it?					
Detect  Do you employ continuous network vulnerability scanning?					
Are you proactively utilising threat intelligence to monitor for the tactics, techniques and procedures (TTP's) of cyber attackers?					
Respond  Do you leverage Endpoint Detection and Response (EDR) as a cyber defence?					
Recover  Do your Business Continuity and Disaster Recovery (BCDR) plans take account of and regularly test for cyber/ransomware threats?					
Total					

> To help with the ongoing enhancement of your Ransomware Defence Maturity Level, Aon have developed a **Ransomware Defence Bundle** designed to help mitigate vulnerabilities and strengthen controls.
To learn more get in touch with your local Aon contact.

Contacts

**Contact our EMEA Security Advisory
Leaders to learn more.**

Kraig Rutland

Vice President EMEA
Cyber Security
+44 (0)7557 578 737
kraig.rutland@aon.co.uk

Andrew Hainault

Managing Director EMEA
Security Advisory
+44 (0)7903 708 834
andrew.hainault@aon.co.uk

Visit aon.com/cyber-solutions

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in over 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance. Aon is proudly celebrating over 20 years of delivering Cyber Solutions with a team of specialists supporting organisations across their entire cyber risk value chain.

This paper constitutes information only. Professional advice should always be sought regarding insurance coverage or specific risk issues including cyber risk services. Aon UK Limited is authorised by the Financial Conduct Authority (FCA) for insurance activities.

The following products or services are not regulated by the FCA:

- Cyber risk services provided by Aon UK Limited
- Cyber security services provided by Stroz Friedberg Limited and its affiliates

© Aon plc 2021. All rights reserved.

