optec

Ransomware Readiness Assessment

A Proactive Approach to Tackling the Ransomware Challenge

Is your organisation ready for ransomware?

Ransomware has become one of the biggest cybersecurity threats facing today's organisations. It's reached epidemic proportions globally and is now the 'go-to method of attack' for cybercriminals. In 2021, the average cost of recovery from a ransomware attack was £1.3 million.

While there's no way to completely protect your organisation against ransomware, you should adopt a comprehensive approach to prevent, detect and recover from attack. This assessment can help you quickly identify gaps in your IT and set you on the right path towards ransomware prevention.

Instructions

To conduct the assessment, use the maturity scorecard below. The scorecard describes a four-level evolutionary path of increasingly organised and systematically more mature processes. For each of the items in the ransomware readiness framework, you can access your organisation's maturity score and consider your priorities.

Maturity Score	Maturity Level	Description
0	Absence	No evidence the action exists in the organisation
1	Reactive	Basic action is in process, but cannot prevent problems from arising
2	Managed	Action is deployed across the organisation with common responsibilities and language in place
3	Proactive	Action is in place to proactively address current issues and challenges
4	Anticipatory	Action is in place to proactively address future issues and challenges

Source: https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.aspx

Mark the box that best fits your organisation's profile.

Ransomware Planning

The best defence against ransomware is to plan for it.

Action	Absence	Reactive	Managed	Proactive	Anticipatory
Conduct an assessment to identify your critical assets and determine the impact to these if an attack were to occur					
Have an incident response plan that includes what to do during a ransomware event and test the plan to ensure complete protection is delivered					
Develop a business continuity and disaster recovery plan					
Identify your legal obligations regarding the reporting of incidents to regulators and create a plan for approaching this					

Mark the box that best fits your organisation's profile.

Ransomware Prevention

Reduce the likelihood of ransomware reaching your users and devices.

Action	Absence	Reactive	Managed	Proactive	Anticipatory
Restrict access to common ransomware entry points and use a secure email gateway to block malicious content					
Use web filtering to stop users from traveling to malicious URLs that could deploy malware					
Reduce the attack surface and protect endpoint devices in order to prevent malware infection					
Enable MFA at all remote access points into the network to provide better security and thwart credential theft					
Use a least privilege model for providing remote access - and regularly review and remove user permissions that are no longer required					
Patch known vulnerabilities in all remote access and external facing devices and keep devices and infrastructure patched					

Mark the box that best fits your organisation's profile.

Ransomware Detection

Be able to quickly detect and respond to malware before it can launch and spread.

Action	Absence	Reactive	Managed	Proactive	Anticipatory
Centrally manage devices in order to only permit applications trusted by the organisation to run on devices					
Use a centralised patch management system to patch all endpoints as vulnerabilities are discovered - including mobile devices, operating systems, software, applications and cloud locations					
Deploy integrated endpoint protection and extended detection and response in order to pinpoint and track data breaches as they happen					
Use intent-based segmentation to segment network and infrastructure assets and prevent malware from moving laterally across your organisation					

Mark the box that best fits your organisation's profile.

Ransomware Recovery

Business continuity and disaster recovery are the most effective ways to recover from ransomware.

Action	Absence	Reactive	Managed	Proactive	Anticipatory
Backup virtual machines, cloud storage and operational systems based on Recovery Point Objectives					
Conduct regular backups of critical files and ensure they can easily be restored from backup - regularly test to ensure performance and data integrity					
Ensure Outlook, Exchange and SharePoint data is backed-up and can quickly be restored to ensure business continuity					
Keep data backups on separate devices and use offline storage where they can't be directly reached by infected devices					
Make sure your backups are immutable to protect against corruption or deletion					
Routinely test data and disaster recovery processes to ensure preparedness					

How Prepared Is Your Organisation?

Considering cybersecurity best practices, how well prepared is your organisation for ransomware?

Maturity Score	Maturity Level	Description	Overall Score
0	Absence	No evidence the action exists in the organisation	
1	Reactive	Basic action is in process, but cannot prevent problems from arising	
2	Managed	Action is deployed across the organisation with common responsibilities and language in place	
3	Proactive	Action is in place to proactively address current issues and challenges	
4	Anticipatory	Action is in place to proactively address future issues and challenges	

What steps do we need to take?

SPEAK TO AN EXPERT

Let our experts help you identify any gaps you need to address for enhanced ransomware protection and the right steps forward for your organisation. **Get in touch with us today.**

For more information on Optec, please visit optec.co.uk.