arcserve®

Protect what's priceless.

RANSOMWARE READINESS ASSESSMENT

A PROACTIVE APPROACH TO ADDRESS THE RANSOMWARE MENACE

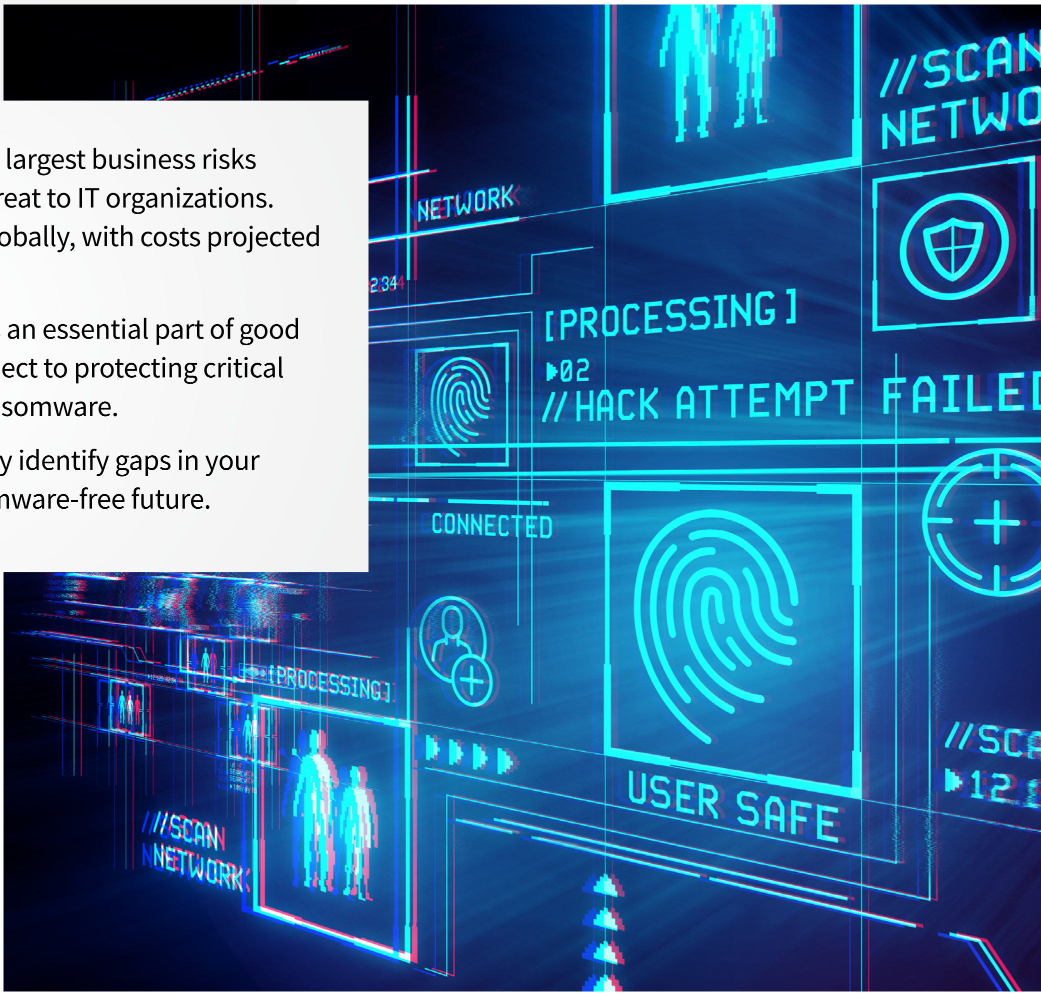
ASSESSMENT

MEASURE YOUR CAPABILITIES AND CHART A PATH TO A RANSOMWARE-FREE FUTURE

Ransomware has become one of the largest business risks and serves as the most menacing threat to IT organizations. It's reached epidemic proportions globally, with costs projected to reach $20 billion by 2021.[1]

Information security management is an essential part of good IT governance, particularly with respect to protecting critical business and personal data from ransomware.

This assessment can help you quickly identify gaps in your IT and chart your course for a ransomware-free future.



[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

RANSOMWARE-FREE CAPABILITY MATURITY SCORECARD

Instructions

To conduct the assessment using the **Capability Maturity Model**[2] (CMM) scorecard below. The scorecard describes a five-level evolutionary path of increasingly organized and systematically more mature processes. For each of the items in the ransomware-free framework, you can assess your organization's maturity score and consider your priorities.

Maturity Score	Maturity Level	Description
0	Absence	No evidence the action exists in the organization
1	Awareness	Limited understanding of the action, with informal processes and procedures in place
2	Repeatable	Basic action process is in place with some supporting documentation.
3	Standardized	The action process is deployed across the organization with common language, definitions, roles and responsibilities in place.
4	Managed	The action process is deployed across the organization with common language, definitions, roles and responsibilities and variations are managed across the organization based on business importance.
5	Operational	The action process is deployed across the organization with common language, definitions, roles and responsibilities and variations are managed across the organization based on business importance. Periodic reviews validate that performance metrics achieved.

[2] The Capability Maturity Model (CMM) was developed for the U.S. Department of Defense Software Engineering Institute (SEI) in 1986 located at Carnegie Mellon University in Pittsburgh, Pennsylvania.

Mark the box that best fits your company profile.

1 Actively manage access

Are we effectively managing access and controls across our systems portfolio?

ACTION	ABSENCE	AWARENESS	REPEATABLE	STANDARDIZED	MANAGED	OPERATIONAL
Restrict access to common ransomware entry points, such as personal email accounts and social networking websites and use web filtering at the gateway and endpoint to block phishing attempts for users who are tricked into clicking on a link.						
Use multi-factor authentication and advanced password standards and include password requirements when users communicate with websites that are uncategorized by the proxy or firewall.						
Use proxy servers and ad-blocking software and restrict permissions to install and run software applications.						
Vet and monitor third parties that have remote access to the organization’s network and your connections to third parties to ensure they are applying cybersecurity best practices.						
Use application whitelisting to allow only approved programs to run on a network.						

2 Manage systems configuration across attack vectors

Have we developed a centralized management and end-to-end approach that addresses the full range of potential attacks?

ACTION	ABSENCE	AWARENESS	REPEATABLE	STANDARDIZED	MANAGED	OPERATIONAL
Assess and categorize business sensitive data and implement physical and logical separation of servers, networks and data stores.						
Ensure antivirus and anti-malware solutions are enabled to automatically update and scan incoming and outgoing emails to detect phishing, prevent email spoofing and filter executable files.						
Use a centralized patch management system to patch all endpoints as vulnerabilities are discovered -including on mobile devices, operating systems, software, and applications, cloud locations and IoT.						
Deploy signatureless deep learning, anti-exploit and anti-ransomware technologies that detect both known and unknown malware.						
Deploy integrated endpoint protection and business continuity technologies to accelerate threat prevention and enable immediate data restoration.						
Secure web applications and web servers using web application firewalls.						
Disable scripts from emailed Microsoft Office files and consider using Office Viewer software to open Office files.						
Audit your network for systems using Remote Desktop Protocol, closing unused ports, using two-factor authentication.						
Detect and diagnose behaviors, such as mass file encryption, as malicious and block behavior.						
Use Unified Threat Management (UTM) appliances that combine firewall, gateway anti-virus, and intrusion detection and prevention capabilities to block access to known malicious IP addresses.						

3 Combine data security and data protection solutions

Does our IT configuration deliver comprehensive endpoint protection, data availability and cybersecurity?

ACTION	ABSENCE	AWARENESS	REPEATABLE	STANDARDIZED	MANAGED	OPERATIONAL
Protect backup repositories from malware, ransomware and zero-day attacks.						
Stop and remove threats such as malware and ransomware from backups.						
Keep data backups on separate devices and use offline storage where they can't be directly reached by infected devices.						
Backup virtual machines, cloud storage and operational systems based on Recovery Point Objectives (RPOs) - considering what amount of data loss is acceptable in the event of a failure.						
Use a system that allows multiple iterations of backups to be saved, in case a copy of the backups includes encrypted or infected files.						
Integrate appliances for disaster recovery and application availability and take advantage of artificial intelligence for endpoint protection.						
Use vulnerability scanning, SSL encryption, and other technical controls to confirm that backups are being performed.						
Use the 3-2-1 rule by creating three copies of your data, storing them on two different media, with one of them being stored off-site.						
Routinely test backups for data integrity and to ensure it is operational.						
Routinely test data and disaster recovery processes to ensure preparedness.						

4 Engage users with training and communications

Are we fully enabling our users with the practices they need to protect against ransomware threats?

ACTION	ABSENCE	AWARENESS	REPEATABLE	STANDARDIZED	MANAGED	OPERATIONAL
— Deliver regular awareness training and communications so everyone in your organization understands the threat of ransomware and is familiar with security techniques.						
— Establish security and ransomware prevention policies and procedures for end users.						
— Guide users to not open suspicious emails, click links or open attachments and to be cautious before visiting unknown websites and also to close their browser when not in use.						
— Ensure employees know where and how to report suspicious activity.						

5 Maintain and test a business continuity and disaster recovery plan

Are we capable of getting our applications and data recovered and operational in the event of a disaster?

ACTION	ABSENCE	AWARENESS	REPEATABLE	STANDARDIZED	MANAGED	OPERATIONAL
— Set up contingency and remediation plans which are crucial to business recovery and continuity - regardless of the source of the outage.						
— Conduct a risk assessment that classifies the types of disasters that can occur and establishes priorities for recovery and business continuity.						
— Deploy both onsite and offsite disaster recovery, backup, and high availability solutions.						
— Have an incident response plan that includes what to do during a ransomware event, including disconnecting the infected system from the network to prevent infection propagation, determining data sensitivity.						
— Test the plan – including technology systems and appliances – to ensure complete protection is delivered.						
— Report any infections to appropriate authorities.						

ASSESSMENT SUMMARY

Considering the five ransomware practices, how well prepared are we for a ransomware-free future?

Maturity Score	Maturity Level	Description	What is our overall level of maturity?
0	Absence	No evidence the action exists in the organization	
1	Awareness	Limited understanding of the action, with informal processes and procedures in place	
2	Repeatable	Basic action process is in place with some supporting documentation.	
3	Standardized	The action process is deployed across the organization with common language, definitions, roles and responsibilities in place.	
4	Managed	The action process is deployed across the organization with common language, definitions, roles and responsibilities and variations are managed across the organization based on business importance.	
5	Operational	The action process is deployed across the organization with common language, definitions, roles and responsibilities and variations are managed across the organization based on business importance. Periodic reviews validate that performance metrics achieved.	

What are our next steps?

TALK TO A RANSOMWARE EXPERT

Explore ransomware best practices and let our experts help you identify any gaps you need to address for a ransomware-free future. **Schedule a consultation.**

For more information on Arcserve, **please visit** arcserve.com