

CHECKLIST | RANSOMWARE PREVENTION BEST PRACTICES

Presented by Metro Insurance Services

Date:

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among private businesses, nonprofits, critical infrastructure organizations, and state, local and government entities.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. The monetary value of ransom demands has also increased, with some demands exceeding \$1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data and publicly naming and shaming victims as secondary forms of extortion. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. Throughout the initial disruption and, at times, extended recovery, the economic and reputational impacts of ransomware incidents have also proven challenging for organizations large and small.

Be Prepared		
1a.	It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important for backups to be maintained offline, as many ransomware variants attempt to find and delete any accessible backups. Keeping current, offline backups is critical because there is no need to pay a ransom for data that is readily accessible to your organization.	<input type="checkbox"/>
1b.	Maintain regularly updated “gold images” of critical systems in the event they need to be rebuilt. This entails maintaining image “templates” that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.	<input type="checkbox"/>
1c.	Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred. <ul style="list-style-type: none">• Note: Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.	<input type="checkbox"/>
1d.	In addition to system images, applicable source code or executables should be available (i.e., stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly. Having separate access to needed software will help in these cases.	<input type="checkbox"/>
2a.	Create, maintain and exercise a basic cyber incident response plan and an associated communications plan that includes response and notification procedures for a ransomware incident.	<input type="checkbox"/>
2b.	Review available incident response guidance.	<input type="checkbox"/>

Ransomware Infection Vector: Internet-facing Vulnerabilities and Misconfigurations		
1.	<p>Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.</p> <ul style="list-style-type: none"> Note: The Cybersecurity and Infrastructure Security Agency (CISA) offers a no-cost Vulnerability Scanning service and other no-cost assessments. 	<input type="checkbox"/>
2a.	Regularly patch and update software and OSs to the latest available versions.	<input type="checkbox"/>
2b.	Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins and document readers—for known vulnerabilities.	<input type="checkbox"/>
3.	Ensure devices are properly configured and security features are enabled. For example, disable ports and protocols that are not being used for a business purpose (e.g., Remote Desktop Protocol (RDP)—Transmission Control Protocol (TCP) Port 3389).	<input type="checkbox"/>
4a.	Employ best practices for the use of RDP and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services and later propagate ransomware. See CISA Alert AA20-073A, Enterprise VPN Security.	<input type="checkbox"/>
4b.	Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multifactor authentication (MFA) and log RDP login attempts.	<input type="checkbox"/>
5a.	Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the actions in 5b. and 5c. to protect their networks.	<input type="checkbox"/>
5b.	<p>Disable SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on the part of existing systems or applications) that may break when disabled.</p> <ul style="list-style-type: none"> Note: Remove dependencies through upgrades and reconfiguration. Upgrade to SMBv3 (or most current version), along with SMB signing. 	<input type="checkbox"/>
5c.	Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.	<input type="checkbox"/>

Ransomware Infection Vector: Phishing		
1.	Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.	<input type="checkbox"/>
2.	Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.	<input type="checkbox"/>
3.	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed sender policy framework and Domain Keys Identified Mail protocols,	<input type="checkbox"/>

	adding a reporting function that allows senders and receivers to improve and monitor the protection of the domain from fraudulent email.	
4.	Consider disabling macro scripts for Microsoft Office files transmitted via email. These macros can be used to deliver ransomware.	<input type="checkbox"/>

Ransomware Infection Vector: Precursor Malware Infection

1a.	Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions. CISA recommends using a centrally managed antivirus solution. This enables the detection of both “precursor” malware and ransomware.	<input type="checkbox"/>
1b.	A ransomware infection may be evidence of a previous, unresolved network compromise. For example, many ransomware infections result from existing malware infections, such as TrickBot, Dridex or Emotet.	<input type="checkbox"/>
1c.	In some cases, ransomware deployment is just the last step in a network compromise and is dropped as a way to obfuscate previous post-compromise activities.	<input type="checkbox"/>
2a.	Use application directory allowlisting on all assets to ensure that only authorized software can run and all unauthorized software is blocked from execution.	<input type="checkbox"/>
2b.	Enable application directory allowlisting through Microsoft Software Restriction Policy or AppLocker.	<input type="checkbox"/>
2c.	Use directory allowlisting rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from PROGRAMFILES, PROGRAMFILES(X86) and SYSTEM32. Disallow all other locations unless an exception is granted.	<input type="checkbox"/>
3.	Consider implementing an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.	<input type="checkbox"/>

Ransomware Infection Vector: Third Parties and Managed Service Providers

1a.	Take into consideration the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting client organizations.	<input type="checkbox"/>
1b.	If a third party or MSP is responsible for maintaining and securing your organization’s backups, ensure they follow the applicable best practices outlined above. Using contract language to formalize your security requirements is a best practice.	<input type="checkbox"/>
2a.	Understand that adversaries may exploit the trusted relationships your organization has with third parties and MSPs. See CISA’s APTs Targeting IT Service Provider Customers.	<input type="checkbox"/>
2b.	Adversaries may target MSPs with the goal of compromising MSP client organizations. They may use MSP network connections and access to client organizations as a key vector to propagate malware and ransomware.	<input type="checkbox"/>

2c.	Adversaries may spoof the identity of—or use compromised email accounts associated with—entities your organization has a trusted relationship with in order to phish your users, enabling network compromise and disclosure of information.	<input type="checkbox"/>
-----	---	--------------------------

General Best Practices and Hardening Guidance		
1a.	Employ MFA for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.	<input type="checkbox"/>
1b.	If you are using passwords, use strong passwords and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.	<input type="checkbox"/>
2a.	Apply the principle of least privilege to all systems and services so users only have the access they need to perform their jobs. Threat actors often seek out privileged accounts to leverage to help saturate networks with ransomware.	<input type="checkbox"/>
2b.	Restrict user permissions to install and run software applications.	<input type="checkbox"/>
2c.	Limit the ability of a local administrator account to log in from a local interactive session (e.g., “Deny access to this computer from the network”) and prevent access via an RDP session.	<input type="checkbox"/>
2d.	Remove unnecessary accounts and groups and restrict root access.	<input type="checkbox"/>
2e.	Control and limit local administration.	<input type="checkbox"/>
2f.	Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.	<input type="checkbox"/>
2g.	Audit user accounts regularly, particularly remote monitoring and management accounts that are publicly accessible. This includes audits of third-party access given to MSPs.	<input type="checkbox"/>
3.	Leverage best practices and enable security settings in association with cloud environments, such as Microsoft Office 365.	<input type="checkbox"/>
4a.	Develop and regularly update a comprehensive network diagram that describes systems and data flows within your organization’s network (see Figure 1). This is useful in a steady state and can help incident responders understand where to focus their efforts.	<input type="checkbox"/>
4b.	The diagram should include depictions of covered major networks, any specific IP addressing schemes and the general network topology (including network connections, interdependencies and access granted to third parties or MSPs).	<input type="checkbox"/>
5a.	Employ logical or physical means of network segmentation to separate various business units or departmental IT resources within your organization and to maintain separation between IT and operational technology. This will help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. See Figures 2 and 3 for depictions of a flat (unsegmented) network and a best practice segmented network.	<input type="checkbox"/>

5b.	Network segmentation can be rendered ineffective if it is breached through user error or nonadherence to organizational policies (e.g., connecting removable storage media or other devices to multiple segments).	<input type="checkbox"/>
6a.	Ensure your organization has a comprehensive asset management approach.	<input type="checkbox"/>
6b.	Understand and inventory your organization’s IT assets, both logical (e.g., data, software) and physical (e.g., hardware).	<input type="checkbox"/>
6c.	Understand which data or systems are most critical for health and safety, revenue generation, or other critical services, as well as any associated interdependencies (i.e., “critical asset or system list”). This will aid your organization in determining restoration priorities should an incident occur. Apply more comprehensive security controls or safeguards to critical assets. This requires organizationwide coordination.	<input type="checkbox"/>
6d.	Use the MS-ISAC Hardware and Software Asset Tracking Spreadsheet .	<input type="checkbox"/>
7a.	Restrict usage of PowerShell, using Group Policy, to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows OSs should be permitted to use PowerShell. Update PowerShell and enable enhanced logging. PowerShell is a cross-platform, command-line, shell and scripting language that is a component of Microsoft Windows. Threat actors use PowerShell to deploy ransomware and hide their malicious activities.	<input type="checkbox"/>
7b.	Update PowerShell instances to version 5.0 or later and uninstall all earlier PowerShell versions. Logs from PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities. <ul style="list-style-type: none"> • Note: PowerShell logs contain valuable data, including historical OS and registry interaction and possible tactics, techniques and procedures of a threat actor’s PowerShell use. 	<input type="checkbox"/>
7c.	Ensure PowerShell instances (use most current version) have module, script block and transcription logging enabled (enhanced logging). <ul style="list-style-type: none"> • Note: The two logs that record PowerShell activity are the “PowerShell” Windows Event Log and the “PowerShell Operational” Log. CISA recommends turning on these two Windows Event Logs with a retention period of 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs as large as possible. 	<input type="checkbox"/>
8a.	Secure domain controllers (DCs). Threat actors often target and use DCs as a staging point to spread ransomware network-wide. The following list contains high-level suggestions on how best to secure a DC: <ul style="list-style-type: none"> • Ensure that DCs are regularly patched. This includes the application of critical patches as soon as possible. • Ensure the most current version of the Windows Server OS is being used on DCs. Security features are better integrated into newer versions of Windows Server OSs, including Active Directory security features. Use Active Directory configuration guides, such as those available from Microsoft, when configuring available security features. • Ensure that no additional software or agents are installed on DCs, as these can be leveraged to run arbitrary code on the system. 	<input type="checkbox"/>

	<ul style="list-style-type: none"> • Access to DCs should be restricted to the administrators’ group. Users within this group should be limited and have separate accounts used for day-to-day operations with nonadministrative permissions. • DC host firewalls should be configured to prevent internet access. Usually, these systems do not have a valid need for direct internet access. Updated servers with internet connectivity can be used to pull necessary updates in lieu of allowing internet access for DCs. 	
8b.	<p>CISA recommends the following DC Group Policy settings (this is not an all-inclusive list, and further steps should be taken to secure DCs within the environment):</p> <ul style="list-style-type: none"> • The Kerberos default protocol is recommended for authentication, but if it is not used, enable NTLM auditing to ensure that only NTLMv2 responses are being sent across the network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible. • Enable additional protections for Local Security Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against the lsass.exe program to ensure an understanding of the programs that will be affected by the enabling of this protection. • Ensure that SMB signing is required between the hosts and the DCs to prevent the use of replay attacks on the network. SMB signing should be enforced throughout the entire domain as an added protection against these attacks elsewhere in the environment. 	<input type="checkbox"/>
8c.	<p>Retain and adequately secure logs from both network devices and local hosts. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred:</p> <ul style="list-style-type: none"> • Set up centralized log management using a security information and event management tool. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact on the organization as a whole. • Maintain and back up logs for critical systems for a minimum of one year, if possible. 	<input type="checkbox"/>
9.	<p>Baseline and analyze network activity over a period of months to determine behavioral patterns so that normal, legitimate activity can be more easily distinguished from anomalous network activity (e.g., normal versus anomalous account activity). Business transaction logging—such as logging activity related to specific or critical applications—is another useful source of information for behavioral analytics.</p>	<input type="checkbox"/>

Source: Cybersecurity and Infrastructure Security Agency (CISA)

APPENDIX

FIGURES

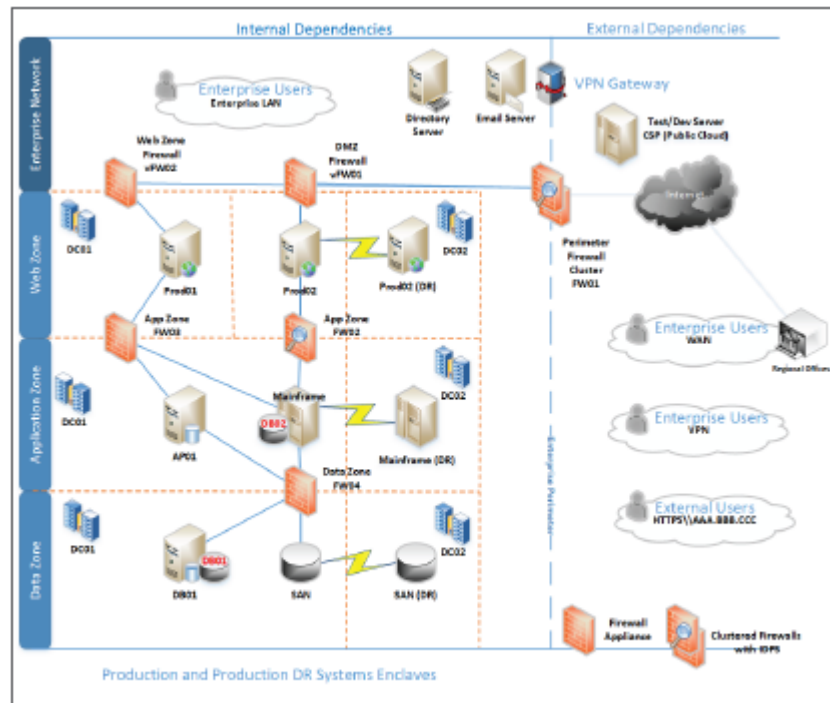


Figure 1. Example Network Diagram

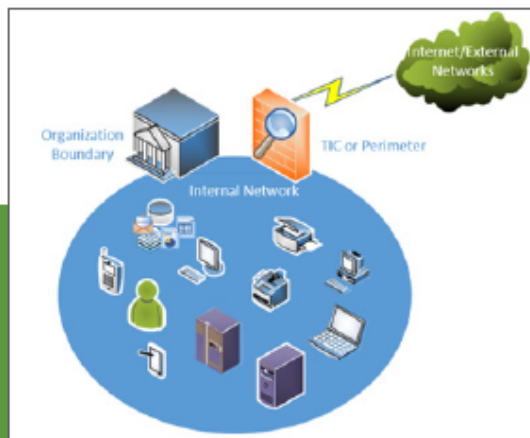


Figure 2. Flat (Unsegmented) Network



Figure 3. Segmented Network

CHECKLIST | RANSOMWARE RESPONSE

Presented by Metro Insurance Services

Date:

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among private businesses, nonprofits, critical infrastructure organizations, and state, local and government entities.

Should your organization become a victim of ransomware, the Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends responding by using the following checklist.

Detection and Analysis		
1a.	Determine which systems were impacted and immediately isolate them.	<input type="checkbox"/>
1b.	If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.	<input type="checkbox"/>
1c.	If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.	<input type="checkbox"/>
1d.	<p>After an initial compromise, malicious actors may monitor your organization’s activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.</p> <ul style="list-style-type: none">• Note: Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out only if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.	<input type="checkbox"/>
2.	Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.	<input type="checkbox"/>
3a.	Triage impacted systems for restoration and recovery.	<input type="checkbox"/>
3b.	<p>Identify and prioritize critical systems for restoration, and confirm the nature of data housed on impacted systems:</p> <ul style="list-style-type: none">• Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation or other critical services, as well as systems they depend on.• Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.	<input type="checkbox"/>

4.	Confer with your team to develop and document an initial understanding of what has occurred based on the initial analysis.	<input type="checkbox"/>
5a.	Engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to and recover from the incident.	<input type="checkbox"/>
5b.	Share the information you have at your disposal to receive the most timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders.	<input type="checkbox"/>
6a.	Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, collect any relevant logs and samples of any “precursor” malware binaries and associated observables or indicators of compromise (e.g., suspected command and control Internet Protocol (IP) addresses, suspicious registry entries or other relevant files detected). The contacts below may be able to assist you in performing these tasks.	<input type="checkbox"/>
6b.	Take care to preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).	<input type="checkbox"/>
7.	Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.	<input type="checkbox"/>
8a.	Research the trusted guidance (i.e., published by sources such as government, MS-ISAC, reputable security vendor, etc.) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.	<input type="checkbox"/>
8b.	Disable the execution of known ransomware binaries. This will minimize damage and impact to your systems. Delete other known associated registry values and files.	<input type="checkbox"/>
9.	Identify the systems and accounts involved in the initial breach. This can include email accounts.	<input type="checkbox"/>
10.	Based on the breach or compromise details determined above, contain any associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration. Securing the network and other information sources from continued credential-based unauthorized access may include disabling virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.	<input type="checkbox"/>
11.	<p>In the event you learn server-side data is being encrypted by an infected workstation, quick identification steps are to:</p> <ul style="list-style-type: none"> • Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files. • Review file properties of encrypted files or ransom notes to identify specific users who may be associated with file ownership. • Review the TerminalServices-RemoteConnectionManager event log to check for successful remote desktop protocol (RDP) network connections. • Review the Windows Security log, server message block (SMB) event logs and any related logs that may identify significant authentication or access events. • Run Wireshark on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., “smb2.filename contains cryptxxx”). 	<input type="checkbox"/>
12a.	Conduct an examination of existing organizational detection or prevention systems (e.g., antivirus, Endpoint Detection & Response, IDS, Intrusion Prevention System) and logs. Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.	<input type="checkbox"/>

12b.	<p>Look for evidence of precursor “dropper” malware. A ransomware event may be evidence of a previous, unresolved network compromise. Many ransomware infections are the result of existing malware infections such as TrickBot, Dridex or Emotet:</p> <ul style="list-style-type: none"> • Operators of these advanced malware variants will often sell access to a network. Malicious actors will sometimes use this access to exfiltrate data and then threaten to release the data publicly before ransoming the network in an attempt to further extort the victim and pressure them into paying. • Malicious actors often drop manually deployed ransomware variants on a network to obfuscate their post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromise. 	<input type="checkbox"/>
13a.	Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.	<input type="checkbox"/>
13b.	Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc.	<input type="checkbox"/>
13c.	Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use of PowerShell scripts).	<input type="checkbox"/>
13d.	Identification may involve the deployment of endpoint detection and response solutions, audits of local and domain accounts, examination of data found in centralized logging systems or deeper forensic analysis of specific systems once movement within the environment has been mapped out.	<input type="checkbox"/>
14.	Rebuild systems based on a prioritization of critical services (e.g., health and safety or revenue-generating services), using pre-configured standard images, if possible.	<input type="checkbox"/>
15.	Once the environment has been fully cleaned and rebuilt (including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms), issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility. This can include applying patches, upgrading software and taking other security precautions not previously taken.	<input type="checkbox"/>
16.	Based on established criteria, which may include taking the steps above or seeking outside assistance, the designated IT or IT security authority declares the ransomware incident over.	<input type="checkbox"/>
17a.	Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.	<input type="checkbox"/>
17b.	Take care not to reinfect clean systems during recovery. For example, if a new Virtual Local Area Network has been created for recovery purposes, ensure only clean systems are added to it.	<input type="checkbox"/>
18.	Document lessons learned from the incident and associated response activities to inform updates to—and refine—organizational policies, plans and procedures and guide future exercises of the same type of incident.	<input type="checkbox"/>
19.	Consider sharing lessons learned and relevant indicators of compromise with the CISA.	<input type="checkbox"/>

Source: Cybersecurity and Infrastructure Security Agency (CISA)

CHECKLIST | WEBSITE RISK EXPOSURE

Presented by Metro Insurance Services

Date:
For:

Review conducted by:
Phone #:

There are a wide variety of digital exposures and liability issues presented by websites. Use this checklist to help identify potential cyber liability coverage gaps and analyze e-commerce risk exposures.

ELECTRONIC LIABILITY: Your website could be putting you at additional risk. Do you have coverage for the following?	YES	NO	N/A
Defamation?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Theft of trade secrets?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Intellectual property?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Business interruption?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Media liability?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Product recall?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Breach of contract?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Breach of security (e.g., compromised customer credit cards or similar site damages)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Publishers liability (e.g., chat rooms or bulletin boards)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

SECURITY ISSUES: With identity theft on the rise, security is crucial. Do you have the following?	YES	NO	N/A
Do you have a procedure for collecting and using information? Who has access to it?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you properly authenticate credit card information?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you have a written privacy policy?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you transfer liability to a third-party vendor?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you create and let all staff know procedures for unauthorized access to a database?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you created a procedure for all staff to follow in regard to a cyberattack?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you instituted a written procedure for staff to follow regarding network security?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

DISCLOSURES, COPYRIGHT AND PRIVACY: These are often overlooked. Consider the following:	YES	NO	N/A
Does the site include written liabilities or disclaimers for errors or omissions in any material?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does it include your policy on requests for permission of use of materials and links?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does the site clearly state ownership and administrative rights of information and media?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does it state site and materials copyrighted?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does the site include term of use agreements?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

ONLINE PURCHASING: E-commerce can provide you with a revenue source without all the expenses of a building. Consider the following:	YES	NO	N/A
Is the product easy to order?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the site secure?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the site's security stated?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is there an acknowledgement of order email?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the return policy clearly stated?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does the site support the Better Business Bureau stamp of approval?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is there a product recall procedure in place?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

LINKS: Links can provide your users with quick and easy access to information, but they do need maintenance. Consider the following:	YES	NO	N/A
Are links checked on a regular basis for accuracy?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are the links relevant?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you include a description of the link?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you include the full URL for the links?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you provide a disclaimer advising the user they are leaving your site?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does the link pull up a new window, or is it framed in your site?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

MESSAGE AND VISUAL IMPACT: In addition to adding potential risks, a well-designed and visually appealing website can be an excellent marketing tool to draw in a client. How does your site stack up? Consider the following:			
	YES	NO	N/A
Is your domain name and message meaningful?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is your homepage attention-getting?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the text clear and concise? Avoid company specific “lingo” unfamiliar to outsiders.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are the graphics used appealing?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the site uncluttered?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does the homepage provide the basic business information, such as your full address, details on how to contact the company and product information?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is there a title for every page?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the site proofread?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the site updated on a regular basis?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is the site easy to navigate?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is there easy access to help?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you have a plan to manage website content to keep it up to date?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

IN THE EVENT OF A BREACH: Even after you’ve done all you can to mitigate the risks, a data breach can still happen. Is your business prepared to deal with one? Consider the following:			
	YES	NO	N/A
Have you notified your local law enforcement agency?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you have a plan for mitigating all of the risks of the breach, including when you will notify those affected?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Will you notify customers, banks, creditors and other affected businesses in a timely manner?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Have you checked the Federal Trade Commission guidelines and other federal and state laws for specific requirements regarding your type of business?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

For more risk management guidance, contact us today.