The CISO Checklist for Ransomware Preparedness

Executive summary

It is essential to ensure we are ready to recover our environments from a cyberattack at a moment's notice. In many cases, data protection has not been considered a strategic investment in the grand scheme of the IT landscape.

This paradigm has shifted in recent years. In today's climate, secure backup is your best line of defense against ransomware. That is why it is important to take the steps needed to protect data today, so it can be recovered tomorrow.

This CISO Checklist for Ransomware Preparedness is designed to help you begin to protect your environment by implementing high impact fixes that will yield results. There are many areas of data protection components and systems that are often overlooked.

At the end of the day, we know threat actors have one thing in mind, getting victims to pay the ransom. Threat actors will actively target data protection systems to attempt to render backups useless to make your environment unrecoverable. That is why it is so important to make sure secure practices are implemented not only throughout your whole IT environment, but specifically when it comes to your data protection environment.

By following the steps outlined in this Checklist, you will have taken a critical step to protect your data. It is important to remember there is not a single way to truly be safe from ransomware. Using this checklist along with ensuring all components of IT security are properly implemented and managed throughout your organization is a fantastic starting point. Remember, in the event of a ransomware attack, secure backup is your last line of defense.

In today's climate, ransomware is a guaranteed threat. According to Veeam's largest independent research reports, the Data Protection Report and the Ransomware Trends Report, 85% of organizations have admitted to having a substantial ransomware attack in 2022.

Components

Be sure to secure the components within your data protection environment.

☐ **Are systems hosting backup components patched and up to date?**	Unpatched vulnerabilities are the number one-way threat actors enter an environment. Ensuring operating systems are up to date helps protect components from attack or compromise.
☐ **Is the backup server separated from the production authentication domain?**	If the threat actor can compromise Active Directory they have the keys to the kingdom. Proper segmentation of assets will stop or slow down attackers.
☐ **Are all backup systems and components protected by MFA?**	Obtaining credentials is easy for threat actors. By ensuring all backup systems are components are protected by MFA, you reduce the risk of a threat actor accessing these systems, even after obtaining credentials.

Permissions

Good security practices like the principle of least privilege can go a long way in protecting your environment from cyberattacks.

☐ **Do you use different user accounts for day-to-day operation, and admin/configuration access?**	Separation of accounts ensures administrative accounts are only used to make configuration changes to components.
☐ **Is access to the backup systems, repositories and database restricted to only authorized users?**	All backup systems and components should be logged to audit who has access to the systems, when they access, and what activities they are carrying out.
☐ **Are passwords complex to current recommendations form standards bodies?**	Passwords should be at least 15 characters, include upper and lower case letters, numbers, and special characters to reduce the chance of being cracked.

Storage

One of the most important aspects to data protection is how you store your backup data.

☐ **Is the backup repository hardened and immutable?**	Hardened, immutable and encrypted repositories will protect data since immutable data cannot be deleted or modified.
☐ **Is the storage supporting the backup repository secured and isolated?**	External storage should also be properly secured and isolated, so it is difficult to perform an attack on backup data from the storage layer.
☐ **Do you have at least three copies of your data?**	Follow the 3-2-1-1-0 rule. Having at least three copies of your backup data ensures you can recover under any scenario. Copies should be distributed across different media types, and different locations.
☐ **Are you storing your backups on at least two different types of media?**	Storing backups on two types of media ensures that even if one type becomes corrupted or compromised, the other will remain unaffected. This is essential to ensuring you always have a copy of your backup data, no matter the scope of a disaster.
☐ **Do you have an air gapped copy of your data?**	Having a true air gapped copy of backup data means it is not connected to any external network or devices. Logical airgaps can still be accessed with stolen credentials.

Encryption

Encryption is key to protecting your data by limiting access to authorized systems and users.

☐ **Are private encryption keys stored securely?**	It is important to know where and how private keys are stored to ensure a bad actor can not decrypt your data.
☐ **Are backups encrypted?**	Encrypting backups can be a deterrent to threat actors. Backup data is not useful if it is exfiltrated and is less valuable.
☐ **Is all backup network traffic encrypted?**	When threat actors are inside an environment they will be able to capture network traffic. Having all traffic encrypted protect in-flight data.

Orchestrated recovery

When a cyber-attack happens, orchestrated recovery is important to ensure systems are back online quickly and functioning as expected.

☐ **Are you aware of the core applications that would allow business continuity after a blackout/service-loss event?**	To recover quickly from a cyberattack, you must know what applications are critical for the business to operate. These applications and their components then need different SLA's to ensure quick recovery times.
☐ **Is your disaster recovery orchestrated through automation?**	Recovery from cyber-attacks can be time intensive and prone to error when done manually. Orchestrated recovery through automation reduces the risk of error and speeds recovery.
☐ **Is there a regular testing regimen in place for recovery?**	Through regular testing, you will find the issues before they impact recovery. Once issues are fixed, regular testing is important to ensure nothing has been missed and to account for application and data changes.