8 cyber resilience best practices

Move confidently from planning to execution before the next attack.

Overview

While you may have a disaster recovery plan in place, recovering from destructive cyberattacks requires a different approach. The reason: You need to be able to respond fast, effectively investigate how the attack occurred, and mitigate threats in order to recover securely.

Follow these 8 best practices and you'll be on your way to true cyber resilience.

1. Be prepared

Your first order of business is to establish a cross-functional ransomware resilience team with all stakeholders. Ransomware incidents affect the whole organization, so it's critical that everyone knows their role during a cyberattack. Consider performing a realistic tabletop exercise with all stakeholders, creating an organization-wide ransomware policy (and keeping it updated), and defining your cyber backup and operational resilience strategies.

2. Be proactive

Understand ransomware operators and their Tools, Techniques, and Procedures (TTPs) through intelligence gathering in your industry or geography. Document and maintain contact information for all members of your response team, ideally through an out-of-band communications channel. Create a channel to report ransomware-like behavior. Assemble a cyber crisis response team and, if necessary, retain the services of an incident response organization.

3. Reduce the attack surface

Identify and patch critical asset vulnerabilities. Harden systems, prioritizing the critical systems and attack vectors ransomware gangs use. Ensure that credentials and access rights on all systems are managed along the lines of least privilege. Implement network segmentation to limit the spread of ransomware and increase the likelihood of detecting lateral movement. And identify poorly secured data repositories containing sensitive data within your organization.

4. Protect your backups

Ensure backup systems are sufficiently air gapped, have a separation of duties, and use immutable data stores that prevent them from being corrupted or deleted by adversaries. Use multifactor authentication (MFA) on backup administrator accounts and role-based access control (RBAC). Build and maintain Golden Masters of critical systems to speed rebuilding. And ensure your backup system can support the cybersecurity functions needed to respond to a ransomware incident.

5. Bolster your ransomware protection

Identify gaps in your existing preventative and detective control coverage against the ATT&CK Techniques used by ransomware gangs. Implement detection of endpoint filesystem anomalies that correspond to ransomware and wiper attacks, such as encryption or deletion of files. Implement email gateway filters to block emails with known malicious indicators. Use applications that allow listing/whitelisting on critical assets to ensure only authorized software can run.

6. Bolster your ransomware detection

Proactively hunt using historical data to find compromises. Implement a mechanism for unusual changes in CPU and disk utilization. Identify unusual network protocols, including I2P or TOR, which are known to be used by ransomware gangs. And identify network connections using known ports or destinations used in ransomware and wiper Command & Control.

7. Respond to the incident

Identify and group similar alerts related to impacted assets. Create an initial loss expectation (blast radius) of the incident. Find staging environments used for data exfiltration, and isolate infected hosts from both wired and wireless networks. Activate the clean room, restore the last backup of impacted systems, and redeploy trusted detection/response tools onto systems inside the clean room. Look for evidence of persistence and identify vulnerabilities in systems exploited in the attack.

8. Communicate

Communicate to internal stakeholders, to the press to help prevent damaging speculation, to impacted data subjects in compliance with regulatory and legal obligations—and to the regulators themselves. Inform your insurance company, law enforcement, and national/industry CERT.

For greater detail on each of these steps, read the white paper.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

9100083-001-EN 4-2025