

30-60-90 DAY

CYBER RECOVERY CHECKLIST

Implement a plan that leaves zero doubt about recovery.

Data fuels organizations, and when it comes to cyber recovery, a clear plan is paramount. IBM reported that it takes more than 73 days to contain a breach once it has been detected.¹ What would happen if a cybercriminal was successful at infiltrating your data and holding it hostage? By creating a cyber recovery checklist, you will be able to clearly identify the tools, solutions, and protocols to help you recover quickly at scale.

IBM reported that it takes more than
73 DAYS
to contain a breach once it has been detected.¹

Recover With Confidence

When it comes to cyber recovery, the consequence of failure is steep. This can often cause decision paralysis. Veritas has compiled extensive research to create this one stop shop of best practices to help you be cyber resilient.

For ease of implementation, we've divided the checklist into three sections. The foundation for your cyber recovery plan starts with day zero to 30. This initial phase includes tactics and solutions that are easy and quick to implement. The second phase, the next 30 days, emphasizes people, processes, and technology. This phase can take a few weeks to set up since it spans wider across the organization. The last phase, another 30 days, is all about refinements, rehearsals, and adjustments. The key to developing a quality cyber recovery plan is knowing where to start and how to prioritize.

PHASE
1

Phase 1: Establish the Foundation

Let's start with our foundational requirements — things that can be implemented within the first 30 days. The good news is, by recognizing your need for this cyber recovery checklist, you are well on your way to securing your data and enabling your organization for rapid recovery.



Create protection and retention policies for all workloads.

This starts with full data visibility. It is imperative to set up guardrails for each data set, including policies to identify mission critical data vs. daily data, what should be stored vs. archived, and for how long. This essential step provides you with a clear dashboard of your data lifecycle, locations, and sensitivity.



Use immutable storage.

Now that you have a clear data dashboard, you can accurately identify your most critical data and set that data up on immutable storage. This will prevent data alteration or deletion in the case of a cyberthreat, bringing you one step closer to cyber recovery with zero doubt.



Implement 3-2-1 backup strategy.

The 3-2-1 backup strategy indicates that you have three copies of your data on two different media with one copy off-site, or isolated. It is recommended that you use a virtual and/or physical air gap, as well as isolation for your SaaS data.



Apply security controls.

Security controls will help to create additional barriers to a cyberthreat impacting your data and infrastructure. A few key controls to implement include multi-factor authentication (MFA), network segmentation, role-based access control (RBAC), and encryption (both in transit and at rest).



Consider purpose-built hardened appliances.

Hardened appliances are amped up with top tier security measures and optimized to protect against malicious threats. These are purpose built to enable faster and more reliable recovery. This step is key to minimizing disruption in your environment in the case of a cyberattack.



Enable AI-powered anomaly detection.

Anomaly detection helps you identify unexpected events in your environment. The sooner you can recognize strange activity in your environment — such as unusual resource utilization — the faster you may be able to detect a cyberthreat. Add to that the speed and agility of AI, and you have everything you need to catch anomalies in your environment quickly and easily.



Turn on malware detection and retention rules.

Event-triggered malware scanning increases your opportunity to act before cybercriminals do. This step is as easy as toggling “malware detection” to ON. Retention rules are just as simple. Make sure to set up the necessary retention policies within your backup and recovery environment.



Update software and security patches.

When an update or a patch is available, don't delay. What may seem like a simple delay can be an invitation to cybercriminals. Patches and updates are released to help strengthen your defenses. Establish a plan for implementation and stick to it.

Phase 2: Proactively Manage Risk

You now have a foundation for understanding your data environment. It's time to focus on proactive risk management. This next phase — days 30 to 60 — is all about assessing people, processes, and technology. This will require coordination across business groups.



Identify “missing” critical assets.

It is important to first identify what data and applications are considered mission critical and prioritize the recovery and availability of those assets first.



Conduct dark data assessment.

Dark data — data with an undetermined business value — can pose a security and regulatory risk, as well as causing unnecessary storage costs. To perform this assessment, you need to identify and configure your target data, scan the data source, and generate a report that will be used to reduce risk and storage costs. Your dark data assessment should result in preventing security threats, optimizing your storage, and identifying personally identifiable information (PII) to reduce your regulatory risk.



Discover and classify sensitive data.

The lack of meaningful visibility into your data translates into uncertainty and risk. To eliminate this risk, it is critical to identify and understand the data within your organization. Once identified, classify that data based on its level of sensitivity or business criticality.



Identify and monitor high-risk end-user behavior.

High-risk end-user behavior can include employees who are likely to click on a phishing email, those who have had secure browsing incidents, or those who frequently share files between their work and personal accounts for “convenience.” It isn't always intentional when a user is high risk. In fact, often, the higher-level authorization or access a user has, the higher risk they pose to the organization. It is important to monitor these users and have an insider threat plan in place when something goes wrong.



Create an isolated recovery environment (IRE) or clean room.

An IRE enables air gap backup copies of important data to prevent the chances of it being compromised. Establishing an IRE gives administrators a clean set of files that they can recover on demand to neutralize the impact of a cyberattack.



Develop recovery runbooks, prioritizing order of operations.

Policies and procedures are only as good as their documentation and follow through. It is crucial to identify the plan for recovery, organize it by priority, and document it clearly.



Integrate with SecOps and establish incident response playbooks.

Integrating SecOps with cyber recovery solutions ensures that response strategies are both rapid and robust, minimizing potential damage. Integrating your cyber resilience tools with SIEM, SOAR, and XDR platforms is a key capability that allows you to recover quickly. SIEM systems aggregate and analyze log data across the network to identify anomalies. SOAR platforms automate the response to these anomalies, reducing the time from detection to resolution. XDR extends these capabilities, providing a unified security posture across various endpoints.

Phase 3: Refine, Rehearse, Adapt

The final phase of our checklist — days 60 to 90 — focuses on establishing policies and long-term strategies. Arguably the most important, this phase will set you up for planning, testing, validating, and refining your cyber recovery policies and procedures that have been defined throughout this checklist.



Adjust data protection policies to drive to 100% backup success, in accordance with SLAs.

Depending on your organization and industry, SLAs can vary. Fast and flexible recovery capabilities give IT administrators the ability to meet ambitious recovery time objectives (RTO), restore point objectives (RPO), and service-level agreements with ease.



Fine tune AI-powered anomaly detection.

Generative AI can be used to help reduce or all together eliminate anomaly detection from false negatives or false positives. This ensures a more accurate reading of your data and any cyberthreat lurking.



Run tabletop exercises.

Now it's time to see how your plan would hold up under pressure. Tabletop exercises allow you to test your plan in various scenarios to see how successful they are and adjust where necessary.



Rehearse recovery and validate results.

To be effective, this step should be ongoing. It is critical to set up an automated and assured rapid recovery testing process.

Cyber Recovery That Leaves You With Zero Doubt

It's too late to begin planning your cyber recovery after an incident occurs. The time to act is now! This checklist gives you everything you need to map out your cyber recovery plan with confidence and empower your team with greater visibility and control. [Learn more about establishing your cyber resiliency strategy with Veritas.](#)

1. [IBM 2023 Cost of a Data Breach Report](#)

About Veritas

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers—including 91% of the Fortune 100—rely on Veritas to help ensure the protection, recoverability and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems and 1,400+ storage targets through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on X at [@veritastechllc](https://twitter.com/veritastechllc).

VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact
information visit:
veritas.com/company/contact