rubrik

WHITE PAPER

How to Build Your Cyber Recovery Playbook

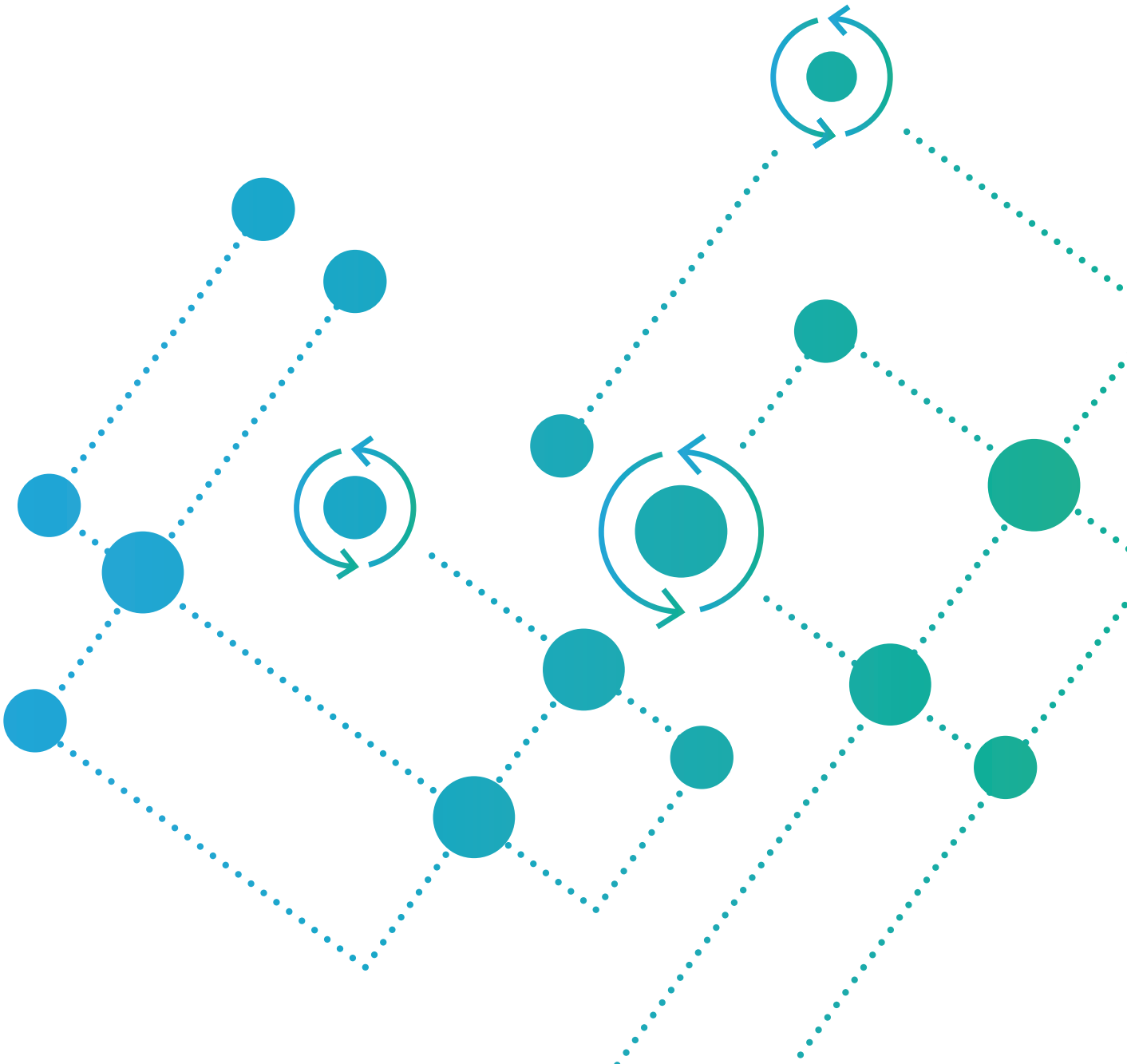

Table of Contents

WHY YOU NEED A GOOD CYBER RECOVERY PLAYBOOK

Cybercrime is a business, with individuals, gangs, and state-sponsored groups dedicated to launching multi-step, targeted campaigns. A recent report by Rubrik Zero Labs found that 53 percent of organizations experienced a material loss of sensitive information last year.[1]

Nearly every organization knows the importance of stopping cyberattacks. Yet, many still look at how to prevent and recover from them from a pretty narrow point of view. In reality, there's a much bigger picture to consider. An organization's planning and preparation phase needs to happen well before a cyberattack strikes. The next part—the attack itself—is what most of us think about, but it's just the middle of the story. The final part is the recovery, which can take days, weeks, or even months.

The more you focus on the front-end preparation, the better equipped you will be to recover from a cyberattack when it happens. This is why creating a cyber recovery playbook is so important. A cyber recovery playbook is a physical document that's part of your business continuity and disaster recovery (BCDR) plan. The playbook should outline the people involved in responding to a cyberattack, the policies and procedures they should follow, the resources they will need, and alternative courses of action they can take based on the nature of the attack.

> Note that the US Cybersecurity and Infrastructure Security Agency (CISA) has a wealth of available information, including a framework for response and recovery planning.

A good cyber recovery playbook can help your organization:

- Respond quickly and confidently in a crisis setting
- Recover data and restart applications faster to bring critical business operations back online
- Reduce costs related to business interruptions, remediation, and recovery
- Meet requirements from the board, executives, auditors, and cyber insurance providers for complete cyber recovery

This document is a framework for helping you develop your cyber recovery playbook. It suggests best practices in areas including preparation, staffing, stakeholder notification, attack containment, data recovery, remediation, and post-event analysis. Figure 1 summarizes the phases of the playbook and the activities that should be documented in it.

1 Rubrik Zero Labs. "The State of Data Security: The Journey to Secure an Uncertain Future." n.d. Rubrik. https://www.rubrik.com/zero-labs/2023-winter.

A NOTE ON BACKUPS

A lot of people think regular backups are their best bet for cyber recovery. The truth is that the legacy approaches to backups many organizations have used in the past aren't ironclad against today's sophisticated cyberattacks. While regular backups are still essential, there are two reasons why traditional backup strategies may fail to protect against cyberattacks.

Recovery takes time even with backups. Backups don't guarantee quick recovery. There are many backup options, from tape to disk to the cloud, but many of the operations involved in running those backups are time-consuming. It can also be difficult to determine exactly what data was affected during an attack and restore just that data. This means many organizations have to restore entire systems, datasets, or databases, which drags out recovery times.

Cybercriminals have developed ways of encrypting or corrupting online backups. According to Rubrik Zero Labs, 93 percent of organizations reported malicious actors attempting to impact data backups, and 73 percent saw attackers at least partially succeed.[2] If backups are compromised, then organizations attempting to use them to recover will realize too late in the game they may not be usable at all.

2 Rubrik Zero Labs. "The State of Data Security: The Hard Truths of Data Security." n.d. Rubrik. https://www.rubrik.com/zero-labs/2023-spring.

PHASE 0: PLANNING AND PREPARATION

Proper preparation prevents poor performance

The first step in developing your recovery playbook is assigning the right people to the planning and recovery team. It is also important to carve out enough time in their schedules to participate in all the research, analysis, and discussion required to develop an effective playbook.

A. CREATING THE PLANNING AND RECOVERY TEAM

The planning and recovery team is responsible for preventing and responding to attacks, and these folks will help define the steps in your recovery playbook. Some of the main contacts you should involve include:

- IT teams
- SecOps
- Risk assessment
- Human resources
- Legal
- CIO/CISO
- Business leadership
- First-line business managers
- Business continuity teams
- CEO

Bring all internal teams together to work through the planning stage. Tabletop exercises are one way to get everyone talking through potential problems in real time. Figure out what could happen during an attack and determine the best way to deal with it.

Make sure your team is clear about their roles and responsibilities, and give them space to communicate and collaborate. Work together to validate data, application, and line-of-business restorations and look for opportunities to ensure functionality.

Remember that your playbook is a living document, so be sure it's evolving as needs change. The document should be accessible offline and should be available to everyone in your planning and recovery team.

Similarly, have a way to contact everyone on the team if corporate communications go down. Keep an inventory of non-business email addresses along with phone numbers or other alternatives. Ideally, you should have an external group messaging system that meets end-to-end encryption requirements.

B. PERFORMING A BUSINESS IMPACT ASSESSMENT

As we will see in the Recovery section below, recovering from a sophisticated cyberattack can take several days. During that time, you'll want to prioritize getting your most critical applications back online first. Doing a business impact assessment will help you determine which business systems should be examined first, and if necessary, restored first, in the event of a cyberattack.

These assessments typically categorize applications in tiers based on factors such as:

- Criticality (i.e., the potential impact on your business value and the health and safety of customers, employees, and members of the public)
- Regulatory requirements and contractual obligations
- Impact on reputation and brand

Assessments usually categorize systems into three or four tiers and sometimes assign recovery goals or service-level agreements (SLAs) for each tier.

The highest priority applications—called "tier 0" and "tier 1" applications—include:

- Infrastructure services, such as DNS servers and enterprise directories needed to operate applications
- Applications that impact the health and safety of customers and employees
- Applications needed to meet regulatory requirements and contractual obligations
- Applications that have a major effect on the costs, revenue, and reputation of the organization

C. IDENTIFYING CRITICAL DATA TO PREVENT DATA EXFILTRATION

To limit the potential impact of data exfiltration, the planning and recovery team should identify critical data. By knowing where your critical data is, you can:

- Quickly determine whether or not an attack reached your sensitive data
- Better protect sensitive data in the first place by taking steps, such as limiting access, encrypting files, deploying additional security controls, backing up more frequently, and eliminating unnecessary duplicate copies of the sensitive data

All data is important, but some data is more important than others. During a cyberattack, it's crucial to know where that data is and if (and to what degree) it has been impacted. In the case of a ransomware attack, for example, many of the cybercrime syndicates have evolved their approaches to include "double extortion ransomware." In double extortion ransomware attacks, malware exfiltrates copies of victims' data before encrypting the original files.

The victims are then threatened with two negative outcomes: (1) losing their production data and (2) having sensitive information leaked on the web. That sensitive data can include product designs and other intellectual property, proprietary software, potentially embarrassing internal emails and documents, and the personally identifiable information (PII) of customers and employees, such as financial account and social security numbers.

Of course, by beefing up measures that protect your entire environment, such as expanding the use of multi-factor authentication (MFA), you increase the protection of all your data, including critical data. So, you'll want to make sure that your organization is up to date on the latest security best practices.

Note that activities to identify and better protect critical data should be ongoing. The location of sensitive information will migrate as applications evolve and organizations take advantage of public and private cloud platforms.

D. DOCUMENTING POLICIES

Take time before a crisis happens to document policies and research disclosure requirements. The planning and recovery team should compile and document regulatory, insurance, and corporate policies that need to be considered in responding to a cyberattack in advance. These include policies concerning:

- When and how much to involve your cyber insurance provider in the response (usually right away, and deeply)
- When and how to involve security forensics firms and outside technology vendors to help analyze and respond to an attack
- If and when to contact law enforcement agencies, such as the FBI, the US Cybersecurity and Infrastructure Security Agency (CISA), and similar authorities around the world
- If and when to disclose details to potentially affected parties, such as customers and business partners
- If and under what circumstances to pay ransoms

DON'T FORGET YOUR CYBER INSURANCE PROVIDER

For many organizations, their cyber insurance provider plays a major role in setting policies about how to respond to cyberattacks and, in the event of a ransomware attack, under what circumstances to pay ransoms. It is critical to get input from the insurance company either directly or through someone in the legal or governance, risk, and compliance (GRC) groups who have detailed knowledge of its practices and requirements.

E. PUTTING IN PLACE RESOURCES FOR BACKUP, RESPONSE, AND RECOVERY

When a cyberattack occurs, it's too late to improve your backup processes or buy and learn new tools to deal with the crisis. For the most part, you must work with the resources you have in place. Ideally, these include:

- Immutable data backups that were made before the attack (more on immutable backups in the last section of this paper)
- Tools for analyzing the extent and impact of attacks
- A secure recovery zone or facility for recovering data and restarting applications

Part of creating the recovery playbook is analyzing the requirements for the recovery zone. It needs to include hardware and networking equipment that is "clean" (newly purchased or wiped so there is no possibility of being compromised by malware). Your planning and recovery team can use the zone to recover data, reinstall applications, and begin running the most critical applications. The zone should be a section of the data center isolated from the compromised corporate network with equipment available on standby. An alternative is to contract with a public cloud provider to provide capacity on demand.

You should also consider arranging for a retainer with a reputable cybersecurity consulting firm that has experience analyzing and containing cyberattacks.

Other important parties to loop in include an infrastructure security vendor, which can help manage the threat, and individuals responsible for engaging other technology vendors. These include backup, hypervisor, network and routing platform, and physical systems vendors. Depending on your organization's size, you may need to have a single person or team responsible for aligning with and engaging outside vendors.

F. CREATING THE PLAYBOOK

The final, crucial step in the preparation process is to create a playbook for the team and supporting groups. The playbook describes the steps that need to be taken under a variety of circumstances and who is responsible for performing them. Since the playbook will be used in high-pressure situations, it needs to be clear and concise. Because cyberattacks can take different forms, the playbook can't be a cookbook with one recipe and should offer plans that cover a variety of likely contingencies.

The next sections of this paper will offer recommendations for four phases to include in the playbook.

Phase 1: Detection, alerting, and containment

Phase 2: Analysis and response

Phase 3: Recovery

Phase 4: Remediation

PHASE 1: DETECTION, ALERTING, AND CONTAINMENT

A. DETECTING ATTACKS EARLY (IF POSSIBLE)

Most cyberattacks are detected once they have interfered with business processes, resulting in a flood of calls to the help desk.

However, sometimes you may find clues pointing to a cyberattack in progress, such as communication with external IP addresses associated with threat actors or botnets or malware known to be used in cybercrime campaigns. When this happens, the cyber recovery playbook should include procedures to confirm the attack.

For example:

- Searching email filters and weblogs to uncover phishing campaigns and other methods used to plant malware and compromise systems
- Checking endpoints and antivirus products to find additional copies of the malware
- Finding compromised or altered credentials, particularly those for administering domains and directories, such as Active Directory
- Monitoring internal networks and network gateways to detect data exfiltration and command and control communications between the attackers and compromised systems

Identifying an attack early may help you contain it before it can inflict serious damage. Detection activities can also help identify what data, if any, has been affected, so you can recover only what you need instead of recovering entire systems.

B. ALERTING IT STAFF AND STAKEHOLDERS

The planning and recovery team is responsible for communicating their decisions regarding an attack to an extended team of stakeholders. The playbook should have detailed instructions about who needs to be notified immediately of a cyberattack, their contact information, the tasks they are expected to perform, and backup contacts in case the primary ones can't be reached.

The contact list should include:

- Members of the cyber recovery team
- Security operations, incident response, and IT operations staff members who will analyze and contain the attack
- System and network administrators and application developers who will be involved in recovering data and restarting applications
- Third parties, such as a cyber insurance provider, a security consulting firm, and the IT vendors whose products were involved in or compromised by the attack, that can help analyze the attack and outline alternative courses of action
- Business managers, application owners, and other internal stakeholders who may be affected by the attack and the related disruption in IT services
- Executives, members of the legal and public relations staff, and others who may need to notify customers, law enforcement and regulatory agencies, other third parties, and the public

C. CONTAINING THE ATTACK

Containing cyberattacks is important for two reasons. In the case of ransomware, the attackers often continue to extend their reach and encrypt new systems even after compromising an initial set of systems. Second, many of the steps involved in containment prevent attackers from coming back later and launching a new attack.

The playbook should outline steps for containing the attack, such as:

- Quarantining all compromised systems
- Locking compromised user accounts and changing their passwords
- Blocking inbound and outbound network traffic from external IP addresses associated with the attack
- Enforcing password changes for systems administrators and others with extensive privileges in case their credentials have been stolen
- Communicating with employees and other users of the organization's systems to stop opening emails, and if possible to log off and shut down their computers

D. RETAINING BACKUPS

Most organizations delete backups periodically. Note in your playbook that when a cyberattack is detected, system administrators should retain all existing backups and halt any lifecycle management of the backups in case they are needed for recovery.

Keep in mind that retaining more backups and keeping them from expiring will require more capacity, so forecast appropriately.

PHASE 2: ANALYSIS AND RESPONSE

A. INVOLVING THE CYBER INSURANCE PROVIDER AND SECURITY EXPERTS

Today, many medium-sized and large organizations dealing with a cyberattack work with their cyber insurance provider (if they have one) and an outside security consulting firm to analyze the attack, decide how to respond, and select an approach to recovering their data and restarting their applications. This is usually a good investment of time and money since these firms have experience and specialized expertise that few enterprises can match. Your playbook should include their contact information and instructions for getting them involved.

B. ANALYZING THE ATTACK

Whether you're working with your cyber insurance provider, an outside security consulting firm, or with internal resources, your playbook should explain how to collect information and analyze the technology and techniques used in the attack.

You should be able to answer questions like:

- What vulnerabilities did the attackers exploit?
- What methods did they use to gain an initial foothold in the network?
- Did they acquire additional credentials on the network, and how did they move to additional systems?
- What data, if any, have they exfiltrated from the network?
- What files have they encrypted?

A particularly valuable output of this analysis is the identification of the "blast radius" of the attack—that is, the systems that have been compromised and the files that have been encrypted or corrupted.

Replacing all of your systems and restoring all of your data is a massive job that can take days or weeks. It also causes unnecessary information loss because data that was not affected by the attack is rolled back to earlier versions. Focusing on a subset of the systems and files dramatically reduces the workload and shortens the time to full recovery.

Your business impact assessment (that you did as part of Phase 0 of this guide) can help you determine:

- The impact of the attack on critical business systems and areas of the business
- The cost of interrupted operations for shorter and longer periods
- The feasibility and likely timeframes for recovery based on different scenarios, such as restoring data from backups
- The risk to your reputation and revenue if exfiltrated data is disclosed

C. DETERMINING THE MOST RECENT USABLE BACKUPS AND HOW QUICKLY THEY CAN BE DEPLOYED

Having a backup process doesn't automatically mean that usable backups are available or can be obtained and deployed quickly. As mentioned earlier, cybercriminal groups have evolved ways to encrypt or corrupt backup files.

In your playbook, include instructions about determining how new your backups are, whether or not they have been corrupted, and how quickly they can be used to recover.

D. "SKIPPING" ACTIVITIES

Your playbook should explain how to "skip" or pause all activities related to data expiration and garbage collection. Any impacted data may have requirements placed upon its retention (for either business, forensics, or legal purposes) far beyond what is typical for the business.

The "skip" action ensures that expiration jobs and garbage collection and consolidation remain unscheduled by the cluster's job management and assignment framework (either as defined by the SLA, or even as administered via the admin UI/CLI).

E. DECIDING ON A RESPONSE TO RANSOM DEMANDS

In the case of a ransomware event, you will have to decide whether or not to pay the attacker's ransom.

The playbook should document whether your organization has a policy against paying ransoms under any circumstances. The official policy of the FBI is that victims should not respond to ransom demands, primarily because payments encourage additional ransomware attacks.[3] The US Treasury Department has warned that paying ransoms to individuals and entities on the government's Specially Designated Nationals and Blocked Persons List (SDN List) is a violation of federal laws, such as the Trading with the Enemy Act.[4]

You should also know that paying a ransom is no guarantee that you will get your data back. In 2022, 46 percent of organizations that paid a ransom recovered half or less of their data using attacker-provided decryption tools, and only 16 percent recovered all of their data, according to Rubrik Zero Labs.[1]

If you do pay the ransom, you may face different consequences or a combination of a few, like:

- The attacker disappears from the web and can't be contacted (which happened with the REvil ransomware gang in July 2021[5])
- The attacker walks away with the ransom and fails to send the decryption keys
- The attacker sends the decryption keys, but they don't work, or work very slowly
- The attacker sends a different encryption key for every one of hundreds of systems, and it takes days or weeks to decrypt the data in all of them
- The attacker maintains a foothold in the enterprise's network and repeats the attack at a later date

A cyber playbook can't anticipate all of the circumstances facing decision-makers, but preparing the playbook allows you to carefully consider alternatives and decide on policies in a calm atmosphere rather than in the pressure-cooker environment of an unfolding attack.

3 Federal Bureau of Investigation. 2021. "Ransomware." Federal Bureau of Investigation. 2021. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

4 "Ransomware Payments May Violate Sanctions Laws, U.S. Treasury Department Warns." n.d. The National Law Review. Accessed July 18, 2023. https://www.natlawreview.com/article/ransomware-payments-may-violate-sanctions-laws-us-treasury-department-warns.

5 Sanger, David E. 2021. "Russia's Most Aggressive Ransomware Group Disappeared. It's Unclear Who Made That Happen." The New York Times, July 13, 2021, sec. U.S. https://www.nytimes.com/2021/07/13/us/politics/russia-hacking-ransomware-revil.html.

PHASE 3: RECOVERY

A. ACTIVATING THE RECOVERY ZONE

You shouldn't try to recover data and restart applications in infrastructure that has been involved in a cyberattack. Instead, your playbook should advise working in a recovery zone with clean servers, a trusted network, and re-installed versions of software tools and applications.

The recovery zone should also have full backup facilities. Although applications will only reside there temporarily, for some time they will be generating live production data.

As mentioned earlier, many organizations set up a recovery zone with dedicated hardware and software on standby to be able to respond quickly to attacks and other threats to business continuity. You may choose that route, or you can also set up a virtual private cloud on a public cloud platform.

B. IDENTIFYING CRITICAL SERVICES AND APPLICATIONS AFFECTED BY THE ATTACK

The playbook developed during planning and preparation should describe what services and applications need to be covered first. See "Performing a business impact assessment" for help determining which applications you should prioritize.

Note in your playbook which applications are considered "tier 0" or "tier 1." These will include your most critical services that should be recovered first. However, note in your playbook that you do not have to restore all of these applications. Instead, assess the "blast radius" of the attack to determine which applications have actually been affected.

C. RESTORING DATA AND RESTARTING APPLICATIONS

Your playbook should instruct your cyber recovery team to recover the data for the tier 0 or tier 1 applications in the recovery zone, then restart those applications and the services that support them. When the applications have been tested, users can be given access to the applications running in the recovery zone and start using them.

Include instructions to use tools that allow selective recovery. With that feature, system administrators can recover only the files that have been encrypted or corrupted in the cyberattack, rather than all the files.

D. MOVING APPLICATIONS BACK TO THE PRODUCTION ENVIRONMENT

After the production environment has been cleaned and remediated (discussed in the next section), your playbook should instruct your system administrators to transition the critical services and applications from the recovery zone back into your production environment in the data center or on a cloud platform. When that is complete, they can restart the tier 2 and tier 3 applications in the production environment.

E. REGULARLY TEST YOUR RECOVERY PLAN

Because your playbook is a living document, you should be prepared to make necessary changes to ensure your organization is truly prepared to recover when an attack happens and meet your recovery SLAs.

Include information about how to pressure test your recovery plan and note how frequently those tests are carried out. Your playbook can also advise you to download and submit reports to your leadership, board of directors, and auditors about your recovery performance to prove the success of your plan.

PHASE 4: REMEDIATION

A. ERADICATING TRACES OF THE ATTACK

The IT security and IT operations groups need to work together to eradicate all traces of the attack, so the attacker cannot renew the attack later. That includes finding and removing malware and other malicious software used in the attack and resetting system configurations, parameters, and registry settings that the attackers changed.

A security consulting company or IT security forensics firm has the experience and tools to root out all of the traces left by the attackers. Include their contact information in your playbook, and involve them early on in the attack so they can step in when it's time to do this work.

B. DOCUMENTING THE INCIDENT AND THE RESPONSE

Threat actors often reuse the same tools and techniques over and over. Your playbook should instruct your cyber recovery team to record details of the attack and your organization's response to it, so your team members and colleagues can recognize renewed attacks and respond with proven tactics.

C. REMEDIATING VULNERABILITIES AND STRENGTHENING SECURITY

A successful cyberattack is evidence that an organization needs to strengthen its security. Analysis of the attack should pinpoint how the attacker exploited vulnerabilities and other security weaknesses to gain a foothold on the network, find critical data, and encrypt (and possibly also exfiltrate) those files.

In your playbook, note that you should use this analysis to remediate vulnerabilities and security issues and to identify controls and processes that will strengthen security and prevent a recurrence of the attack.

HOW RUBRIK CAN HELP

Rubrik is a cybersecurity company that supports many of the practices outlined in this paper. Rubrik Security Cloud is built on zero trust principles and delivers complete cyber resilience in a single platform across enterprise, cloud, and SaaS.

IDENTIFY AND PROTECT CRITICAL DATA

In this guide, Phase 0: Planning and Preparation highlighted the value of identifying critical data, so organizations can better protect it through measures like limiting access, encrypting files, deploying additional security controls, and backing up more frequently.

Rubrik Data Security Posture Management (DSPM) automatically discovers and classifies sensitive data; provides proactive data risk and threat alerts based on posture, user access, and activity; and automatically creates a heat map of high-risk assets.

As part of DSPM, Rubrik User Access provides visibility into unqualified access to sensitive data and helps organizations accelerate incident response with user context and without deploying external agents.

Rubrik also offers Sensitive Data Monitoring, which discovers and classifies sensitive data, such as personally identifiable information (PII). Sensitive Data Monitoring helps you discover what kind of sensitive data you have and where that data lives, so you can use those insights to better protect your data and reduce sensitive data exposure.

Finally, Rubrik SLA Domains help you consolidate data protection policies, providing a unified approach to manage data protection across various workloads and environments.

DETECT ATTACKS EARLY

Phase 1: Detection, Alerting, and Containment mentioned the fact that organizations can detect evidence of cyberattacks in their early stages by identifying unexpected changes to files.

Rubrik Anomaly Detection uses machine learning to establish normal baseline activities for each machine, then monitors the machines and flags behaviors that vary significantly from the baseline. These clues can enable you to react quickly and contain ransomware before it causes major damage.

Rubrik Threat Monitoring automatically identifies indicators of compromise (IOCs) within backup snapshots. Threat Monitoring proactively scans for threats out-of-band from production infrastructure based on vetted threat intelligence, accelerating investigation and reducing the risk of reinfection.

RESPONDING TO ATTACKS

Phase 2: Analysis and Response noted how important it is to know what was impacted during an attack, so you can recover just the data you need. The section also pointed out the importance of verifying that usable backups are available because cybercriminal groups have evolved ways to encrypt or corrupt backup files.

Rubrik Anomaly Detection and Threat Hunting are key in the analysis portion. Anomaly Detection helps you assess the blast radius of an attack and identify malicious activity, enabling incident responders to accelerate recovery time.

Threat Hunting analyzes backups to pinpoint clean uninfected snapshots to use for recovery. It also delivers insights from IOC scans to provide evidence during internal and external cyber investigations into security incidents.

Then, Rubrik Threat Containment isolates the infected snapshots to reduce the risk of reintroducing the malware into the environment during a recovery operation. You can download your quarantined data for offline analysis to understand the root cause, point of origin, and other details about the attack.

EXPEDITED RECOVERY

Phase 3: Recovery talks about prioritizing the most critical data and applications after an attack and the importance of treating your recovery plan like a living document, so you can continue to improve your process.

Rubrik Cyber Recovery helps you perform local or remote recoveries, bundling and prioritizing critical services into a recovery workflow. Those workflows automate and orchestrate recovery for an application or service so that organizations can get back on their feet faster.

Rubrik Cyber Recovery Simulation also gives you the ability to test, validate, and automate your recovery plan in an isolated environment. You can monitor your recovery progress, measure outcomes (like execution time), and check the status of validation scripts. You may also clone production data into isolated recovery environments to investigate snapshots for malware.

Finally, Rubrik simplifies the execution of your cyber recovery plan with Ruby AI, the generative AI companion for Rubrik Security Cloud. Ruby uses data points pulled from data security applications to provide proactive recommendations and guided task lists that help you respond immediately to a cyber incident.

MOVING FORWARD AFTER AN ATTACK

Phase 4: Remediation shares important steps organizations need to take after an attack, including ensuring all malware is eradicated, documenting the incident and response, and taking care of any vulnerabilities.

The findings from Rubrik Threat Hunting tell you what kind of malware was used in an attack, where the malware was sourced from, which group is known for using that malware, and which kinds of vulnerabilities that group targets.

Building your recovery playbook is a crucial step, but your cyber readiness comes down to having a strong foundation. You need a cyber resilience platform that helps you achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. For more information on how Rubrik can help you prepare for and recover from cyberattacks, visit www.rubrik.com.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

wp-how-to-build-your-cyber-recovery-playbook / 20240513