rubrik

WHITE PAPER

# Framework for a Comprehensive Ransomware Recovery Plan

How your organization can prepare for and quickly recover from a ransomware attack

August 2021

# TABLE OF CONTENTS

## WHY YOU NEED A GOOD RANSOMWARE RECOVERY PLAN

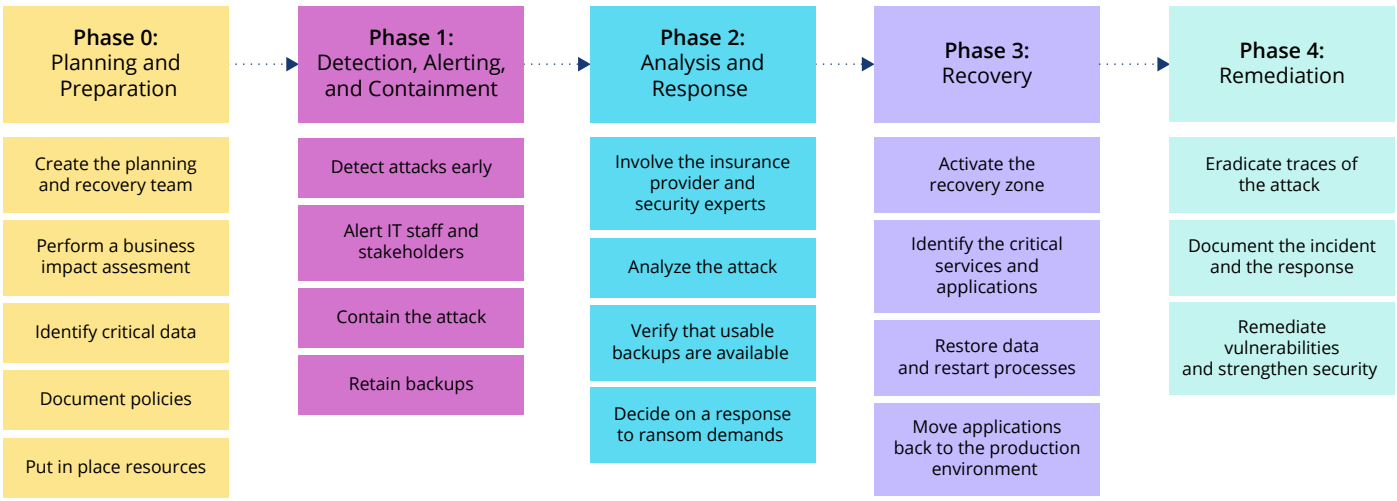
Ransomware attacks have evolved from crude efforts by small-time hackers into multi-step, targeted campaigns from sophisticated cybercriminal gangs and state-sponsored groups. Instead of merely encrypting data on a few disk drives, the new attacks often target infrastructure, encrypt backups, and exfiltrate sensitive information and threaten to disclose it to the world. Even after enterprises pay ransoms, it can take days or weeks to recover data, remediate security issues, and restart all operations. To complicate matters further, parts of the recovery process may be driven by regulatory requirements for disclosure, policies dictated by cybersecurity insurance providers, and business needs to prioritize mission-critical applications.

These complications, together with the ever-growing costs of ransomware attacks, make it imperative to develop a good ransomware recovery plan. Enterprises should create a detailed playbook that outlines the people involved in responding to a ransomware attack, the policies and procedures they should follow, the resources they will need, and alternative courses of action they can follow based on the nature of the attack.

A good ransomware recovery plan can help your organization:

- Respond quickly and confidently in a crisis setting
- Recover data and restart applications faster, starting with the most critical business operations
- Reduce costs related to business interruptions, remediation and recovery, and potentially ransom payments
- Meet requirements from the board, executives, auditors, and cybersecurity insurers for complete ransomware recovery and business continuity plans

This document lays out a framework for a comprehensive ransomware recovery plan. It suggests best practices in areas including preparation, staffing, stakeholder notification, containing the attack, data recovery, remediation, and learning from experience. Figure 1 summarizes the phases of the plan and the activities that should be documented in the playbook.



## DO REGULAR BACKUPS PROTECT AGAINST RANSOMWARE?

Not necessarily. A common misconception about ransomware is that "we are protected because we back up all of our data." Regular backups are essential, but they can lull organizations into a false sense of security. There are two reasons why traditional backup strategies may fail to protect against ransomware attacks.

**Cybercriminals have developed ways of encrypting or corrupting online backups.** An estimated two-thirds of ransomware attacks target backup systems. Often, when attackers gain a foothold on a network, one of their first actions is to start encrypting or corrupting backup data. Typically, this occurs two weeks or more before they begin encrypting production data. When enterprises realize they are under attack, they find weeks of their backups are unusable.

**Recovering backed-up data can take so long that organizations are forced to pay ransoms anyway.** Backing up data to tapes and storing them offsite used to provide a "gold standard' of data protection, but this is no longer the case. It can take several days to find the latest tapes, bring them back onsite, mount, and run them. Also, it is difficult to restore selectively from tape; you have to restore all files, not just the ones that were encrypted. Many enterprises cannot afford to wait for these operations to complete before restarting critical business systems.

## PHASE 0: PLANNING AND PREPARATION

### PROPER PREPARATION PREVENTS POOR PERFORMANCE

A ransomware recovery plan can be either a standalone document or a substantial section of a business continuity and disaster recovery (BCDR) plan. Either way, it is critical that the organization invest in developing a plan that will work under real-world conditions in a high-stress environment.

First and foremost, that calls for assigning the right people to the team. It is also important to carve out enough time in their schedules to participate in all the research, analysis, and discussion required to come up with an effective plan.

In addition, organizations need to consider actions that must be taken in advance, before a ransomware attack becomes visible. This includes educating people outside of the IT organization in how to recognize and thwart attacks (for example by reporting phishing emails) and in how to contain attacks when they are detected. It also involves putting in place resources that will be needed when the plan is implemented, such as a secure recovery zone (which will be discussed later in this section).

Finally, organizations should look at the planning process as a source of ideas for strengthening their security. The analysis and discussion that goes into creating the plan will identify actions that can prevent or reduce the impact of ransomware attacks, and data breaches as well.

Here are some of the activities that should be involved in creating the plan, and in preparing for ransomware attacks before they strike.

### A. CREATE THE PLANNING AND RECOVERY TEAM

The first step in developing a ransomware recovery plan is to assemble a ransomware (or business continuity) planning and recovery team that will create the plan and coordinate the response when an attack takes place. The size and composition of the team will vary according to the size and nature of the enterprise, but at a minimum it should include a core group with:

- **An executive sponsor,** ideally from a business unit that would be affected by ransomware, who can secure resources and cooperation within the enterprise and communicate with top management and outside parties in the event of an attack
- **A representative from IT security or security operations** with knowledge of ransomware attack methods and the security defenses in place
- **Representatives from the IT operations and networking teams** with knowledge of the computing environment and backup and recovery processes
- **Someone from the legal department or governance, risk, and compliance (GRC) group** with knowledge of compliance and cyber insurance issues

Depending on the circumstances, the complete team might also include:

- **Members of the incident response group** responsible for analyzing and containing attacks
- **Business managers** who can assess the priority of applications and business systems
- **Members of the IT operations and IT security teams** responsible for safely restoring data and applications
- **Members of the application development group** responsible for restarting applications
- **A representative from public relations or public affairs** responsible for managing public announcements and handling potential news coverage

## B. PERFORM A BUSINESS IMPACT ASSESSMENT

As we will see in the Recovery section below, regardless of whether an enterprise pays ransom or not, recovery from a sophisticated ransomware attack can take several days. Not all applications can be restarted at once. It is therefore very important to perform a business impact assessment. The assessment determines which business systems should be examined first to determine if they have been impacted by an attack, and if necessary, restored first. These assessments typically categorize applications in tiers, based on factors such as:

- Criticality (i.e., potential impact on the health and safety of customers, employees, and members of the public)
- Regulatory requirements and contractual obligations
- Higher costs and lost revenue
- Impact on reputation and brand

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

## C. IDENTIFY CRITICAL DATA TO PREVENT DATA EXFILTRATION

Unfortunately, many of the cybercrime syndicates involved in ransomware have upgraded their campaigns with "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: losing their production data, *and* having sensitive information leaked on the web such as personally identifiable information (PII) of customers and employees, financial account and social security numbers, product designs and other intellectual property, proprietary software, and potentially embarrassing internal emails and documents.

To limit the potential impact of double extortion ransomware, the ransomware recovery team should identify critical data so the organization can:

- In the event of an attack, quickly determine whether or not the ransomware attack reached the sensitive data
- Better protect the data in the first place by taking steps such as limiting access, encrypting files, deploying additional security controls, and backing up more frequently

If the organization can determine quickly that sensitive data was not, in fact, lost, then it may be able to limit regulatory fines and costs related to breach notification. And of course, reducing the amount of sensitive information exposed to ransomware reduces the time and effort needed for recovery.

Organizations should also consider measures that protect the entire environment, such as expanding the use of multi-factor authentication (MFA). Many ransomware campaigns use stolen or weak passwords or brute force password attacks to access target networks and systems. By thwarting those methods, MFA can limit the spread of ransomware.

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

## D. DOCUMENT POLICIES

The middle of a crisis is no time to begin researching disclosure requirements or starting to think about whether the organization is able or willing to pay ransoms. The team should compile and document in advance regulatory, insurance, and corporate policies that need to be considered in responding to a ransomware attack. These include policies concerning:

- When and how much to involve the enterprise's 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 U.S. 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 enterprises, their cyber insurance provider plays a major role in setting policies about how to respond to ransomware attacks and 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 GRC groups who has a detailed knowledge of its practices and requirements.

## E. PUT IN PLACE RESOURCES FOR BACKUP, RESPONSE, RECOVERY, AND RANSOM PAYMENTS

When a ransomware attack strikes, 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:

- Data backups that were made before the attack (or immutable backups, discussed 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
- A streamlined process for authorizing ransomware payments and a ready mechanism to purchase cryptocurrency for the payments (if necessary)

Part of creating the recovery plan 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) where the recovery team can recover data, reinstall applications, and begin supporting 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.

Organizations should also consider arranging for a retainer with a reputable cybersecurity consulting firm that has experience analyzing and containing ransomware attacks.

## F. CREATE A 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 ransomware attacks 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 look at the types of processes that can be described in the playbook, organized in four phases:

Phase 1: Detection, Alerting, and Containment

Phase 2: Analysis and Response

Phase 3: Recovery

Phase 4: Remediation

## PHASE 1: DETECTION, ALERTING, AND CONTAINMENT

### A. DETECT ATTACKS EARLY (IF POSSIBLE)

Most ransomware attacks are detected only in their final phase, after they have already encrypted data and interfered with business processing (resulting in a flood of calls to the help desk). In these cases, organizations need to move immediately to alert and contain the attacks.

However, sometimes organizations may find clues pointing to ransomware attacks in progress, such as suspicious emails, communication with external IP addresses associated with threat actors or botnets, or malware known to be used in ransomware campaigns. When this happens, the ransomware playbook should include procedures to ramp up detection. For example:

- Searching email filters and web logs to uncover phishing campaigns and other methods used to plant malware and compromise systems
- Checking endpoints and antivirus products to find additional copies of malware associated with ransomware
- Finding compromised or altered credentials, particularly those for administering domains and enterprise directories such as Active Directory
- Monitoring internal networks and network gateways to detect data exfiltration and command and control (C2) communications between the attackers and compromised systems

Positively identifying an attack early may enable an enterprise to contain it before it can inflict serious damage. Detection activities can also help identify what data, if any, has been exfiltrated, so the organization can assess the risks of data disclosure if the ransom is not paid.

### B. ALERT IT STAFF AND STAKEHOLDERS

The playbook should have detailed instructions about who needs to be notified immediately of a ransomware attack, their contact information, the tasks they are expected to perform, and backup contacts in case the primary ones can't be reached.

The contact lists should include:

- Members of the ransomware 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 that can help analyze the attack and outline alternative courses of action, such as the cyber insurance provider, a security consulting firm, and the IT vendors whose products were involved in or compromised by the attack
- 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 staffs, and others who may need to notify customers, law enforcement and regulatory agencies, other third parties, and the public.

## C. CONTAIN THE ATTACK

Containing ransomware attacks is important for two reasons. First, the attackers often continue to extend their reach and encrypt new systems even after encrypting an initial set of systems and declaring their presence. 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 (if they are not already using MFA), in case their credentials have been stolen
- Communicating with employees and other users of the enterprise's systems to stop opening emails, and if possible to log off and shut down their computers

## D. RETAIN BACKUPS

Most organizations delete backup files periodically. When a ransomware attack is detected, system administrators should retain all existing backup files in case they are needed for recovery.

## PHASE 2: ANALYSIS AND RESPONSE

### A. INVOLVE THE CYBER INSURANCE PROVIDER AND SECURITY EXPERTS

Today, many medium-sized and large organizations faced with a serious ransomware attack work with their cyber insurance provider (if they have one) and an outside security consulting firm to analyze the attack, decide how to respond to the ransom demand, 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.

### B. ANALYZE THE ATTACK

Before deciding on a response to the attackers and a recovery plan, it is essential to analyze and understand the ransomware attack, its impacts, and feasible courses of action.

The playbook should provide guidance on how to collect information and analyze the technology and techniques used in the attack. It should describe the steps to take so the organization can answer questions such as:

- 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 an organization's systems and restoring all of its 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. Enabling the organization to focus on a subset of the systems and files dramatically reduces the workload and shortens the time to full recovery.

The analysis can also draw on the business impact assessment performed earlier to 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 and paying the ransom and recovering data using decryption keys provided by the attacker
- The risk to the organization's reputation and revenue if exfiltrated data is disclosed

### C. DETERMINE THE MOST RECENT USABLE BACKUPS AND HOW QUICKLY THEY CAN BE OBTAINED AND DEPLOYED

The fact that an organization has 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. Sometimes recovery processes, especially those based on storing tapes at remote sites, are so slow that organizations can't afford to wait. Organizations should determine the state of their backups before deciding how to respond to ransom demands.

## D. DECIDE ON A RESPONSE TO THE RANSOM DEMANDS

The ransomware response plan should include policies and guidance on how to respond to ransom demands.

The first decision is whether the organization should have 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.[1] The U.S. 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[2].

However, law enforcement agencies and other government authorities have generally recognized that enterprises need to make decisions that ensure their survival and limit harm to customers and clients that depend on their goods and services.

In most cases, organizations need to weigh the costs and benefits of paying ransoms versus recovering their data from backups and restarting applications in a safe environment. But the factors leading to the decision are more complicated than most people realize.

Paying the ransom offers the possibility of receiving decryption keys from the attacker and resuming operations quickly, at relatively little cost beyond the ransom payment (especially if the ransom is covered by insurance). However, this happy conclusion is by no means assured. Other possible outcomes include:

- The attacker disappears from the web and can't be contacted (which happened to the REvil ransomware gang in July 2021)
- 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

Refusing to pay the ransom frees the enterprise from the onus of rewarding criminals, but the process of recovering data from backups and restarting applications can be problematic if:

- The recent data backups have been encrypted or corrupted
- A safe recovery zone needs to be assembled from scratch
- The organization can't determine the "blast radius" and must recover all of its data and restart all of its applications.

In addition, refusing to pay the ransom increases the chance that sensitive or proprietary information will be disclosed. This must be factored into the cost-benefit analysis for paying or not paying ransom.

Actually, there is a third option: pay the ransom *and* begin the process to recover data. However, this approach incurs both the cost of the ransomware payment and the effort and cost of recovering the data internally.

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

The playbook also ensures that regulatory requirements and enterprise policies are considered, and that key players such as the cyber insurance provider and outside security consulting firm are brought into the discussion

---

1 "The FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity." https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

2 Ransomware Payments May Violate Sanctions Laws, U.S. Treasury Department Warns: https://www.natlawreview.com/article/ransomware-payments-may-violate-sanctions-laws-us-treasury-department-warns

## PHASE 3: RECOVERY

Recovery scenarios will differ based on the nature and extent of the ransomware attack, and on the decision about whether or not to pay the ransom. In this section we assume that the organization has decided to restore the data from backups and restart applications.

### A. ACTIVATE THE RECOVERY ZONE

It is not a good idea for organizations to recover data and restart applications infrastructure that has been compromised by a ransomware attack. Instead, they should work 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 period of time they will be generating live production data.

As mentioned earlier, many enterprises set up a recovery zone with dedicated hardware and software on standby, to be able to respond quickly to ransomware attacks and other threats to business continuity. Organizations can also set up a virtual private cloud on a public cloud platform.

### B. IDENTIFY THE 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. These include infrastructure services such as DNS servers and enterprise directories needed to operate applications, together with applications that impact the health and safety of customers and employees, that are needed to meet regulatory requirements and contractual obligations, and that have a major effect on the costs, revenue, and reputation of the enterprise. These are usually the "Tier 0" and "Tier 1" services and applications determined by the business impact assessment discussed earlier.

However, it may not be necessary to restore all of the Tier 1 applications. Those outside of the "blast radius" of the attack do not need to be recovered.

### C. RESTORE THE DATA AND RESTART APPLICATIONS

The ransomware recovery team should recover the data for the Tier 0 and 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.

The recovery process will go much faster if the organization has data tools that allow selective recovery. With that feature, system administrators can recover only the files that have been encrypted or corrupted in the ransomware attack, rather than all the files.

### D. MOVE APPLICATIONS BACK TO THE PRODUCTION ENVIRONMENT

After the production environment has been cleaned and remediated (discussed in the next section), system administrators can transition the critical services and applications from the recovery zone back into the organization's 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.

## PHASE 4: REMEDIATION

When an attack has been contained and data recovered, it is not the time merely to sigh in relief. The next ransomware attack is already on the way. This is the critical time to capture knowledge about the attack, identify strengths and weaknesses in the response, and take steps to thwart similar attacks.

### A. ERADICATE TRACES OF THE ATTACK

The IT security and IT operations groups need to work together to eradicate all traces of the ransomware 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 were changed by the attackers.

This is one of the areas where it is a good idea to call in a security consulting company or IT security forensics firm that has the experience and tools to root out all of the traces left by the attackers.

### B. DOCUMENT THE INCIDENT AND THE RESPONSE

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

### C. REMEDIATE VULNERABILITIES AND STRENGTHEN SECURITY

A successful ransomware attack is evidence that the organization's security needs to be strengthened. 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. The organization 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, the Zero Trust Data Security Company™, offers an industry-leading backup and recovery platform that supports many of the practices outlined in this paper.

### IDENTIFY AND PROTECT CRITICAL DATA

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

Rubrik Sensitive Data Discovery discovers and classifies sensitive data, including personally identifiable information (PII). Sensitive Data Discovery scans backup data and reports sensitive data being stored, so organizations can make informed decisions about how to better protect that information.

### DETECT ATTACKS EARLY

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

Rubrik Ransomware Investigation uses machine learning to establish normal baseline activities for each machine, then monitors the machines and flags behaviors that vary significantly from the baseline, behaviors such as unusual file change rates, abnormal system sizes, and entropy changes. These clues can enable organizations to react quickly and contain ransomware before it causes major damage.

### IMMUTABLE BACKUPS

The discussion of *Phase 2: Analysis and Response* pointed out the importance of verifying that usable backups are available, because cybercriminal groups have evolved ways to encrypt or corrupt backup files.

Rubrik's backup and recovery solution features an architecture built on natively immutable backups; that is, backups that cannot be encrypted, corrupted, or tampered with by attackers. Immutability is enabled by a purpose-built file system that doesn't rely on insecure, standard protocols like SMB or NFS. External clients cannot discover or access backup files. The files themselves cannot be overwritten. These and other features of the solution ensure that backup files in their original form are always available in minutes to support analysis and data recovery.

### GRANULAR RECOVERY

The discussion of *Phase 3: Recovery* explains the advantage of recovering only the data that has been altered by the attack, rather than all data in the environment.

Rubrik Ransomware Investigation quickly identifies which applications and files were impacted by a ransomware attack and where they are located. This allows the ransomware recovery team to spend less time recovering files and to restart applications faster.

**For more information on how Rubrik can help you prepare for and recover from ransomware attacks, visit www.rubrik.com.**

## APPENDIX: KEY DECISIONS

### PHASE 0: PLANNING AND PREPARATION

- Who should be on the ransomware planning and recovery team?
- What applications and systems have the most impact on the business and need to be recovered first?
- Where is critical data located, and what should be done to make sure it is securely backed up and protected from exfiltration?
- What regulatory, insurance, and corporate policies need to be followed?
- What resources should be put in place in advance for backup, response, recovery, and ransom payments?
- What processes need to be described in the ransomware recovery playbook?

### PHASE 1: DETECTION, ALERTING, AND CONTAINMENT

- How can the organization detect attacks early and identify what data has been exfiltrated and encrypted?
- Who should be on the alert list for IT staff and stakeholders?
- What steps should be taken by the IT staff and employees to contain the attack and limit its spread?

### PHASE 2: ANALYSIS AND RESPONSE

- How should the organization engage the cyber insurance provider and security consultants to help analyze and respond to an attack?
- How should we analyze the attack to understand its methods and impact?
- Where are the most recent backups, and how quickly can they be obtained and deployed?
- How should we respond to the ransom demand, based on our policies and the costs and benefits of paying the ransom versus recovering data and restarting applications?

### PHASE 3: RECOVERY

- How should we recover data in our clean recovery zone?
- Which critical services and applications should we recover first?
- What is the best way to restore lost data and restart the applications?
- When can we move applications from the recovery zone back into the production environment?

### PHASE 4: REMEDIATION

- How can we eradicate traces of the ransomware attack so the attackers cannot relaunch it later?
- What should we document about the attack and response and what can we learn from them?
- What vulnerabilities and security weaknesses do we need to remediate so they can no longer be exploited by attackers?

rubrik

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

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



wp-framework-for-a-comprehensive-ransomware-recovery-plan / 20220826