LEARNING MADE EASY

Rubrik 2nd Special Edition

# Ransomware Recovery

for dummies®

A Wiley Brand

Detect ransomware early

Find out how to recover as fast as possible

10 tips for fighting ransomware

Compliments of

rubrik

Michael G. Solomon

# About Rubrik

Rubrik is a cybersecurity company with a mission to secure the world's data. Rubrik pioneered Zero Trust Data Security™ to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, delivers data protection and cyber resilience in a single platform across enterprise, cloud, and SaaS applications. The platform automates policy management of data and enforcement of data security through the entire data lifecycle. Rubrik helps organizations uphold data integrity, deliver data availability, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

# Ransomware Recovery

Rubrik 2nd Special Edition

**by Michael G. Solomon**

for dummies®
A Wiley Brand

## Ransomware Recovery For Dummies®, Rubrik 2nd Special Edition

Published by
**John Wiley & Sons, Inc.**
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

ISBN 978-1-394-18851-2 (pbk); ISBN 978-1-394-18865-9 (ebk)

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

## Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

**Development Editor:** Rebecca Senninger

**Acquisition Editor:** Traci Martin

**Editorial Manager:** Rev Mengle

**Business Development Representative:** William Hull

**Production Editor:** Mohammed Zafar

# Table of Contents

# Introduction

Welcome to *Ransomware Recovery For Dummies*, your guide to learning about ransomware attacks and how to recover from them. Malicious software, called malware, attacks have matured from being annoying to causing business process disruption and even data destruction. A type of malware that is growing in popularity is ransomware. Ransomware gets its name from its behavior. Ransomware encrypts critical files on a victim's computer and demands a ransom be paid for the decryption key. The attacker doesn't actually destroy any data but makes that data unavailable to the victim until the ransom is paid.

The classic advice to best recover from a ransomware attack is to completely restore an affected computer from the most recent backup image. While this approach may sound reasonable, it has its problems. More sophisticated ransomware seeks out backup images and encrypts them as well as the main data. Even if a good backup image is available, restoring a complete environment takes time and may overwrite many transactions. There has to be a better way.

An effective ransomware recovery plan must allow the affected organization to restore normal operations quickly with minimal data loss.

## About This Book

*Ransomware Recovery For Dummies* introduces a sensible approach to quickly recovering from ransomware attacks. By starting with the threat ransomware poses, you learn how to build a recovery plan that makes sense and keeps your organization safe.

After exploring the ransomware basics, you find out about the importance of a backup solutions provider and what features you need to address ransomware. You learn how to put the pieces of the ransomware recovery puzzle in place to develop an effective recovery plan. Finally, you review ten top tips for building the most effective ransomware recovery plan.

## Foolish Assumptions

I wrote this book based on certain assumptions about you, the reader. First, I assume that whether you're coming from the technical or business side of things, you've at least heard of ransomware. Regardless of your role, however, I assume you're interested in finding out more about the threat of ransomware and how to keep it from disrupting your organization's business operations. I also assume you want to know more about the steps you need to take to build a solid ransomware recovery plan.

## Icons Used in This Book

Every *For Dummies* book has small images, called icons, sprinkled throughout the margins. I use the following icons in this book:

TIP

This icon guides you to faster, easier ways to perform a task.

REMEMBER

This icon highlights concepts worth remembering and other important topics.

WARNING

If you see this icon, proceed with caution. Here you find advice on how to avoid the most common pitfalls.

## Beyond This Book

There's only so much about ransomware that can fit in this book. Innovative companies have studied the problem in depth and have come up with some interesting and effective solutions. Rubrik is a leader in providing ransomware detection and recovery services for organizations of every size. For more information about Rubrik's offerings, go to `www.rubrik.com/products/ransomware-investigation`.

IN THIS CHAPTER

- » Describing what ransomware is and its impact on IT
- » Exploring real ransomware attacks
- » Examining ransomware trends
- » Using layers to defend against attacks

# Chapter 1 Introducing the Problem of Ransomware

Ransomware is a type of malicious software (malware) that encrypts a victim's data and demands a ransom payment in exchange for the decryption. Ransomware is one of the fastest growing and most feared types of malware. A successful ransomware attack leaves its victims with the choice of losing valuable, sometimes irreplaceable, data or paying a ransom to get it back. As data becomes more valuable to both individuals and businesses, ransomware becomes a greater threat. In this chapter, you find out more about what ransomware is, how it impacts IT, and how you can reduce your risk of becoming a victim.

## Describing Ransomware and Its Impact on IT

Ransomware first gained notoriety as a threat to personal data. Most early ransomware attacks focused on individuals and leveraged their increasing reliance on personal data and media to extort them. The thought of losing personal pictures, videos, and documents provided enough pressure to convince some victims to pay the ransom. But with every ransom payment, attackers became increasingly emboldened and set their sights on larger targets.

## Exploring the problem of ransomware

Today ransomware is a real threat to individuals and businesses. About half of businesses have dealt with a ransomware attack within the last year, according to a report released by Rubrik Zero Labs in 2022. Additionally, in the report "The State of Ransomware 2022," cybersecurity company Sophos said that 46 percent of organizations that were hit with ransomware paid the ransom, and on average organizations that paid only got 61 percent of their data back. There is no indication that ransomware is going away anytime soon. Instead, ransomware tactics are becoming more focused and sophisticated.

Attackers have discovered that businesses and critical service providers are often more likely to pay large ransom amounts to end debilitating business interruptions than individuals. Most of today's organizations rely on data and information systems to carry out day-to-day operations. Denying access to critical data is on par with a natural disaster. But while many organizations have disaster recovery plans, most don't include a proper response to a permanent loss of critical operational data. So, it's important to understand how the ransomware threat is different from most other threats to avoid facing devastating disruptions to critical business functions.

## Understanding how ransomware affects IT

A common attitude about ransomware is to simply avoid becoming a victim. While that approach sounds good, it means that your organization would need to build a completely secure environment and no one could ever make a mistake. Ultimately, this approach is impossible to realize. Even organizations with the most advanced cybersecurity maturity routinely assess their environments for new or undiscovered vulnerabilities because they know a completely secure environment just doesn't exist.

REMEMBER

Even with the best security controls in place, people sometimes make mistakes and click things they shouldn't, introducing threats into the environment.

The real question is: "How can we recover if any of our preventative controls fail to stop a ransomware attack?" The answer is to implement plans to prevent, assess, *and* recover from ransomware attacks.

## Exploring Real-Life Ransomware Attacks

Before you learn the details of how to prepare for ransomware, take a look at two real organizations that faced ransomware attacks. One was caught by surprise, but the other had carefully planned for the possibility of an attack.

### The final straw for Lincoln

Lincoln College, a historically Black college located in the state of Illinois, had to close its doors after over 150 years. A ransomware attack kept key personnel from critical recruiting, retention, and fundraising for nearly three months. After paying a $100,000 ransom to the attackers and getting its data back, Lincoln College personnel were unable to make up the lost time and recruit enough students or raise enough money. The ransomware attack made recovering from COVID-19 and other challenges impossible and Lincoln College had to shut its doors.

WARNING

If you do receive a ransom demand, make every effort to resist paying. Each ransom paid increases the attackers' profits and keeps them in business. Paying a ransom can also mark you as an easy target for future attacks.

### Ransomware didn't change Payette's plans

One Saturday morning Payette's director of IT received the call that IT managers dread: The systems were down. Payette, an architectural firm, had over 40TB of plans, images, and other data in its IT environment. It turned out to be a ransomware attack. Payette's IT director knew that its network segmentation, backup processes, and careful recovery planning prepared its staff for just this type of attack. Instead of panicking, Payette's IT staff reacted to the early warning, stopped the attacks, recovered all the affected data, and were back online in less than 24 hours.

Planning and preparation allowed the organization to completely recover before the attackers even sent a ransom demand.

## Examining Ransomware Trends

Several trends in ransomware have emerged, and none of them is good. But despite these trends, it’s still possible to stay a few steps ahead of the attackers.

Here are some of the current trends in ransomware attacks:

- **Increasing ransom amounts.** Attackers are focusing their attacks on fewer targets but demanding much higher ransom payments.
- **Emerging commodity malware.** Cybercriminals don’t have to write their own malware to use ransomware. Ransomware as a Service (RaaS) vendors make it easy to become a ransomware attacker.
- **Targeting remote work and study situations.** Increased reliance on working and studying remotely, a shift accelerated by the response to COVID-19, led attackers to focus on collaboration and education providers. Although nearly all COVID-19 related restrictions have been relaxed or eliminated, remote work and study remains popular.
- **Exfiltrating data.** In addition to simply encrypting data, some attacks also steal copies of the data. That data can be sold for profit or leaked to cause reputational harm and trigger lawsuits or fines.
- **Taking a second pass at extortion.** Cybercriminals often also use exfiltrated data to extort additional funds from their victims. Typically, they promise not to release the data if the target pays them a specified amount of money.
- **Searching out and compromising backups.** Many current ransomware variants don’t stop at encrypting local data. They search for any connected data sources and attempt to encrypt all backup copies as well.
- **Continuing rapid growth.** Larger ransoms, ease of malware access, and better, more-targeted strategies have all encouraged more people to participate in cybercrime.

## Increasing Resiliency Using Layers of Defense

Defending against ransomware may seem like a daunting task given the scale and sophistication of these attacks. However, a well-thought out defense can prevent many types of ransomware attacks and help you recover quickly from any that may get through your perimeter defenses. A common strategy is to build multiple layers of defense, or what's known in cybersecurity as *defense in depth*. It basically means to put as many controls between your data and an attacker as possible.

Most people think of controls that prevent an attack as being the best controls. Preventing an attack is the best outcome, but you can't count on preventing every attack. If you don't plan for a successful attack, you won't be prepared if it happens.

Preventative controls are the first level of defense and include personnel training and firewalls. These measures aim to repel most attacks before they get a foothold. Most malware attacks, including ransomware, start with someone clicking a malicious link. Firewalls can help block obviously suspicious traffic, but an authorized user who clicks a malicious link is asking for trouble. So, it's important to train your personnel to recognize malicious messages and links.

Prevention is important, but humans are fallible. So, you also need to know what to do if ransomware evades your frontline defenses. If this happens, you need to know that your systems are being attacked. A strong detection layer will flag the threat and help you take action before it's too late. Today, monitoring and behavior analysis technology can alert you to an in-progress attack nearly instantaneously.

TIP

You should have real-time monitoring in place for all primary copies of critical data and added intelligence on your backup data to provide a last line of defense.

After you identify the threat, you need to stop the attack and assess the damage it did. You accomplish this by following procedures for disconnecting affected computers from your network and shutting them down. When you reboot them in a controlled environment you can evaluate the damage.

The next layer of defense depends on the cyber recovery solution you implemented. Once you identify the damaged files, you can retrieve images of the files from your backup, which will have a copy from before the attack started. Your cyber recovery solution should make it easy to quickly recover specific file images from a known point in time.

However, your backups will also be a prime target for sophisticated ransomware. The only backups you can trust are those with integrity guarantees. So finally, your cyber recovery solution must prevent any process, including ransomware, from changing any backup image once it's written to the file system.

If you implement all these layers of defense, you'll have the building blocks in place to defend against and quickly recover from cyber attacks.

IN THIS CHAPTER

- » Identifying ransomware vulnerabilities
- » Denying ransomware an opening to attack
- » Educating users on avoiding ransomware traps
- » Adopting best practices to avoid ransomware attacks

# Chapter 2 Preventing Ransomware Attacks

Surviving in the era of frequent malware attacks is only possible through a combination of avoiding most attacks and recovering from the rest. As we discussed in the last chapter, you must have a robust plan in place to handle successful attacks, but the best scenario is when you can avoid the attack altogether. To do that, you need to first understand the nature of the attack, then take measures to prevent the attack, and finally deal with any attacks that are successful. In this chapter, you find out how to implement measures to avoid ransomware attacks.

## Understanding Ransomware Vulnerabilities

Ransomware poses a serious problem, but it isn't an invincible type of malware. Understanding how ransomware works can help inform practices and controls that prevent most ransomware attacks from succeeding. In this section, you find out about some of the vulnerabilities that exist and how ransomware attackers carry out their plans.

## Examining how ransomware attacks computers

Ransomware depends on the ability to run a malicious program on a victim's computer. There are several ways to get a ransomware executable to a victim. The most popular methods involve tricking a user into opening a malicious link, navigating to a malicious website, or attaching an infected device. Each of these actions leads to downloading and executing a malicious program that starts the ransomware attack.

## Tricking a user into infecting a computer

By far the most common way for ransomware to infect a computer is for the user to take some action that runs the attacker's malicious code. While most users won't deliberately run malicious code on their computers, it isn't hard to trick users into innocently doing the attacker's dirty work. Convincing an authorized user to carry out an action for an unauthorized person is called social engineering.

Most people are vulnerable to social engineering because they want to be helpful, are interested in free stuff, and don't want to get into trouble. Attackers know that they can leverage one or more of these motivations. That's why many ransomware infections start with an unsuspecting user clicking a link on a website or in an email that either helps someone ("Click here to donate to a worthy charity"), satisfies their curiosity ("Click here to claim your cash"), or seemingly helps them avoid getting into trouble ("Click here to change your password").

## Using a shiny object to automatically infect computers

Ransomware doesn't always require a user to click a link. A drive-by download attack downloads malicious code when a user visits an infected website. Another type of attack consists of dropping infected USB keys at physical locations where people are likely to notice them. When someone inserts the USB key into their computer, the ransomware is copied and launches.

WARNING

Many types of attackers use the USB key trick or attractive downloadable files to plant malware. Don't blindly trust any device or file from any unknown source, especially those offered for free.

# Training Users to Avoid Becoming Victims

One of the best investments any organization can make to avoid ransomware is end user training. Users provide nearly all the entry points for successful ransomware attacks and play a vital role in stopping attacks before they start. Training users to recognize potential attacks and resist the temptation to click questionable links can result in a much lower probability of attack success.

Avoid focusing your end user security awareness training on only what users should and shouldn't do. In addition to specific acceptable use training, make it a point of your training to enlist users as security operatives. Security is everyone's responsibility, not just a small group of security specialists.

REMEMBER

Let all personnel know that good security is a team effort, and everyone needs to be diligent. One careless mistake can expose an entire organization to attack, so everyone must pitch in to defeat the attackers.

## Recognizing potential attacks

Because users provide a ransomware entry point so frequently, a sure way to reduce the attack potential is to teach users to be attentive and to recognize suspicious content. Show users examples of phishing emails, and provide guidelines on how to identify a potential attack.

Phishing emails are becoming more and more sophisticated, but most are easy to spot. Teach users to pay attention to grammar (does the message make sense?), salutations (are you addressed by name?), and specific content that can make malicious messages stick out (does the message contain details or is it generic?). Once users know what to look for, they can play a part in preventing attacks.

### Responding to suspicious content

Recognizing suspicious content is a good start, but users also need to know what to do next. Your organization should have a specific place to report suspicious email messages, other media, or behavior. For email messages, users should forward anything that looks odd to a designated email address. Your security personnel should monitor that email address, examine any reported messages, and explain to users whether the message was malicious and how they would be able to tell.

### Repeating the message

It would be great if security awareness training "stuck" forever, but unfortunately it doesn't happen that way. Users forget how important security is; they get busy with deadlines; and they get weary of always being diligent. One consistent characteristic of successful security awareness programs is their ongoing nature.

Instead of only offering security awareness training once, you should require recurrent periodic training. Also, mix up the delivery style. A monthly or quarterly "Lunch and Learn" series often works better than an annual half day session. The goal should be to keep reminding personnel of their role in security and how to best fill that role.

## Implementing Security Best Practices

Instead of trying to reinvent the wheel, a great place to start when building a security plan is with well-established best practices. Fortunately, many organizations have found some tried and true best practices to be helpful in preventing ransomware attacks. You won't find a single repository of best practices, so this section lists some of the most useful actions an organization can take to prevent ransomware attacks.

### Practicing safe user behavior

Once your personnel understand how ransomware works, they're more likely to accept guidelines for online behavior. Users can do (or avoid) many things to make the IT environment safer and less prone to ransomware attacks. Here are some ways users can stay safe:

- Verify email senders before opening a message.
- Don't open attachments unless they trust the sender.
- Don't open unexpected attachments.
- Don't follow links in email messages.
- Don't respond to suspicious looking messages.
- Forward any suspicious messages to their security group.
- Only visit websites they trust.
- Don't provide personal information unless they trust the website, the reason the data is needed, and only for interactions they initiated.
- Don't attach/insert/mount an external device (such as a USB key) unless they trust its source.
- Always use a virtual private network (VPN) when connecting from a remote location.
- Keep their software and operating system patched and up to date.

Following these best practices makes it difficult for any attacker to launch a successful ransomware attack.

## Hardening the IT environment

IT and security personnel also have best practices. Implementing the following best practices helps provide and maintain a more secure environment for your users.

- Identify all critical data.
- Create periodic backup copies of all critical data.
- Develop and test a comprehensive recovery plan.
- Update all computers and devices with the latest security patches.
- Require a VPN for all remote access.
- Require antivirus/antimalware software on all computers and devices.
- Implement malware scanning and filtering on mail servers.
- Implement firewalls with restrictive rulesets at each trust boundary.

- Conduct ongoing security awareness training for all personnel.
- Establish, publicize, and staff a support function to investigate reported suspicious messages or websites.

While no amount of prevention is 100 percent effective, every little bit helps. Every ransomware attack you prevent is one from which you don’t have to recover. The best strategy is to prevent every attack that you can, and prepare to recover from the rest.

**IN THIS CHAPTER**

- » **Building your recovery plan**
- » **Ensuring integrity for the last line of defense**
- » **Introducing immutability**
- » **Recovering from an attack**

# Chapter 3 Preparing to Defend Against Ransomware

Thriving through a ransomware attack is no accident. The only way to avoid becoming a ransomware victim is to plan for an attack and take steps to recover before the attack happens. In this chapter, you find out how to build a plan you can use if you find your company the target of ransomware.

## Developing a Recovery Plan

Recovering from a successful ransomware attack is very difficult, if not impossible, if you aren't prepared. But don't lose hope; knowing how to develop a good plan can make recovering from a ransomware attack much easier and faster than winging it.

### Assessing your needs

The first step in planning to survive a ransomware attack is to understand the data and processes that are most important to your organization. A Business Impact Assessment (BIA) is an important exercise in which you identify your most critical processes and the resources that support them. In short, what does your organization need to be able to do to stay in business?

After you know what your organization needs to carry out critical business functions, you'll have a good idea of what data is important to you. For example, an online retailer likely places a high value on its customer and product databases. A library of how-to videos may not be as critical to the retailer's day-to-day operations.

Attackers generally want to capture data that you value most. In other words, data required by your critical business functions. Chances are higher that you'll pay a ransom to get back the data you need to stay in business.

## Building a recovery plan

Once you understand what data is most critical to your organization (and the attackers), it's time to develop a plan to recover that data in the event of a successful ransomware attack. Your plan will provide *data resilience* (the ability to bounce back from a loss of critical primary data). You find out more about what to include in your plan in Chapters 4 and 5, but for now, start thinking about assembling a planning team and how you'll document the plan. You should include representatives from any group of individuals that can influence, or may be affected by, the recovery plan.

## Testing your plan

Once you build your ransomware recovery plan, you need to test it to make sure it works. The last thing you want to happen is to invest the time and effort into developing a plan to make your data resilient only to find out after an attack that a small but critical part was left out. A plan that doesn't work doesn't provide value (or the ability to recover).

You can carry out different types of tests, each one getting closer to a real attack, to make sure your plan will work. Most organizations start with checklist tests, where stakeholders review the plan together and ensure all tasks are addressed. A more comprehensive test is a simulation in which stakeholders carry out the actions they would do when faced with a real attack. The final type of test involves conducting an actual destructive attack in which files are altered to see whether the recovery team can restore them to a useful state. Of course, the last type of test carries risk, but it's also the best test for a recovery plan.

# Protecting the Last Line of Defense

Any ransomware that successfully encrypts files relies on the fact that the victim can't access a copy of the affected file. That means the attackers try very hard to find any backup copies of files and encrypt those too. Because most backup strategies follow a similar approach, it's relatively easy for attackers to find and infect most backup repositories.

Recovering files encrypted by ransomware is a three-step process: 1) Identify and stop the attack. 2) Define the scope of the damage. 3) Recover unencrypted (pristine) versions of the damaged files from a backup.

The third, and most critical, step depends entirely on the assurance that your backups have not been affected by the ransomware. That makes your choice of backup services crucial to recovering from a ransomware attack.

# Examining the Importance of Backup Immutability

A successful recovery plan centers on the ability to trust that your backups are pristine. If you can trust that ransomware hasn't altered your backed up files, you can recover from a ransomware attack.

## Defining immutability

In order for your data to be resilient your backups need to be immutable, meaning they can't be altered once they're written — not even by ransomware. If you have immutable backups, you have a perfect repository of pre-ransomware data that you can use for recovery.

### Enforcing immutability for backups

Immutability to support security goals is not a new idea. Logging systems have used immutability for years. Attackers learned long ago that an easy way to cover their tracks and destroy evidence of their crimes was to delete or alter log files. Security professionals quickly realized they needed logging strategies that would allow a service to write a log file entry, but never allow that entry to be changed.

One example of a cyber recovery company that offers immutable backups is Rubrik. Rubrik developed a unique filesystem from scratch that makes all the backup files it creates immutable. With Rubrik, you write backups using its application programming interface (API) call. Once they're written, they can't be altered. The filesystem immutability guarantees that you have pristine files you can use to recover quickly from a ransomware attack.

## Recovering Data

During a ransomware attack, you need to identify which files were affected before recovering them. While it's true that you could simply recover all files, doing so would dramatically drag out the recovery time. You need to minimize downtime to maintain business continuity. To do that, you want to focus on recovering only what's necessary to continue business operations.

You identified the data associated with your organization's critical business functions when you created your recovery plan. Now, you need to determine which of the critical files were encrypted.

WARNING

Most ransomware attackers provide decryption keys after receiving the ransom payment, but trusting a cybercriminal is always risky.

After you identify the files you want to recover, the next step is to carry out the recovery. We cover spotting threats, determining their damage, and performing a recovery in the next two chapters.

IN THIS CHAPTER

- **Identifying an attack as it's happening**
- **Alerting the right people to respond to an attack**
- **Assessing the extent of an attack's damage**

# Chapter 4

# Identifying a Ransomware Attack and Assessing the Blast Radius

Despite your best efforts to prevent every ransomware attack, a successful attack is still possible. In this chapter, you find out how to identify a ransomware attack and how to assess the extent of the damage.

## Finding an Attack Sooner Than Later

A ransomware attack succeeds by infecting one or more systems, finding critical files, and then encrypting them. Because it takes time to encrypt files, the earlier you detect and stop the attack, the fewer files you have to recover. To stop an attack early, you have to be able to observe your data. Data observability refers to the ability to monitor your data for risks, including indicators of compromise, so you can react quickly.

### Responding effectively depends on early warning

As with any type of attack, early detection gives you a better opportunity to contain the damage and recover faster. If you get involved early, the attacker can't do as much damage as they'd like, and you'll have less to clean up.

Early involvement in the recovery effort depends entirely on your ability to observe suspicious changes in your data. Recent ransomware attacks have decreased the time between the attack initiation and ransom request from more than a month to around three days (see `https://venturebeat.com/security/ransomware-3-days/`). That means the attackers are getting more efficient at their work.

### Reducing the recovery workload

Even if you detect an attack in just a few days, you could have a lot of work ahead of you. Every second is more time that cybercriminals have to encrypt files. An early warning and a quick response can dramatically reduce the number of files that need to be recovered, the scope of recovery work, and the amount of time until you're up and running again.

## Exploring Methods of Detecting Attacks

Ransomware software activities aren't the same as normal operations. While other applications do encrypt files, ransomware encrypts many files in a short period of time. Recognizing a ransomware attack depends on your organization's data observability capabilities and the extent to which they can recognize unusual behavior or changes to data. Your ability to monitor data and manage anomalies is crucial to responding to a ransomware attack. In this section, you find out about two approaches to detecting ransomware attacks.

### Recognizing ransomware signatures

One approach to ransomware detection is an extension of general malware detection. It isn't hard to detect known malware by comparing a portion of an executable program's code with a database of code signatures. If you find a match, you've probably found a malware program. Ransomware signature matching works in the same way. The main drawback to this approach is that you must keep your signature databases updated or any completely new or slightly modified ransomware will be missed. A new attack won't be detected until someone reports it and its signature gets added to the next release of the signature database.

WARNING

One of the disadvantages to signature matching is that ransomware is getting smarter and evolving rapidly, so there are new signatures all the time.

### Leveraging machine learning to recognize anomalies

Another approach to detecting malicious behavior is to use machine learning (ML) algorithms to compare normal behavior and file-system states to current behavior. ML algorithms are very good at learning what "normal" looks like and flagging any behavior or configuration that looks abnormal. ML algorithms can look at running processes and the resources they're using, as well as unusual changes to the filesystem.

Continuing with our previous example, Rubrik uses ML to analyze filesystem changes. Its Ransomware Monitoring & Investigation service looks at how the data is changing and how quickly those changes are taking place. It also scans for signs of encryption and file entropy changes.

TIP

Your first line of defense should be any of a number of real-time detection and monitoring tools to catch suspicious changes early.

## Responding to an Attack

Responding to any security incident, including a detected ransomware attack, should simply be a matter of following your response plan.

## Preparing the response team

You must assemble and train the members of your ransomware response team before they'll be ready to help your organization recover from an attack. The ransomware response team may be the same team that responds to other security incidents, but its members need to have special training for ransomware response.

## Containing the damage and identifying what files were affected

The first phase of recovery is to contain the attack and assess how much damage has already occurred.

## Stopping further damage

The response team should already have a good idea of which computers are participating in the attack by analyzing logs of network activity directed to the victim nodes. Their first action should be to stop the ransomware processes, generally by shutting down any affected computers.

After disconnecting affected computers and devices from all networks, you can start the process of removing the ransomware without spreading the damage to other nodes.

## Assessing the blast radius

The scope of the damage already done is often referred to as the blast radius. The blast radius is defined as the collection of files that have been modified in the attack. Most ransomware adds to or changes the filename extension as it encrypts each file, making identifying damaged files easier. Some ransomware builds a file containing metadata describing the files it has encrypted. Either way, you should be able to determine how big your blast radius is. Blast radius is related to attack time — the longer you wait, the more damage you have to clean up.

Assessing the blast radius prepares you for the next step — the recovery. If you have a solid, well-tested ransomware plan, recovery should be straightforward.

IN THIS CHAPTER

» **Developing a plan to meet your recovery goals**

» **Limiting the recovery process to only what you need**

» **Automating recovery for speed and reliability**

# Chapter 5
# Recovering Your Data with Surgical Precision

Once you've detected an attack, stopped the damage, and identified what files have been affected, it's time to trigger your recovery plan. A good recovery plan makes getting back to normal operations as quick and painless as possible. Precision and speed are essential to a fast and reliable recovery. In this chapter, you find out how to build, test, and follow a ransomware recovery plan that will get your organization back on track after a ransomware attack.

## Building a Rapid Recovery Plan

An effective ransomware recovery plan should give you the flexibility to recover files in a granular fashion, meaning that you can easily fetch clean copies of the files affected by the attack without having to restore all backed up files. Once you know which files you need to recover, you can execute the steps to recover those files.

### Backing up is only the first step

A good backup strategy is the foundation of ransomware recovery, but the plan doesn't stop there. The backups must also be immutable and easy to access. Your recovery plan must also outline detailed and simple procedures for recovering data as well as testing the plan itself.

TIP

Never trust an untested plan. Tests should be recurring and of different intensity levels, from simple readthroughs up to full failure recovery. The closer you move toward full failure testing the risk increases, so you must carefully evaluate how you test your recovery plan to avoid introducing excessive risk.

### Assessing recovery time drives recovery success

An important business requirement of any recovery plan is meeting the organization's recovery point objective (RPO) and recovery time objective (RTO). The RPO is the maximum amount of data your organization can afford to lose without seriously impacting critical business functions. RPO is measured in time. So, if the RPO is 24 hours, then the maximum amount of data that can be lost is the amount that was created 24 hours before an attack or failure. The RTO is the maximum amount of time it should take to restore normal operations after an attack or failure.

Your recovery plan must detail how to restore the organization to its RPO within the RTO. If the recovery process takes longer than the RTO, your business processes will suffer.

## Recovering Only What Is Necessary

Many ransomware recovery plans are based on restoring entire computers. Whether you use virtualization and checkpoints or a full backup image to restore a computer, you're painting with a very wide brush. A good threat remediation plan is more selective. A ransomware attack doesn't encrypt every file so you shouldn't restore every file to recover. In this section, you find a better way to avoid extra work and save time.

## Focusing on only what you need

A heavy-handed approach to ransomware attack recovery could add additional damage to the attack. People routinely make updates and changes to data through the course of normal day-to-day business functions. Many of these changes are coordinated across multiple files, databases, or even computers. If you're hit with a ransomware attack and do a wholesale restore, then you'll lose all the updates that were made to that data since the backup was written — even if that data wasn't affected by the ransomware attack. This can cause you to get out of sync with other systems or lose important information, such as transaction data.

For example, suppose your organization sells pet supplies online. A ransomware attack starts encrypting Microsoft Word and Adobe Acrobat documents on your order processing server. You detect the attack after several hours and follow an old ransomware recovery procedure. The outdated procedure directed the incident response team to shut down the computer and restore everything to a point in time before the attack. Instead of just recovering the affected files, you eliminate all orders that were taken since the attack started and orphan all orders that have already been sent to your shipping department. Your billing department is unhappy because of the mess your "recovery" has created.

TIP

A far better approach would be to incorporate a multi-layered service, such as Rubrik Data Remediation, into your recovery plan to make it easy to recover only what you need.

In addition to avoiding a recovery operation that overwrites too much data, recovering only what you need is faster, especially if your backup solution provider exposes APIs that you can use.

# Automating Recovery at Scale

The final step to a smooth ransomware recovery process is the ability to automate repetitive and redundant actions. If you have 10,000 files that an attack encrypted, automating the restore process for all those files makes the process faster and more dependable. In this section, you find out about practical strategies for fast and effective file restoration through automation.

## Implementing APIs for unattended recovery

An effective way to quickly access and retrieve files from an immutable backup file system is by using APIs. APIs can provide secure access to files on demand and through a variety of host languages. With flexible APIs, you can write software to access your files in your favorite language. The beauty of using effective APIs is that they let you bypass an inflexible user interface to directly access your data. It's your data. You should be able to access it however you want. Flexible and secure APIs help you do that.

## Scripting for high performance

Although APIs are often used to provide direct access to individual files, embedding those APIs in scripts can result in high-performance access to multiple files. APIs for data access called from within scripts provide the icing on the cake for ransomware recovery. Once you identify a list of files the ransomware attack encrypted, you can write a script in your favorite scripting language to carry out the restore. For each file in your list, all you need to do is query your backup data using an API to find the last backup version before the attack, and then call another API to restore it. Your scripts, supported by your cyber recovery solution's APIs, will restore your organization to an operational status quickly and efficiently.

A good cyber recovery solution, such as Rubrik, the example we've used throughout this book, will offer effective APIs that support the ability to easily access and restore specific files quickly and at scale.

Chapter 6

# Ten Tips to Handling Ransomware Attacks

After learning about ransomware, it may seem that surviving an attack is a daunting task. However, once you understand the attacks, how to avoid them, and how to recover from them, planning to confront ransomware can be a straightforward project. This list gives you ten tips to putting a plan together to thrive in the face of a ransomware attack.

- **Train users to avoid ransomware attacks.** Train all users on how to recognize common ransomware attacks and how to avoid becoming a victim. Provide a method for users to report suspicious messages or websites and train them to use it.
- **Turn on mail server filtering.** Today's mail servers either include options or support add-ons to filter mail messages and attachments for suspicious content. Research how to enable this feature for your mail server and use it.
- **Identify critical data.** Take inventory of your organization's critical business functions and the data each one needs to operate. Create a manifest of data that's critical to your organization's operations. This list of data should be the focus of your protection and recovery efforts.
- **Choose the right backup service provider.** Choose a backup service provider that can guarantee immutable

backups and easy access to unencrypted data through flexible but secure APIs. Both of these features are integral to Rubrik Security Cloud's design.

- **Back up data to an immutable destination.** Frequently back up all the data on your manifest to a backup service provider that guarantees immutability to ensure ransomware can't encrypt your backups.
- **Develop a recovery plan.** While backing up critical data is a great first step, you also need to develop a formal plan for recovering data. Document the conditions under which you should recover, who will carry out the recovery operations, how to identify what to recover, and how to recover identified data.
- **Train and deploy an incident response team.** Assemble a team of personnel with the express purpose of responding to a suspected ransomware attack. The team should be fully versed in the recovery plan and comfortable with their clearly defined roles. Ensure each team member participates in frequent tests to keep everyone ready to respond whenever the demand arises.
- **Create automation templates for quick recovery.** When you need to activate your plan, all you should need to provide is a list of data to recover. That means your plan should include script templates to carry out the recovery process for just the data you need to recover. Script templates give you the ability to test the recovery process many times and fine-tune it.
- **Test your plan frequently.** In addition to testing individual scripts, it's important to test the entire recovery plan frequently. The only valid plan is one that meets your RPO and RTO requirements. Ensure all participating personnel are comfortable with their roles and the plan flow. Frequent tests validate the plan's effectiveness in changing environments and keeps personnel fresh and ready to go.
- **Monitor data for suspicious changes.** Implement file integrity monitoring on production filesystems to detect suspicious changes, such as those consistent with ransomware. You should also implement monitoring for backup locations. Any unauthorized backup changes or unusual changes to previously backed up data should be noted. Ensure your backup service provider delivers alerts for suspicious changes.

# Recover faster from ransomware

Businesses run on data. Cybercriminals know this and have gotten increasingly better at penetrating traditional infrastructure and perimeter security, encrypting critical data, and holding it for ransom. Ransomware has become a real threat. But you can learn to fight it using the guidance in this book. *Ransomware Recovery For Dummies* will teach you how ransomware works, how to prepare for it, and how to recover from it quickly.

## Inside…

- Explore real-life ransomware attacks
- Learn best practices to avoid ransomware
- Find out how to build an iron-clad recovery plan
- Discover how to get back to business as quickly as possible

rubrik

**Michael G. Solomon, PhD,** is a cybersecurity consultant who provides executive level guidance to help clients align compliance requirements with strategic goals. Dr. Solomon is a Professor at the University of the Cumberlands and holds a PhD in Computer Science and Informatics from Emory University

ISBN: 978-1-394-18851-2
Not For Resale

9 781394 188512

for dummies®
A Wiley Brand

# WILEY END USER LICENSE AGREEMENT