proofpoint.

E-BOOK

The 2021 Ransomware Survival Guide

What Every Organization Needs to Know Before, During and After an Attack

proofpoint.com

Table of Contents

Executive Summary

Ransomware is an old threat that persists as a modern-day problem. This type of malware—which gets its name from the payment it demands after locking away victims' files— is a major issue for any organization that relies on IT.[1] It's one of today's most disruptive types of cyber attacks, putting victims out of business[2], forcing hospitals to turn away patients,[3] and bringing entire city governments to a standstill.[4]

Despite a sharp decline in the overall volume of ransomware attempts from historical peaks,[5] the number of organizations experiencing ransomware attacks increased by 15% over one year and have more than tripled in frequency over two years, according to the Ponemon Institute.[6]

Aside from the ransom itself (assuming victims pay), these attacks can exact a heavy toll: business disruption, remediation costs and a diminished brand.[7]

Aside from the ransom itself (assuming victims pay), these attacks can exact a heavy toll: business disruption, remediation costs and a diminished brand.

Why Ransomware is Still Around

Ransomware has persisted because of four primary drivers:

- Ransoms are easier to collect than in other types of fraud, thanks to Bitcoin and other digital currency
- Attackers have many distribution channels—including existing compromises of an environment—boosting the chances of success
- A large pool of targets relies heavily on IT but have weak or outdated cyber defenses and poor backup and recovery routines
- Attackers are getting better at targeting and more sophisticated in their tactics

[1] Verizon. "2019 Data Breach Investigations Report."

[2] Jessie Davis (Health IT Security). "Michigan Practice to Shutter after Hackers Delete Patient Files." April 2019.

[3] Lindsey O'Donnell (Threat Post). "Ransomware Attacks Leave U.S. Hospitals Turning Away Patients." October 2019.

[4] Manny Fernandez, David Sanger, Marina Trahan Martinez (The New York Times) "Ransomware Attacks Are Testing Resolve of Cities Across America." August 2019.

[5] Proofpoint. "Quarterly Threat Report Q3 2018." October 2018,

[6] Ponemon Institute. "Ninth Annual Cost of Cybercrime Study." 2019.

[7] Ibid.

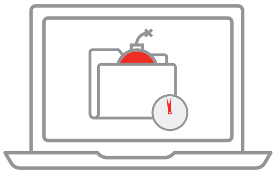
Surviving Ransomware

Most companies are ill-prepared for a ransomware attack. Although 66% of those surveyed in a Ponemon poll agree that ransomware is "very serious," only 13% said their company can prevent it.[8]

Ransomware compromises systems and data, but the attacks that lead up to it target people. Like most cyber attacks, ransomware usually requires someone to act on the attacker's behalf, such as opening an attachment or clicking a URL. That's why fighting ransomware requires a people-centric approach.

Consider this guide a starting point.

Before the Attack



The best security strategy is to avoid ransomware altogether. This requires planning and work—before the crisis hits.

Back up and restore

One of the most important parts of any ransomware security strategy is regular data backups. Because many ransomware strains target network-connected backups, maintain those backups offsite or in the cloud.

Surprisingly few organizations run backup and restore drills. Both halves are important; restore drills are the only way to know ahead of time whether your backup plan is working.

Update and patch

Keep operating systems, security software, applications and network hardware patched and up to date.

Train and educate users

Employee training and awareness are critical. Your people should know what to do, what not to do, how to avoid ransomware and how to report it. If employees receive a ransomware demand, they should know to immediately report it to the security team—and never, ever try to pay on their own.

Invest in robust people-centric security solutions

Even the best user training won't stop all ransomware.

Advanced email security solutions protect against malicious attachments, documents and URLs in emails that lead to ransomware. These solutions also protect against other malware, typically delivered through email, that can install malware in targeted follow-up attacks.

[8] Ponemon Institute. "The Rise of Ransomware." January 2017

During the Attack: Contain the Damage and Get Back to Business

While the best ransomware strategy is to avoid it in the first place, this advice means nothing if you're newly infected.

You have short-term problems to resolve, like getting computers, phones and networks back online and dealing with ransom demands.

Call law enforcement

Ransomware—like any form of theft and extortion—is a crime. Notifying the proper authorities is a necessary first step.

Disconnect from the network

The moment employees see the ransomware demand or notice something is odd, they should disconnect from the network and take the infected machine to the IT department.

Only the IT security team should attempt a reboot, and even that will only work in the event it is fake scareware or run-of-the-mill malware.

Determine scope of problem based on threat intelligence

Your response—including whether to pay the ransom—hinges on several factors:

- The type of attack, specifically the ransomware strain used and the attacker behind it
- The presence of earlier malware payloads that may have been used for reconnaissance or loading the ransomware
- Who in your network is compromised
- What network permissions any compromised accounts have

Many ransomware infections are often the result of secondary infections on already compromised networks. That means each of the factors are critical in assessing the scope of the problem and preventing further infections and data loss.

Orchestrate a response

A big part of your response is deciding whether to pay the ransom. The answer is complicated and may require you to consult law enforcement and your legal counsel. In some cases, paying may be unavoidable.

In any case, organizations must proceed thoughtfully. Whenever possible, organizations should have plans—and contingency plans—in place before an attack. And these plans should be tailored to the business. A hospital's response to ransomware on mission-critical patient care systems may be very different than a federal agency's.

Don't count on free ransomware decryption tools

Most free tools work for only a single strain of ransomware or even a single attack campaign. As attackers update their ransomware, the free tools fall out of date and likely won't work for your ransomware.

Restore from backup

The only way to completely recover from a ransomware infection is restoring everything from backup. But even with recent backups, paying the ransom might make more financial and operational sense.

After the Attack: Review and Reinforce

We recommend a top-to-bottom security assessment to find threats that may still linger in your environment. Take a hard look at your security tools and procedures—and where they fell short.

Cleanup

Some ransomware is delivered through other threats or backdoor Trojans that can lead to future attacks. Often, the victim's environment was already compromised, opening a door for the ransomware.

Look closer for hidden threats that you may have overlooked in the chaos.

Post-mortem review

Review your threat preparedness, the chain of events that led to the infection, and your response. Without figuring out how the ransomware attack got through, you have no way of stopping the next attack.

Assess user awareness

A well-informed employee is your last line of defense. Make sure employees, staff and faculty are up to the task. Regular assessments and phishing simulations can help pinpoint who is most vulnerable, and to which email lures and other tactics.

Education and training

Develop a curriculum to address employee vulnerability to cyber attacks. It should be based on real-world attack campaigns and tactics. Create a crisis communications plan in the event of a future attack, and follow-up with drills and penetration testing.

Reinforce your defenses

Today's fast-changing threat landscape requires security solutions that can analyze, identify and block—in real time—the malicious URLs and attachments that serve as ransomware's primary attack vehicles.

Seek out security solutions that can adapt to new and emerging threats and help you respond to them faster.

Introduction: An Old and Ongoing Threat

If you want a glimpse into how insidious ransomware attacks are today, visit Lake City, Fla. The city of 12,000 people was just one of many municipalities hit by ransomware in 2019. Like most ransomware attacks, this one encrypted all the data on the city's computer system, locking out city officials until they paid a "ransom" to regain access.

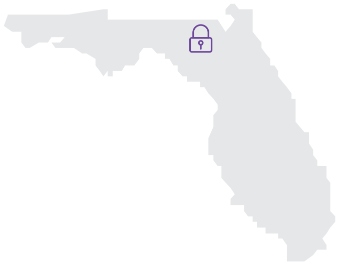
"They were super crafty," said Brian Hawkins, the city's IT director, describing the perpetrators.[9]

It all started with someone clicking the wrong email attachment, sent with the seemingly innocuous subject line "you have an invoice ready." Soon, the resulting ransomware was spreading throughout the city's network, encrypting every file it touched along the way.

"Phones were down, email was out of commission, computers did not work and even the photocopiers were inoperable," The New York Times reported.[10]

A Heavy Toll

Lake City's insurer eventually had to pay a ransom of $460,000 to the cyber attacker via Bitcoin to decrypt all the data. Officials spent several weeks fully restoring its IT infrastructure.[11]



Lake City, Florida paid a ransom of

$460,000

To decrypt the data on the city's computer system.

Lake City isn't alone. In July 2019, attackers struck the Georgia Department of Public Safety, affecting multiple agencies—primarily state troopers. Three months later, 50 people were still working to mitigate the damage.[12]

Close to two dozen cities in Texas were attacked about a month later in a coordinated ransomware attack, according to the state's Department of Information Resources (DIR).

A handful of other larger cities such as Baltimore, Md., and Albany, N.Y. have also been struck. But many much smaller cities, such as Lake City, seem particularly rich targets, presumably because they are regarded as "sleepy, cash-strapped local governments … least likely to have updated their cyber defenses or backed up their data," according to another New York Times report.[13]

[9] Frances Robles (The New York Times). "When Ransomware Cripples a City, Who's to Blame?" August 2019.

[10] Ibid.

[11] Ibid.

[12] Wright Gazaway (WTOC). "Ga. Dept. of Public Safety still dealing with ransomware attack." October 2019.

[13] Manny Fernandez, David Sanger, Marina Trahan Martinez (The New York Times) "Ransomware Attacks Are Testing Resolve of Cities Across America." August 2019.

Fewer Attacks, But More Damaging

Overall ransomware volume has fallen sharply. But the attacks that do occur "are more targeted, more profitable and cause greater economic damage," says the European Union Agency for Law Enforcement Cooperation, better known as Europol.[14]

"As long as ransomware provides a relatively easy income for cyber criminals, and continues to cause significant damage and financial losses, it is likely to remain the top cyber crime threat," the agency notes.[15]

It's a jarring prediction. But even more alarming is how unprepared most organizations are for a ransomware attack.

Just 13% of IT experts surveyed by Ponemon Institute said their organization can prevent ransomware. And more than 68% consider themselves "vulnerable" or "very vulnerable."[16]

This guide is designed to improve those odds. We'll reveal the factors behind ransomware's persistence, what to do if it happens to you, and most important, how to avoid falling victim in the first place.

> "As long as ransomware provides a relatively easy income for cyber criminals, and continues to cause significant damage and financial losses, it is likely to remain the top cyber crime threat,"
>
> **Europol,** European Union Agency for Law Enforcement Cooperation

[14] European Union Agency for Law Enforcement Cooperation (Europol). "Internet Organized Crime Assessment." October 2019.

[15] Ibid.

[16] Ponemon Institute. "The Rise of Ransomware." January 2017.

How Ransomware Works

Ransomware works by blocking access to a computer system or data, usually by encrypting files with specific extensions (JPG, DOC, PPT, and so on). Files remain out of reach until the victim pays the attacker for an encryption key code to unlock the files. In many cases, the payment demand comes with a deadline. If not met, that ransom can double, or the data can be lost forever, leaked and even destroyed.

The Real-World Costs

Nearly 60% of companies surveyed by the Ponemon Institute agreed that a ransomware attack would have “serious financial consequences” for their business.[17] And those consequences are growing. The average annual cost of dealing with a ransomware attack rose by 21% in 2018 over the year before, according to a 2019 study from Ponemon.[18]

Aside from the ransom itself (assuming victims pay), those costs include business disruption, information loss, revenue loss and damage to equipment.[19]

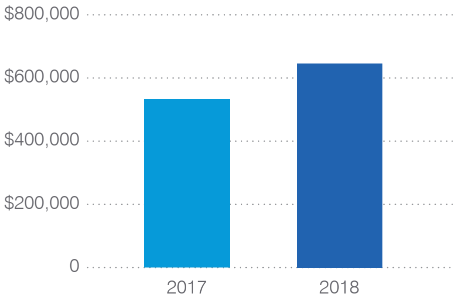
There’s another cost that may be difficult to put into dollars and cents but is nonetheless critical: the cost of a diminished brand.

Consider the WannaCry attack. While it didn’t net much of a payday for the attackers, the ransomware was highly disruptive. Not having access to critical information and working systems can slow emergency response and jeopardize public safety.

The healthcare sector has been hit especially hard. Infections lock away patient records, slow workflow, and even affect patient monitoring systems. This can make ransomware remediation a matter of life and death.

Rising Ransomware Costs

The average cost to resolve a ransomware attack **rose 21%** between 2017 and 2018, the largest jump among all types of cyber attacks.



[17] Ibid.

[18] Ponemon Institute. “Ninth Annual Cost of Cybercrime Study.” March 2019.

[19] Ibid.

Exploiting the Human Factor

Most ransomware starts, directly or indirectly, with a phishing email. These emails trick users into opening a malicious attachment or clicking a malicious URL. In recent attacks, the ransomware was a secondary infection that attackers use after first compromising networks through phishing emails and web-based attacks that deliver other forms of malware.

Throughout 2020, ransomware cyberattacks have targeted small municipalities throughout the United States through email. While these are hardly the only targets, municipalities have proven particularly vulnerable.

A May 2019 ransomware attack against Riviera Beach, Fla.'s city government is just one example. The city was running an older computer network that the original vendor had stopped servicing. Though an $800K IT security overhaul had been approved months earlier, the largely interim government had not yet deployed the system. That's when a police department employee clicked on an infected email attachment.[20]

The impact of that click was immediate: email, phones, police records, and the library were all knocked offline and inaccessible. Water utility pump stations failed. Direct deposited checks had to be handwritten by finance department staffers working overtime, speeding tickets hand scrawled by exhausted police officers.

After three weeks of trying to get around this extortion, Riviera Beach came to the grim determination the only way to get back online involved paying 65 Bitcoin—about $600,000—to unknown cyber attackers.

The attacks on cities in Florida, Texas and elsewhere have been attributed to a ransomware strain called Ryuk, which identifies files on the targeted entity's network and encrypts them. Ryuk is considered one component of a "triple threat" to these networks. This trio also includes Emotet, which distributes spam email to various addresses, and TrickBot, a modular Trojan that is usually used to download and install other malware such as Ryuk.[21]

Once ransomware enters a target network, it begins to encrypt files. Then a message appears on infected machines demanding payment, usually over the anonymous Tor network using Bitcoin. Victims can't close or get around the message. No amount of CTRL+ALT+DEL or rebooting will solve the problem.

[20] Taylor Armerding (Forbes). "Get Ready For A Ransomware Tsunami." July 2019.

[21] Jareth (Security Boulevard). "Ransomware Wreaks Havoc in the South, generates $1 million for hackers." September 2019.

What Happened to Ransomware Volume?

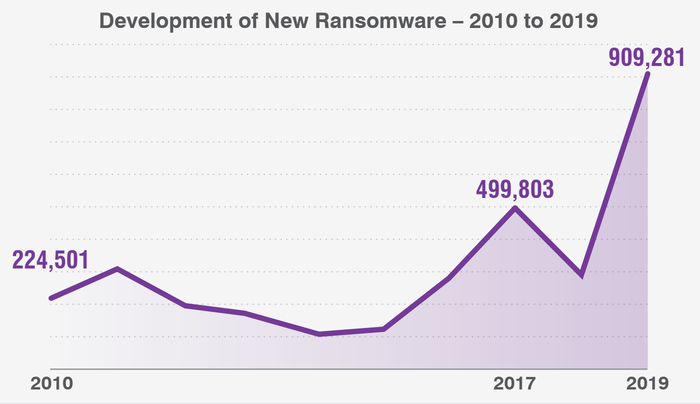
Ransomware attacks have fallen to a fraction of their 2017 heyday, though high-profile attacks still make headlines. Security researchers have a few hunches about this apparent vanishing act.

One of the leading theories follows the money. The value of cryptocurrency, attackers' preferred form of payment, has fallen from 2017 highs and remains volatile. That has made ransomware less of a sure bet for attackers.

Another possibility is that ransomware attackers "overharvested" the pool of potential victims. Ransomware's meteoric rise—and the headlines it generated—may have spurred organizations to act. Many have bolstered their cyber defenses, trained users to be more security-aware and adopted more robust backup regimens. The result: fewer organizations paid the ransoms.

More important, we're also seeing the use of ransomware in more carefully targeted, high-ransom attacks on victims who are most likely to pay. This is a big shift from the "spray-and-pray" ransomware campaigns of 2017.

In many recent cases, the targeted organizations may have already been compromised before being hit with ransomware. This condition allowed attackers to install ransomware on key, vulnerable pieces of infrastructure after carefully studying the target to determine where a system lockout would hurt the most. The approach boosted the chances of a payout, reducing the need or incentive to launch massive ransomware campaigns.



Source: AV-Test Institute. "Security Report 2019/2020." September 2020.

Where It Comes From

Ransomware is distributed through three main attack vectors:

- Email, including ransomware attachments and URLs that lead to malicious files
- Infected websites/links through social media and malware-infected advertising (malvertising)
- Other malware (such as loaders and stealers) that can infect already-compromised systems with ransomware

Even when the ransomware stems from other malware, an email is usually the initial vector.

These emails look legitimate and can fool unsuspecting employees. Often, the messages masquerade as official software updates, unpaid invoices or even a note from the boss targeted to a direct report.

Why It's Still Around

Ransomware is a decades-old exploit. But it has become a bigger threat because of four primary drivers.

More distribution channels

Cyber criminals can attack thousands of entities simultaneously using a variety of attack vehicles, opening the door for secondary ransomware attacks.

Conventional email gateways are overwhelmed with threats from all sides:

- Massive botnet-driven email campaigns
- Polymorphic malware that outpaces security vendors' ability to build new malware signatures
- Malicious URLs and malvertising that contain no attachments

Together, these factors make compromises more likely, giving ransomware more opportunities to gain a foothold.

Better targeting and more advanced tactics

Ransomware used to be a numbers game: attack hundreds of thousands of recipients in high-volume, low-ransom email campaigns and hope enough victims took the bait.

Today, attackers are getting choosier about their targets. They seek out vulnerable business- and mission-critical data and systems that victims desperately need access to in hopes of a bigger payout.

At the same time, ransomware attacks are growing more sophisticated. Instead of using ransomware in the first stage of an attack, cyber criminals compromise systems with more robust, multipurpose malware. Once they have a foothold, they deploy ransomware to devices of interest.

More lucrative targets

Instead of targeting individuals, cyber criminals are increasingly turning their sights to organizations with sensitive data, thinly stretched IT departments, and a high incentive to quickly settle the matter. Adding fuel to the fire is the security challenges common in hospitals, police departments, schools, and other state and local governments.

For these organizations, network downtime is not a viable option. It's no wonder that many make the quick calculation that forking over a ransom is the best business move.

Bitcoin and other digital currencies

Since its debut in 2009, Bitcoin has been a boon to civil libertarians and cyber criminals alike. Payments can't be traced back to sender or recipient, providing an anonymous, friction-free way to transact private commerce.

By demanding payment in Bitcoin, cyber criminals get anonymity that makes collecting ransoms far easier than before. Earlier forms of ransomware might require a pre-purchased debit card. While this approach can bypass banks' anti-fraud measures, it's much more cumbersome on both sides of the transaction.

All major variants of ransomware require payment in bitcoin. (**See sidebar**, page 12)

The Bitcoin Money Trail

In traditional kidnapping for ransom, the biggest challenge has always been collecting and getting away with the ransom itself. Unfortunately, ransomware cyber criminals have a much easier path.

The most popular form of payment involves untraceable cryptocurrencies, the most well-known of which is Bitcoin. Bitcoin enables person-to-person payment via the internet and does not involve a bank or government. As of December 2019, there are about 18 million bitcoins in circulation, according to the Buy Bitcoin Worldwide site. Since its debut in 2008, the currency has seen wild value fluctuations, peaking at nearly $20,000 in late 2017. At the time of this publication, one bitcoin was worth about $7,000 USD.[22]

A simple way of thinking about cryptocurrencies is to imagine them as the electronic equivalent of a casino chip. The tokens have no intrinsic value in the real world, but users can purchase tokens in their local currency and use them within the establishment—in this case the internet—then trade them in for currency upon exiting.

Similarly, cryptocurrencies can be purchased online using a credit card or bank account, from legitimate sources. In the case of ransomware, victims convert their local currency into “three bitcoins” for example, then send the bitcoins from a bitcoin wallet using the anonymous Bitcoin address provided by the attacker.

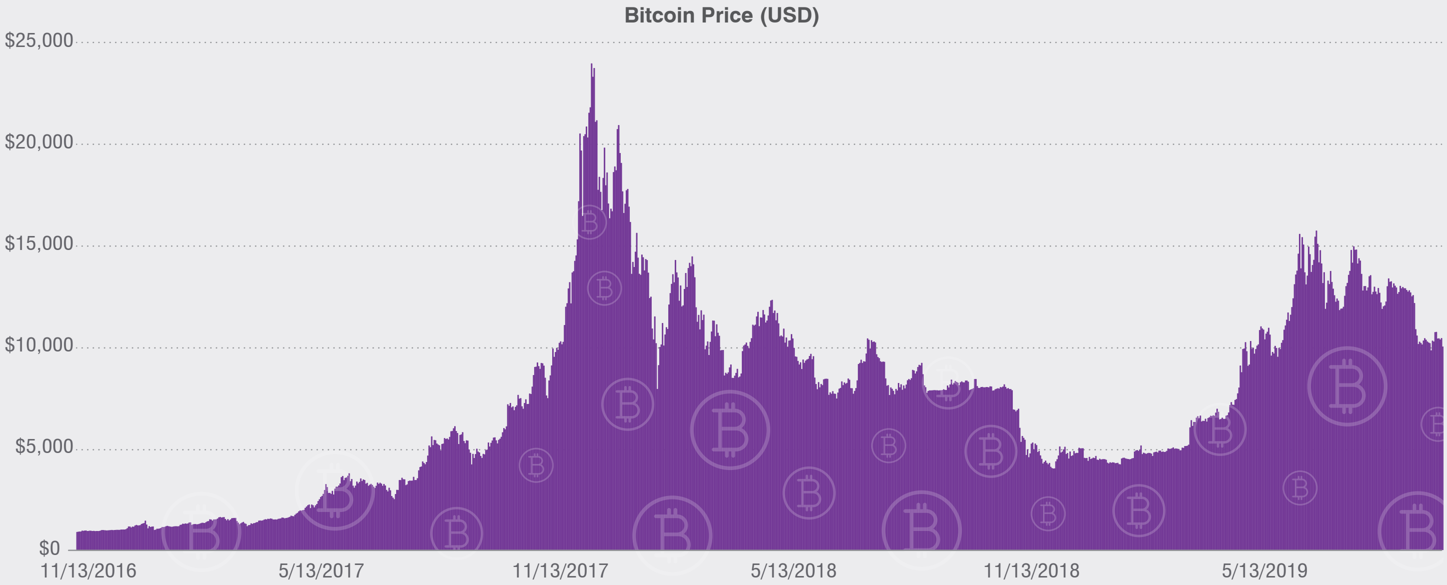
The coins don’t always go directly to the attacker. Typically, the tokens will land at a “tumbler,” an electronic service that mixes the bitcoins in with others, then dispenses coins out to the attacker (differently numbered, but the same value minus commission).

Much like money laundering in the physical world, the attackers can end up with untraceable payment. That payment then converts back into their local physical currency by trading in their bitcoins (tokens) for physical cash.

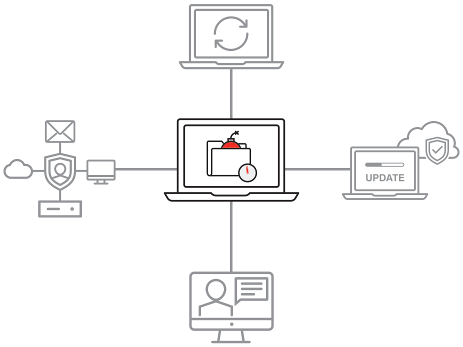
Unlike government-backed currency, cryptocurrencies are not widely recognized as money. They are instead regarded as something equivalent to poker chips or gaming tokens. Therefore, the transmission system and tumblers are neither regulated nor considered money laundering—though the effect is arguably the same.

The appeal of Bitcoin is obvious. It gives attackers a hard-to-trace, globally available cyber currency that converts directly to local hard currency, in other words, “unmarked bills.”

Such an approach has clear benefits over the use of stolen credit cards, whose value plummets by the day as financial institutions have become more adept at swiftly shutting down victims’ accounts.



[22] Bitcoin Price Index. Coindesk.com/price/bitcoin.



Before the Attack: Preventing Ransomware

The best security strategy is to avoid this extortion altogether. This is well within the power of most companies, but it requires planning and work—before the crisis hits.

Back Up and Restore

The most important part of any ransomware security strategy is regular data backups. Most companies do this, but surprisingly few run backup and restore drills. Both processes are important; restore drills are the only way to know ahead of time whether your backup plan is working.

You may have some kinks to work through before crisis mode hits. If backup-and-restore testing is done regularly, a ransomware infection won't have a devastating impact; you'll have a safe, recent restore point.

To repeat: most companies and individuals do backups. But regular testing of a full restore is just as critical.

Update and Patch

Ensure operating systems, security software, applications, and network hardware are fully patched and updated. It sounds basic enough. But according to a recent survey, more than half of organizations say there's no easy way to track whether vulnerabilities are being patched in a timely manner. And respondents reported that updates vary wildly in terms of complexity and release schedule.

But there are places to go to get a handle on patch management, such as the **Center for Internet Security** (CIS), a non-profit organization that shares and promotes best practices for IT security management, including the threat of ransomware.

Overcoming “patch fatigue” is necessary—and essential to maintaining a safe environment.

Train and Educate Users to Spot and Report Suspicious Email

Most ransomware begins with a single well-intentioned employee opening what appears to be a work-related email.

That's why employee training and awareness are critical. Your people should know what to do, what not to do, how to avoid ransomware, and how to report it. If anyone receives a ransomware demand, they should know to immediately report it to the security team—and never, ever try to pay on their own. Payment may carry serious brand reputation and security ramifications. This decision should be weighed carefully by upper-level management with advice of legal counsel.

Our research shows that cyber criminals actively exploit human error and curiosity. It's part of a larger cyber-crime trend—fooling humans into becoming unwitting accomplices in the quest to lock information and demand payment.

These attacks play on the user's lack of awareness. They usually require people to open malicious document attachments, download and open or execute documents or scripts, or take some other action. Once users click the "Enable Content" button to turn on macros in a malicious document, for example, it downloads ransomware and starts the attack process.

The most effective training teaches users about real-world attack techniques and campaigns. And it incorporates the latest threat intelligence to make users aware of the threats they're most likely to face. Phishing simulations can identify users who are especially prone to falling for ransomware and other attack tactics.

Invest in Robust, People-Centric Email, Web and Cloud Security Solutions

Even the best user training won't stop all ransomware. Today's phishing email is sophisticated and highly targeted. Attackers carefully research their targets to create email that looks legitimate and preys on human nature to get them to click.

Traditional legacy mail gateways, web filters, and antivirus software should be updated and running on all networks. But they alone cannot counter the ransomware threat. An effective email security solution must go deeper.

Because email is the initial infection point for most ransomware, you need advanced solutions that protect this critical vector.

That means analyzing embedded URLs and attachments to ensure no malicious content breaches the system. Cyber thieves are always one step ahead, and typical email security configurations rely far too heavily on outdated signatures.

Advanced email security solutions protect against malicious attachments, documents and URLs in emails that lead to ransomware. And email authentication based on the DMARC standard can stop attacks that rely on domain spoofing—impersonating your organization's email domain to gain users' trust. Your email security solution should also protect against other types of identity deception, such as display-name spoofing and lookalike domains.

Cloud-based email accounts are another prime vector for spreading malware. Cyber criminals can take control of users' cloud accounts to target other users within your organization, an attack known as email account compromise (EAC). Email accounts can be compromised in a few ways, including:

- Automated brute-force attacks, trying out countless username/password combination until something works
- Outside credential theft—knowing users often reuse passwords across accounts
- Credential-stealing malware

Securing users' cloud accounts is a critical part of protecting against ransomware attacks.

Finally, require remote users to connect to the internet through a corporate VPN so that they are protected by your cybersecurity defenses wherever they are.

Talking Tech: What the FBI Recommends

Beyond the security basics covered throughout this guide, the FBI also recommends these technical measures to head off ransomware attacks.

Audit and manage user privileges

Take a least-privilege approach to file, directory, and network share permissions.

Users who don't need to edit a file, for example should have read-only access only. In many cases, users shouldn't have access at all. A cashier doesn't need access to the company's financial records. And a hospital CEO doesn't need to look at patient health records.

Give users no more access than they need to do their jobs.

Stop code from running in certain locations

Deploy software controls to stop code from executing in common ransomware locations. These include temporary folders created by web browsers and compressed file directories in Windows' AppData/LocalAppData folder.

Restrict unknown software

Consider a safelist policy that allows systems to execute only known and vetted programs. Such a policy would prevent most ransomware from running, though it may not be feasible in every workplace.

Use virtual-machine technology

Virtual-machine (VM) technology executes apps and even entire operating systems in an isolated environment.

Think of it as a software "detonation chamber." Running sensitive or unvetted code within a VM environment or VM container ensures that any security issues that arise are confined to that virtual environment—leaving other parts of the system untouched.

Keep systems and data segmented

Keep valuable data and systems separated so that a security issue on one system doesn't affect other systems. For example, sensitive research or business data should not reside on the same server and network segment as an organization's email environment.

Learn more

The FBI offers detailed guidance in **"How to Protect Your Networks from Ransomware,"** available at **www.fbi.gov**.

During the Attack: Getting Back to Basics

You've been hit with ransomware. Now what?

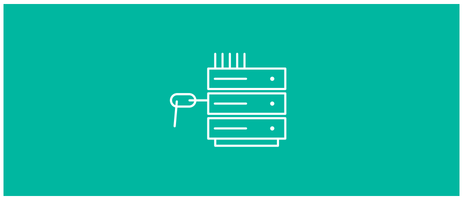
While the best ransomware strategy is to avoid it in the first place, this advice means nothing if you're newly infected. You have short-term problems to resolve, like getting computers, phones and networks back online, and dealing with ransom demands.

But a panicked response won't help—and may make things worse.

Call Law Enforcement

Ransomware—like other forms of theft and extortion—are a crime. Nobody has the right to seize devices, networks or data, let alone demand a ransom in exchange for it. Notifying the proper authorities is a necessary first step.

Contact local or federal law enforcement right away. Do not be afraid to just pick up your phone and call them. They are there to help you.



Disconnect From the Network

The second employees see the ransomware demand or notice something's odd—such as suddenly losing access to their own files—they should disconnect from the network and take the infected machine to the IT department.

We advise against having employees reboot their system. Only the IT security team should attempt a reboot, and even that will only work in the event it is "scareware," or fake ransomware.

In those cases, what appears to be ransomware is better described as "scareware." It may lock the user's screen with a ransom demand and payment instructions, but the data is not actually encrypted. In those scenarios, standard anti-malware tools can help.

Knowing the differences isn't always easy. Determine the scope of problem using threat intelligence. While all ransomware is bad, some attacks are worse than others. Your response—including whether to paying the ransom—hinges on several factors.

Ask the questions:

- **What type of attack is it?** Is this attack a secondary infection? Did it come from downloaders, remote access Trojans (RATs), or other malware installed on the infected machine or others on the network?
- **Who in your network is compromised?** How widespread are the infections? Is other malware on your network scouting your network, exfiltrating data, or ready to drop ransomware on other devices?
- **What network permissions do compromised accounts or devices have?** Ransomware may have been installed only after attackers had already moved laterally within the network or stolen credentials and other data.

Your answers should help network administrators scope the problem, devise an action plan and possibly curtail the spread.

Orchestrate a Response

Depending on network configuration, containing the spread to a single workstation might be possible.

Best case scenario: a new computer is swapped out for the infected machine and a restore from backup is completed. Worst case: every network machine is infected. This will require a quick cost-benefit calculation that weighs the time and resources needed to restore the data versus simply paying the ransom.

A big part of your response is deciding whether to pay the ransom. The answer is complicated and may require you to consult law enforcement and your legal counsel. For some victims, paying may be unavoidable (see **To pay or not to pay: ransomware's moral dilemma** on page 19).

Don't count on free ransomware decryption tools. Some security vendors offer free ransomware decryption programs. In some cases, they can help you retrieve your data without paying the ransom.

But most work for only a single strain of ransomware or even a single attack campaign. As attackers update their ransomware, the free tools fall out of date and likely won't work for your ransomware.

You may get lucky with a free decryption tool, but don't make it part of your incident response plan.

Restore from Backup

The only way to completely recover from a ransomware infection is restoring everything from backup—backups that should be happening every day. This might come last in terms of steps to take once infected but should be first in terms of prevention.

Even with recent backups, though, paying the ransom might make more financial and operational sense. Restoring backups takes time and effort. Some businesses might not be able to afford the downtime.

To Pay or Not to Pay: Ransomware's Moral Dilemma

Ransomware is bad enough in itself. But one of its especially loathsome aspects is that it forces victims to make both a Hobson's Choice and a moral one. When you're under the gun of a ransomware threat, you don't often have the luxury of time to carefully weigh the moral nuances of paying up. The attack is here—now.

Up until now, malware exploits have mostly required a straightforward course of action: fraud detection, report filing and resolution. Ransomware now introduces morality into the equation.

Paying up isn't just a repugnant but a necessary evil. It actively funds the attacker that has just broken into your network and stolen your data. It marks you as someone with a vulnerable network and incentive to pay. And it enables the cyber criminal to bankroll future attacks.

But recent attacks highlight an uncomfortable fact: there isn't always a black and white answer on whether to pay.

No organization wants to be extorted, let alone fund criminal rings. Then again, many victims may feel they have no choice. In some ways, it's the price to pay for having underfunded IT departments running unpatched or outdated software. There are still hospitals in the U.S. running Windows XP on legacy devices. And the ransom demand is often a relatively small price to pay when lives are on the line.

At times, even the FBI has advised victims to "just pay the ransom," according to Joseph Bonavolonta, Assistant Special Agent in Charge of the Cyber and Counterintelligence Program in the FBI's Boston office. The Bureau officially discourages paying. Even if you do pay, the agency points out, you still may not get your data back.

Another campaign to urge people to refuse to pay ransoms comes from Europol, the European Union's police agency. Its "No More Ransom" initiative, launched three years ago, is a public-private partnership intended to help cyber attack victims rebuild their data files.

The initiative has helped 200,000 ransomware victims recover their files and avoid paying $108 million in ransom. The No More Ransom tools are available to everyone, not just those in the EU.

Organizations must weigh conflicting considerations when choosing the best course of action. These factors can include:

- Time and resources getting back online
- Responsibilities to shareholders to keep the business up and running
- Safety of customers and employees
- What criminal activity the payment will potentially fund

As with most complicated questions, no two organizations will answer them in the same way.

After the Attack: Review and Reinforce

Regardless of the damage caused by ransomware, the attack reveals a security failure resulted in a device or network compromise. Now that things are back to normal, you have an opportunity to learn from the security breach and avoid future attacks.

We recommend a top-to-bottom security assessment, perhaps by an outside services firm, to find threats that may still linger in your environment. Now is also the time to take a hard look at your security tools and procedures—and where they fell short.

Cleanup

Some ransomware contains other threats or backdoor Trojans that can lead to future attacks. In other cases, a preexisting compromise opened the door to a ransomware infection. That's why wiping every device and restoring from a clean backup is a must. Look closer for hidden threats that you may have overlooked in the chaos.

Post-Mortem Review

Review your threat preparedness and response. How was the crisis plan executed? Can we improve networking configurations to contain future attacks? Can we implement a more robust email security solution? Should we take a whole new approach to cybersecurity in general?

Audit current security measures and ask if this is enough to combat today's threats. Turn this into a learning experience— because it very well might happen again. Without figuring out how the ransomware attack got through, you have no way of stopping the next attack.

Assess User Awareness

Most strains of ransomware rely on human interaction to deploy payloads. Should current security measures fail and a fake "unpaid invoice" makes it onto the email server, a well-informed employee is the last line of defense between a company, hospital or school staying online or becoming another ransomware statistic. Ensure employees, staff or faculty are up to the task.

It might also be worthwhile to invest in phishing simulation tools to drive employee awareness, identify those who are especially vulnerable, and improve overall security. By mirroring real-world attacks and the latest social engineering techniques and attack methods, phishing simulations can help analyze and identify people-related security vulnerabilities ahead of actual attacks.

Education and Training

After user awareness is analyzed, develop a curriculum to address employee vulnerability to cyber attacks, including lessons learned from previous encounters. The most effective training includes follow-up training for people who are more vulnerable, heavily targeted or have elevated privileges to sensitive data, systems and other resources.

And your training program should integrate into your other cyber defenses to help people not just identify attacks but promptly report them.

Invest in Modern Defenses

Today's cyber attacks target people, not infrastructure. Seek out security solutions that take a people-centric approach to keeping them protected.

Attackers do not view the world in terms of a network diagram. Deploy a solution that gives you visibility into who's being attacked, how they're being attacked, and whether they clicked. Consider the individual risk each user represents, including how they're targeted, what data they have access to, and whether they tend to fall prey to attacks.

At the same time, keep risky web content out of your environment. Web isolation technology can render web pages from suspicious and unverified URLs in a protected container within users' normal web browser. Web isolation can be a critical safeguard for shared email accounts, which are difficult to secure with multifactor authentication. The same technology can isolate users' personal web browsing and web-based email services, giving them freedom and privacy without compromising the enterprise.

Focused, targeted attacks call for advanced threat intelligence. Seek out a solution that combines static and dynamic techniques to detect new attack tools, tactics, and targets—and then learns from them.

Next Steps

As long as cyber criminals can find a way to make money from it, ransomware will exist in one form or another. The recommendations in this guide can start you on the path of dealing with ransomware before, during and after an attack.

Of course, the easiest way to combat ransomware is to stop it at the gates. That requires cyber defenses built for today's threats.

Robust cybersecurity is people-centric cybersecurity. It makes users more resilient through awareness training based on real-world attack techniques. It identifies and kills ransomware targeting your people. And it contains threats and helps you respond quickly and effectively when something goes wrong.

To learn more about how you can stop ransomware attacks, visit **www.proofpoint.com**.

Checklist

Here's a quick checklist to assess whether you're ready to prevent and manage ransomware threats.

Before: Preventing Ransomware

❑ Backup and restore
❑ Update and patch
❑ Train and educate users
❑ Invest in robust people-centric security solutions

During: Getting Back to Business

❑ Call law enforcement
❑ Disconnect from the network
❑ Determine scope of problem based on threat intelligence
❑ Orchestrate a response
❑ Don't count on free ransomware decryption tools
❑ Restore from backup

After: Review and Reinforce

❑ Clean up
❑ Conduct a post-mortem review
❑ Assess user awareness
❑ Educate and train users
❑ Invest in modern defenses

Your files have been
ENCRYPTED
To unlock them, pay .25 Bitcoin
Your files have been
ENCRYPTED
To unlock them, pay .25 Bitcoin

LEARN MORE

For more information, visit **proofpoint.com**.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.