



# Ransomware Survival Guide

Provided by: ToughComp

## Table of Contents

- Introduction ..... 3
- Types of Ransomware Incidents ..... 4
  - Factors Influencing Rising Incident Frequency and Severity ..... 5
- Attack Vectors and Techniques ..... 7
- Frequently Targeted Industries..... 9
- Prevention Measures ..... 11
  - Technical Procedures ..... 11
  - Operational Procedures ..... 14
- Response Protocols..... 16
  - Navigating Ransom Demands ..... 17
- Recovery Considerations ..... 18
- Conclusion..... 19
- Appendix ..... 20

## Introduction

Ransomware is any type of malicious software—also called malware—that infects a victim’s device or server and prevents the technology from working as it should or blocks access to certain data (e.g., confidential files or sensitive information) stored on such technology until the victim pays a ransom. Typically, the cybercriminals behind ransomware attacks demand bitcoin, a type of digital currency that can be difficult for authorities to trace. Businesses of all sizes and sectors can be targeted by ransomware, as it’s not only capable of infecting personal devices but also entire organizational networks. According to the latest research from technology corporation IBM, ransomware is one of the most damaging cyberattack methods, incurring an average of more than \$4.6 million in total losses per incident (not including the actual ransom payment).

Compounding concerns, ransomware incidents have surged in both cost and frequency throughout the past decade, largely driven by evolving attack vectors and techniques. After all, while ransomware attacks were originally limited to device-locking tactics, these incidents can now be carried out in several different ways and through various avenues. Additionally, the Ransomware-as-a-Service (RaaS) model no longer requires cybercriminals to possess advanced hacking skills to launch attacks, allowing those of varying digital capabilities to deploy these damaging incidents. The emergence of double and triple extortion ransomware attacks has also raised the stakes for businesses targeted by such incidents, posing the threat of even larger losses.

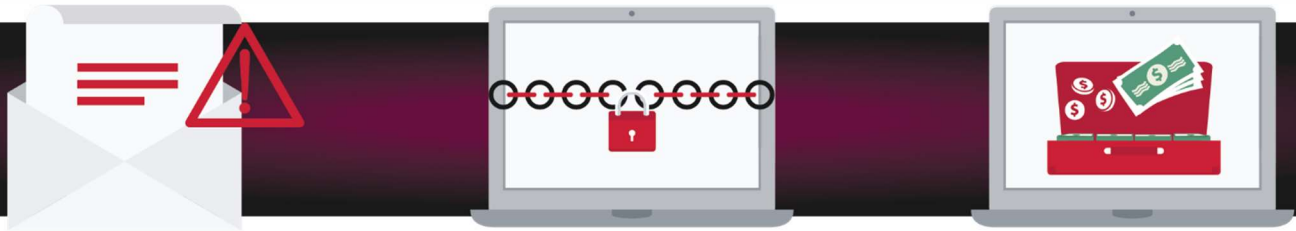
Amid these trends, the FBI’s Internet Crime Complaint Center recorded a 243% jump in the number of ransomware attacks reported between 2013 and 2020. According to a recent report by software company KnowBe4, these incidents currently represent more than one-fifth (21%) of all cyberattacks, costing victims an estimated \$20 billion in 2021 alone. Cybersecurity experts anticipate these trends will continue worsening, with global ransomware damages projected to exceed \$30 billion in 2023. Consequently, some cyber insurers have even implemented stricter underwriting standards (e.g., the need for policyholders to have documented cybersecurity practices and incident response plans) or additional coverage restrictions (e.g., ransomware exclusions) to limit their likelihood of making large-scale payouts following such attacks.

With these trends and information in mind, it has become increasingly critical for businesses across industry lines to better understand ransomware incidents, prevention measures and response procedures. In doing so, businesses can adequately limit their risk of being targeted in these attacks and minimize related losses in the event that such incidents do occur. This guide provides businesses with more information on types of ransomware incidents, attack vectors and techniques, frequently targeted industries, prevention strategies, response protocols and recovery considerations. It also contains an appendix with a number of cybersecurity resources—such as case studies, checklists, articles and infographics—that can help businesses mitigate their ransomware exposures.

Remember that this guide is not intended to be exhaustive, nor should any discussion or opinions be construed as legal advice. Employers should contact legal counsel or trusted insurance professionals for appropriate advice. Reach out to ToughComp today for additional risk management guidance and insurance solutions.

## Types of Ransomware Incidents

All ransomware attacks leverage the same general tactics of infiltrating a victim's device or server with malware and demanding payment in exchange for the restoration of their technology and data. Yet, specific attack layouts and extortion-related threats can vary between incidents.



Here's an outline of six of the most common types of ransomware incidents:

- 1. Locker ransomware**—Known as the original form of ransomware, this attack method entails a cybercriminal deploying an advanced malware program that physically locks the victim out of their device and requires them to make a payment in order to access their technology (as well as any data stored on it). During a locker ransomware incident, the victim will usually only be able to view their device's lock screen or interact with screen messaging containing the ransom demand. The device's mouse or keyboard (if applicable) may also be partially enabled to permit the victim to deliver a payment to the cybercriminal. While locker ransomware blocks access to technology and data, it typically doesn't damage or destroy such assets.
- 2. Encrypting ransomware**—Also called crypto ransomware or data kidnapping, this attack method refers to a cybercriminal launching malware to gain unauthorized access to the victim's device and encrypting sensitive information, files or other data stored on this technology—therefore making it unreadable. While the victim may still be able to utilize their device during such an incident, they wouldn't be able to view or obtain their data due to the encryption. From there, the cybercriminal will prompt the victim to make a payment in order to receive the necessary keys to decrypt their data, threatening to permanently delete this information if the ransom deadline passes.
- 3. Leakware**—Sometimes dubbed doxware or data exfiltration, this attack method follows the same layout as encrypting ransomware; however, rather than threatening to delete data stored on the victim's compromised technology if they don't meet the ransom demand, the cybercriminal will warn that they will release this information publicly in the absence of payment. Leakware incidents can be particularly damaging among businesses that store large amounts of confidential stakeholder data (e.g., financial information, contact details or medical records).
- 4. Destructive ransomware**—This form of attack also mirrors the layout of encrypting ransomware, the only difference being that the cybercriminal may not follow through on their promise of decrypting the victim's data. Instead, they proceed with deleting this information even after the ransom is paid—compounding the victim's overall losses. In most cases, destructive ransomware incidents are assumed to be carried out by nation-state threat actors or large-scale hacktivist groups as opposed to average cybercriminals.

5. **Mobile ransomware**—In contrast to other incidents, this attack method solely pertains to ransomware deployed on victims' mobile devices (e.g., smartphones or tablets). Such an incident generally involves a cybercriminal leveraging a malware-ridden application or device download to compromise the victim's technology and execute their attack. Because mobile devices often have automated cloud backup systems in place to help protect sensitive files and information, this form of ransomware typically doesn't rely on data encryption procedures.
6. **Scareware**—This type of attack entails a cybercriminal utilizing various scare tactics to frighten and manipulate the victim into paying a ransom, often through seemingly legitimate prompts (e.g., a fraudulent virus infection alert urging the victim to purchase security software for their device or a deceptive message claiming to be from law enforcement that accuses the victim of a crime and demands payment for an associated fine). Scareware may either initially contain malware or eventually coerce the victim into downloading malware.

### Factors Influencing Rising Incident Frequency and Severity

When ransomware attacks first emerged in the late 1980s, only the most advanced and highly skilled cybercriminals were capable of deploying these incidents. Such was the case for much of the past 30 years until RaaS debuted in the late 2010s. RaaS refers to a dark-web business model that permits sophisticated cybercriminals to sell their ransomware software to willing buyers (usually less skilled cybercriminals), who then utilize the software to launch attacks and secure ransom payments. These customers are usually provided with access to not only the ransomware software but also some form of a product portal. This portal may include detailed instructions for software implementation, user reviews, support forums and special discounts or offers for future purchases from the RaaS developer.

Customers may receive permanent access to the software they buy or only be given an allotted amount of time to utilize it. Depending on the developer, RaaS purchases can be a one-time sale or a monthly subscription service. In any case, the RaaS model poses a serious threat to all businesses, as it allows cybercriminals of any skill level to execute ransomware attacks.

**According to cybersecurity company Fortinet, the number of ransomware variants circulating worldwide nearly doubled between 2021 and 2022, suggesting a substantial increase in cybercriminals' utilization of the RaaS model.**

What's worse, a growing proportion of ransomware attacks have evolved into double or triple extortion incidents. Double extortion mirrors the layout of typical ransomware attacks, but cybercriminals copy or transfer victims' data to deploy an extra threat: Victims must pay ransoms not only to regain access to their technology and data but also to keep that data from being shared publicly (similar to leakware). Triple extortion takes this threat one step further, with cybercriminals utilizing stolen data to seek out victims' third-party associates (e.g., customers, suppliers and business partners) and demand additional ransoms from these parties to prevent their information from being exposed.

**Double and triple extortion are on the rise, as more than two-thirds (70%) of ransomware attacks now involve some form of data exfiltration, according to media company HealthITSecurity.**

These attacks can be significantly more damaging for affected businesses than average ransomware incidents. This is because even if businesses have protocols in place that allow them to recover their compromised information without paying ransoms, they may still be pressured to do so in order to keep their data from going public and protect their associates from being targeted—with no genuine guarantee that such payments will actually stop these threats from being carried out.

## Attack Vectors and Techniques

Because all ransomware incidents begin with cybercriminals infecting their victims' technology via malware, it's important to understand the different vectors and techniques that lead to these initial infections. The following are some of the most frequently utilized strategies for deploying malware and subsequent ransomware attacks:

- **Phishing scams**—With phishing scams, cybercriminals leverage fraudulent messages—namely, emails—to manipulate victims into sharing sensitive information, clicking deceptive links or opening harmful attachments. Such scams usually rely on social engineering tactics to trick victims (e.g., impersonating recognized senders, using threatening language or claiming urgent action is needed on a particular matter). These scams are a common vector for ransomware attacks, as the links or attachments in phishing messages often contain malware.

**According to IBM, phishing scams and other social engineering incidents contribute to nearly half (45%) of all ransomware attacks.**

In addition to traditional phishing scams, smishing—targeting victims with similar tactics through text messages rather than emails—is becoming an increasingly common vector for ransomware attacks (especially mobile ransomware incidents). This is likely due to the rising number of individuals utilizing their smartphones for both personal and work-related purposes.

- **Software vulnerabilities**—A variety of software vulnerabilities can provide entry points for cybercriminals to inject their victims' devices or servers with malware and execute ransomware incidents, thus serving as another potential attack vector. These vulnerabilities may include outdated security programs, poorly written or unpatched applications, systems designed to be accessed outside organizational networks and unsecured third-party platforms. Zero-day vulnerabilities, which either refer to those currently unknown to the cybersecurity community or those that have been identified but not yet addressed, pose particularly severe ransomware exposures. It should be noted that ransomware incidents could stem from software vulnerabilities within victims' own technology, as well as vulnerabilities among their clients' or suppliers' technology.
- **Remote desk protocol (RDP) pitfalls**—RDP consists of a digital interface allowing users to connect remotely to other servers or devices. Through RDP ports, employees can retrieve files and applications stored on their organization's networks while working from home, and IT departments can identify and fix employees' technical problems remotely. Unfortunately, RDP ports are also a vector for launching ransomware attacks. Such incidents usually stem from organizations leaving their RDP ports exposed to the internet. Although this exposure may provide convenience for employers in the scope of remote work operations, internet-exposed RDP ports are easy for cybercriminals to identify and offer a clear access point for deploying malware and related



ransomware attacks. In fact, a recent report conducted by cybersecurity firm Kaspersky revealed that nearly 1.3 million RDP-based cyberattacks occur each day.

- **Credential theft**—Gaining unauthorized access to victims’ technology via credential theft is another possible ransomware attack vector. Once a cybercriminal steals a victim’s credentials—whether they did so by leveraging password-cracking software, purchasing these details on the dark web or using brute-force techniques—they can easily infect the victim’s compromised technology with malware and carry out a ransomware attack. Devices and servers with minimal access requirements could be especially vulnerable to credential theft, malware infections and associated ransomware incidents.
- **Drive-by downloads**—Some cybercriminals are able to leverage deceptive applications, websites, software programs and digital advertisements to pass malware onto victims’ devices or servers without their knowledge, setting the scene for future ransomware incidents. This attack vector is also known as a drive-by download. Examples of drive-by downloads include exploit kits, which utilize compromised websites to scan visitors’ browsers for potential vulnerabilities and launch malware on the weakest systems; malvertisements, which are malware-ridden digital advertisements that can infect those who come across them online (even if they aren’t clicked on or otherwise interacted with); and Trojan horses, which are deceptive malware programs that appear to be legitimate software programs until they are opened.



## Frequently Targeted Industries

Any organization is at risk of experiencing a ransomware attack at any given time—potentially resulting in prolonged business interruption concerns, reputational damages and financial losses.

**According to managed services company TPx Communications, a business falls victim to a ransomware incident every 11 seconds, with downtime from such attacks often lasting more than a week. Downtime and related restoration efforts following ransomware incidents cost an average of \$274,000 per attack, sometimes costing up to 50 times more than the ransom demand itself.**

Considering these findings, it's vital for all businesses—regardless of size or sector—to clearly understand ransomware incidents and address their related exposures. However, certain industries carry elevated ransomware risks. In particular, sectors that have greater financial resources or store significant amounts of critical data are generally considered more attractive ransomware targets by cybercriminals. Here's a breakdown of those industries:



**Education**—Schools, universities and other educational institutions can be appealing targets because they possess a variety of data on faculty and students and often lack the resources needed to protect against advanced cyberthreats. Software company Emsisoft reported that 88 ransomware incidents occurred across the U.S. education sector in 2021 alone, disrupting operations for more than 1,000 schools. Half of these incidents even resulted in teachers' and students' personal information being leaked online.



**Finance**—Most financial institutions (e.g., banks) not only contain the capital necessary to deliver large ransom payments but also have access to sensitive client information and assets—therefore making these businesses top ransomware targets. According to recent research from IT security company Sophos, more than half (55%) of all financial institutions have experienced a ransomware attack, with the average remediation cost for such incidents in this industry sitting at \$1.59 million.



**Government**—Cybercriminals looking to cause widespread infrastructure damage are more likely to target government organizations in ransomware attacks. These organizations also generally hold highly confidential data on their community members—such as property deeds and Social Security numbers—making them increasingly attractive ransomware targets. Compounding concerns, many local government organizations (e.g., city and county administrations) utilize outdated technology, allowing cybercriminals easier access to their systems.



**Energy and utilities**—Similar to government organizations, energy and utility companies are at greater risk of being targeted in ransomware attacks by cybercriminals aiming to cause infrastructure damage. Because these companies' services are so essential to their communities, they may also feel more pressure to remedy ransomware incidents as quickly as possible. This can make them more prone to complying with

cybercriminals' ransom demands. According to security firm CyberSaint, 43% of energy, oil and utility companies that have experienced ransomware attacks paid the ransom.



**Health care**—Hospitals, treatment facilities and other health care institutions store a substantial number of medical records and personal data on their patients, making them more vulnerable to ransomware attacks. This information is also critical to such institutions' operations, heightening the likelihood of these incidents resulting in prolonged disruptions and treatment delays for patients.



**Manufacturing**—The manufacturing sector has emerged as a top ransomware target in recent years. According to Sophos, more than one-third (36%) of industrial and manufacturing companies have faced a ransomware incident, with almost half of these companies having their data encrypted amid such attacks. Additionally, IBM reported that it resolved more of these incidents in the manufacturing industry during 2021 than in any other sector.

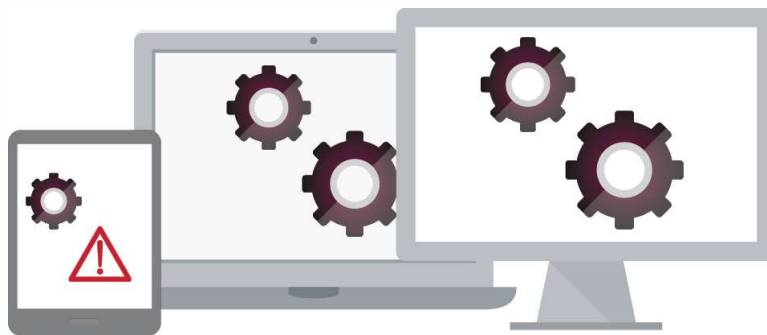
## Prevention Measures

Although ransomware attacks have become a rising concern for businesses across industry lines, there are ways to help prevent these incidents from happening and mitigate their impact. Businesses can adopt both technical and operational cybersecurity procedures to reduce their ransomware exposures and limit the likelihood of being targeted or facing severe damages from such attacks.

### Technical Procedures

Businesses should consider making the following adjustments to their technological processes in order to effectively minimize their ransomware risks:

- **Perform frequent data backups.** By keeping sensitive data secure, businesses can make it increasingly difficult for cybercriminals to access this information and use it against them amid ransomware attacks. One of the best ways to do this is by conducting frequent and secure data backups. First and foremost, businesses should determine safe locations to store their critical data, whether it's within cloud-based applications, on-site hard drives or external data centers. From there, businesses should establish concrete schedules for backing up this information and outline data recovery procedures to ensure swift restoration amid possible cyber incidents.
- **Leverage patch management plans.** To reduce their software vulnerabilities and, in turn, eliminate potential ransomware attack vectors for cybercriminals, businesses should conduct regular software updates. That's where patch management can help. Patch management refers to the process of acquiring and applying software updates, called patches, at various endpoints, such as smartphones, desktop computers, laptops, tablets and other devices that communicate back and forth with the networks in which they are connected. Patches modify operating systems and software to enhance security, fix bugs and improve performance. They are created by vendors and address key vulnerabilities cybercriminals may target.



The patch management process can be carried out by organizations' IT departments, automated patch management tools or a combination of both. Steps in the patch management process include identifying IT assets and their locations, assessing critical systems and vulnerabilities, testing and applying patches, tracking progress and maintaining records of such progress. As it pertains to limiting their ransomware exposures, businesses should be sure to establish patch management plans that include frameworks for prioritizing, testing and deploying software updates.

- **Utilize endpoint detection and response (EDR) solutions.** Businesses can use EDR solutions to continuously monitor security-related threat information across their devices and servers in order to better detect and respond to ransomware attacks and other kinds of malware. These solutions provide visibility into cybersecurity incidents occurring on various endpoints to help prevent digital damage and minimize future attacks. Namely, EDR solutions offer advanced threat detection, investigation and response capabilities—including incident data search and investigation triage, suspicious activity validation, threat hunting, and malicious activity detection and containment—by constantly analyzing events from endpoints to identify suspicious activity.

Implementing EDR solutions is critical in helping businesses leverage automated remediation amid potential ransomware incidents and promote more contextualized threat hunting through ongoing endpoint data analysis. Depending on their specific ransomware risks, some businesses may even want to go one step further and utilize extended detection and response (XDR) solutions. XDR is an evolution of EDR; while EDR can only detect and respond to threats inside managed endpoints, thus limiting the scope of threats that can be detected, XDR goes beyond the capabilities of EDR by analyzing all security layers and offering businesses a more holistic view of possible cyber exposures.

- **Enforce access control policies.** Access controls can make it significantly more complicated for cybercriminals to gain unauthorized entry into organizational accounts, devices and servers, further minimizing potential ransomware attack vectors. Some of the most valuable access control policies for businesses to consider include:
  - **The principle of least privilege (POLP)**—POLP is a cybersecurity concept that refers to allowing employees access to only the networks, data and technology necessary for performing their job duties. By implementing POLP, businesses can ensure cybercriminals won't receive full access to all company assets by compromising a single employee's account, therefore limiting available resources to leverage in a ransomware attack.
  - **Multifactor authentication (MFA)**—On the other hand, MFA is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify their identity for login. This additional login hurdle means that cybercriminals won't be able to easily unlock accounts, even if they have employees' passwords in hand. It's best practice for businesses to enable MFA for remote access to their networks, administrative functions within their networks and any enterprise-level cloud applications.
- **Segment and segregate networks.** When organizational networks lack sufficient restrictions and are closely interconnected, cybercriminals can easily hack into such networks and cause more widespread operational disruptions and damage amid ransomware attacks. That's why network segmentation and segregation are crucial. Network segmentation refers to dividing larger networks into smaller segments (also called subnetworks) through the use of switches and routers, permitting businesses to better monitor and control traffic flow between these segments.

Network segregation entails isolating crucial networks (i.e., those containing sensitive data and resources) from external networks, such as the internet. This gives businesses the opportunity to leverage additional security protocols and access restrictions within their most critical networks, making it more difficult for cybercriminals to penetrate these networks laterally. Both network segmentation and segregation allow businesses to take a granular approach to cybersecurity,

limiting the risk of cybercriminals gaining expansive access to their IT infrastructures (and the vital assets within them) and causing significant losses during ransomware incidents.

- **Establish RDP safeguards.** As RDP ports continue to be exploited in ransomware attacks, businesses must take steps to protect these ports. To properly safeguard their RDP ports, it's important for businesses to keep these ports turned off whenever they aren't in use, ensure such ports aren't left open to the internet and promote overall interface security through the use of a virtual private connection and MFA.
- **Implement email authentication technology.** As it relates to preventing ransomware incidents that begin with phishing scams, email authentication technology is a useful tool. This technology monitors incoming emails and determines the validity of these messages based on specific sender verification standards that businesses have in place. There are several different verification standards that businesses can choose from, but the most common is sender policy framework (SPF), which focuses on verifying senders' IP addresses and domains.



Upon verifying emails, email authentication technology permits them to pass through organizations' IT infrastructures and into employees' inboxes. When emails can't be authenticated, they will either appear as flagged in employees' inboxes or get blocked from reaching inboxes altogether. With SPF, unauthenticated emails may even be filtered directly into employees' spam folders. Ultimately, email authentication technology can make all the difference in keeping dangerous emails out of employees' inboxes and putting a stop to cybercriminals' ransomware tactics before they can begin.

- **Prioritize end-of-life (EOL) software management.** At some point, all software will reach the end of its life. This means manufacturers will no longer develop or service these products, discontinuing technical support, upgrades, bug fixes and security improvements. Consequently, EOL software will have vulnerabilities cybercriminals can easily exploit to deploy ransomware attacks. As such, it's clear that proactive EOL software management is necessary to prevent unwelcome surprises and maintain organizational cybersecurity.

In particular, businesses should adopt life cycle management plans that outline ways to introduce new software and provide methods for phasing out unsupported software; utilize device management tools to push software updates, certifications and other necessary upgrades to numerous devices simultaneously; and review the EOL status of new software before selecting it for current use to avoid any confusion on when it will no longer be supported and plan for replacements as needed.

## Operational Procedures

In addition to adjusting their technological processes, businesses should also consider implementing changes within their operations to combat ransomware exposures:

- **Provide cybersecurity training.** Employees are widely considered organizations' first line of defense against ransomware incidents, especially since all it takes is one staff mistake to compromise and wreak havoc on an entire workplace system. In light of this, it's crucial for businesses to offer cybersecurity training. This training should center around helping employees identify and respond to common cyberthreats and ransomware attack vectors. Namely, such training should provide employees with the following best practices:
  - Avoid opening or responding to emails or texts from individuals or organizations you don't know. If a message claims to be from a trusted source, be sure to verify their identity by double-checking the email address or phone number.
  - Never click on suspicious links or pop-ups—whether they're in an email, text message or website. Similarly, avoid downloading attachments or software programs from unknown sources or locations.
  - Browse only safe and secure websites on organizational devices. Refrain from using workplace devices for personal browsing.
  - Contact your manager or the IT department immediately for guidance if you suspect a ransomware attack.

Because ransomware risks continue to evolve, this training shouldn't be a one-time occurrence. Businesses should provide cybersecurity training regularly and update it when needed to reflect the latest threats, attack trends and workplace changes.

- **Have a plan.** In the event that a ransomware attack is suspected or detected, it's essential for businesses to have dedicated cyber incident response plans in place that outline steps to ensure timely remediation and keep damages to a minimum. These response plans should address a variety of possible ransomware attack scenarios and be communicated to all applicable parties. Both the Cybersecurity & Infrastructure Security Agency ([CISA](#)) and the National Institute of Standards and Technology ([NIST](#)) have resources available to help businesses create such plans. At a glance, a solid response plan should outline:



Who is part of the cyber incident response team (e.g., company executives, IT specialists, legal experts, media professionals and HR leaders)



What roles and responsibilities each member of the response team must uphold during an incident







What the company's key functions are, and how these operations will continue throughout an incident



How critical workplace decisions will be made during an incident



-  When and how stakeholders and the public (if necessary) should be informed of an incident
-  Which federal, state and local regulations the company must follow when responding to an incident (e.g., reporting protocols)
-  When and how the company should seek assistance from additional parties to help recover from an incident (e.g., law enforcement and insurance professionals)
-  How an incident will be investigated, and what forensic activities will be leveraged to identify the cause and prevent future incidents

- **Conduct tabletop exercises and penetration testing.** It's not enough for businesses to simply create cyber incident response plans. Rather, they should routinely assess these plans for ongoing security gaps and make changes as needed to ensure maximum protection amid ransomware attacks. Common assessment techniques include:
  - **Penetration testing**—Such testing consists of an IT professional mimicking the actions of a cybercriminal to determine whether an organization's workplace technology possesses any vulnerabilities and is able to withstand attack efforts. This testing usually targets a specific type of workplace technology—such as the organization's network(s), website, applications, software, security systems or physical assets (e.g., computers and smart devices)—and may leverage various attack vectors. Conducting penetration tests can help businesses review the effectiveness of their cybersecurity measures, identify the most likely avenues for ransomware attacks and discover potential weaknesses.
  - **Tabletop exercises**—A tabletop exercise is an activity that allows an organization to simulate a realistic cyberattack scenario for the purpose of testing its incident response plan's efficiency. In other words, this exercise serves as a cyberattack drill, giving participants (typically members of the incident response team) the opportunity to practice responding to an attack. Conducting tabletop exercises is a valuable way for businesses to assess the overall reliability of their incident response plans as well as ensure these plans will run smoothly during an actual ransomware attack.
- **Consult trusted experts and professionals.** Businesses don't have to navigate and address their ransomware exposures alone. Instead, they can seek assistance and supplement their existing resources with guidance from a wide range of trusted external parties—including insurance professionals, legal counsel, cybersecurity firms, law enforcement and government agencies (e.g., CISA and NIST).
- **Purchase sufficient coverage.** It's critical for businesses to purchase adequate cyber insurance to secure ample financial protection against potential losses that may arise from ransomware incidents. Businesses should consult trusted insurance professionals to discuss their specific coverage needs.



## Response Protocols

Even with effective prevention measures in place, some businesses may still be targeted in ransomware attacks. However, the way they respond to these incidents can make all the difference in keeping related disruptions and damages to a minimum. As such, businesses should consider the following ransomware attack response protocols:

- **Validate the incident.** Notification of suspected ransomware attacks will likely arise from one of two possible avenues: alerts from cybersecurity scanning or monitoring tools (e.g., EDR/XDR solutions or antivirus software) or employee reports of suspicious activity. First and foremost, businesses should ensure these avenues are always open by performing routine maintenance on all cybersecurity tools and educating employees on proper reporting measures—particularly as they pertain to identifying phishing scams, encrypted data or compromised technology. As soon as a potential attack has been reported, a business should assess the associated alert or report and determine whether the incident is a genuine threat. If the attack can be validated, the business should immediately call upon the cyber incident response team to decide the next steps.
- **Execute the response plan.** Upon confirmation of a ransomware attack, a business should coordinate with the cyber incident response team and execute the response plan. In the scope of a ransomware incident, specific procedures outlined in the response plan will likely include:



Analyzing which systems and data have been impacted by the incident and informing employees, making it clear that they shouldn't respond to any ransom demands



Isolating all infected devices or servers and taking affected networks offline (or powering them down if going offline is not feasible)



Accessing backups of any impacted data (if possible) and keeping this information in a secure, offline location



Triaging system remediation efforts by prioritizing the recovery of the most critical assets (e.g., technology and data that is vital to health and safety, revenue generation or key operations) and deprioritizing assets that either aren't deemed as valuable or haven't been impacted



Documenting as many details as possible about the incident and its impact in order to provide ample information to insurers, forensic investigators and law enforcement



Utilizing offline communication methods (e.g., phone calls) to discuss future steps with the response team to prevent cybercriminals from intercepting any important conversations

- **Contact applicable parties.** Depending on the nature and severity of a ransomware incident, there are various parties that a business will need to inform about the attack—whether it’s for the purpose of ensuring financial protection, getting additional remediation assistance, discussing legal ramifications or notifying impacted individuals (i.e., those who may have had their data exposed). These parties may include:
  - Insurers, brokers and risk management professionals
  - IT experts and cybersecurity firms
  - HR, communications and media professionals
  - Law enforcement and forensic investigators
  - Government agencies and legal counsel
  - Stakeholders (e.g., customers, investors and suppliers)

In any case, communication is key both during and after a ransomware incident. If a business fails or neglects to inform necessary parties of an attack, it could face substantially higher losses, regulatory penalties and widespread reputational damage.

### Navigating Ransom Demands

One of the most difficult decisions businesses will have to make amid ransomware attacks is whether to pay the ransom. Yet, businesses that pay ransom demands may be more likely to be targeted in future ransomware attacks, as cybercriminals will remember their willingness to deliver payments in the past.

**The FBI generally advises against complying with ransom demands, as there is no guarantee that cybercriminals will follow through with their end of the negotiations, potentially compounding overall losses.**

Businesses and their cyber incident response teams should work together to establish clear criteria on when they will adhere to ransom demands (if at all). Such criteria should be based on existing system recovery and data backup capabilities, as well as the nature of organizational operations. For instance, businesses that store highly confidential data or are responsible for maintaining critical infrastructure may be more vulnerable to excessive disruptions and damages during prolonged ransomware attacks, possibly motivating them to remedy such incidents faster via ransom payments. In some instances, it may even be valuable for businesses to have crisis negotiation experts on standby to further assist them in navigating ransom demands when incidents occur.

Nevertheless, businesses should be sure to consult trusted insurance professionals to discuss how their cyber coverage will (or won’t) respond to ransom payments, as some policies may have exclusions for losses resulting from compliance with ransom demands.

## Recovery Considerations

In the aftermath of ransomware attacks, businesses should take certain steps to ensure a successful recovery process, identify key takeaways and make adjustments as needed to prevent future incidents. Here are some recovery considerations for businesses to keep in mind:



**Restore systems and data.** The first priority for any business following a ransomware attack is to restore all impacted systems and data. This may include wiping any devices or servers of malware, taking affected networks back online and transferring data backups to their primary locations. In some cases, this could also entail purchasing new technology or software to replace any severely damaged assets.



**Look for remaining threats.** Even after restoring systems and data, it's possible that cyberthreats and vulnerabilities from a ransomware incident may remain within a business's devices, servers or networks. That's why it's vital to conduct an in-depth "cleanup" of this technology to make sure any ongoing concerns have been addressed. This may require the assistance of external cybersecurity professionals.



**Perform a post-incident analysis.** To properly assess how a ransomware attack was handled and identify any shortcomings, it's best for a business to conduct a post-incident analysis. Specifically, this analysis should focus on where the attack originated; how the attack was detected (as well as how quickly such detection occurred); how effective the incident response plan was in handling the attack; and the different technical, operational and financial impacts of the attack. Depending on the attack's origin and the overall damages, it may also be worthwhile to evaluate whether employee training (or lack thereof), software vulnerabilities or data backup processes played a role in the incident.



**Identify weaknesses and fill any gaps.** Based on the results of the post-incident analysis, a business should point out its cybersecurity weaknesses and make an effort to fill possible gaps with bolstered defenses. Doing so is critical to help prevent future incidents and minimize associated damages. Necessary adjustments may include modifying the cyber incident response plan, enhancing employee training, updating or introducing new software, improving data backup protocols and implementing stricter security policies.

## Conclusion

As a whole, it's evident that ransomware attacks have become a pressing concern for all businesses, regardless of size or industry. With these incidents on the rise, businesses simply can't afford to ignore their ransomware exposures. Nonetheless, by implementing effective prevention, response and recovery procedures, businesses can not only limit their likelihood of experiencing such incidents but also mitigate possible losses when attacks arise.

Above all, it's crucial for businesses to understand that they aren't alone in managing their cyber risks and safeguarding against ransomware attacks. There is a wide range of resources and guidance available from trusted experts and professionals. For more information, contact ToughComp today.

The background is a dark gradient with a central circular motif. Inside the circle, there is a faint illustration of a laptop with a padlock on its base and a magnifying glass over a stack of coins. To the right of the circle, there are circuit-like lines and nodes. On the far right edge, there is a bright, glowing light effect.

# Appendix

# The History of Ransomware

Ransomware attacks have evolved significantly since they first emerged in the late 1980s. Here's a timeline of how this increasingly common cyberattack method has changed and developed over the past several decades:



## 1989: Ransomware Makes Its Debut

At this time, the first-ever ransomware attack was recorded. This incident — coined the AIDS trojan — was distributed via thousands of infected floppy disks at a World Health Organization conference for AIDS. After users inserted the compromised discs within their computers, their personal files were hidden, and a message appeared that demanded the victims send \$189 (equivalent to \$437 in 2022) to a P.O. Box in Panama to retrieve their files. However, this attack was shut down quite easily with file decryption technology.



## 1996: Experts Warn of Dangers to Come

While the 1990s passed by without any notable ransomware attacks occurring, computer scientists issued a warning in 1996 that more advanced forms of malware and data encryption were likely to emerge in the coming years — making ransomware a rising cyberthreat.



## 2005: Ransomware Sees an Uptick

During this time, ransomware incidents began to increase worldwide, often centered within Russia and Eastern Europe. This uptick can largely be attributed to a rise in the circulation of different ransomware variants, asymmetric encryption software and extortion methods. Nevertheless, these attacks were still relying on simple code, allowing most targets to deter such incidents with standard antivirus software. As a result, cybercriminals began transitioning to new attack vectors, such as phishing scams.



## 2009-2013: Cryptocurrency Creates Further Complications

Throughout this period, more advanced viruses and encryption software emerged (e.g., Vundo, WinLock, Reveton and CryptoLocker), compounding ransomware concerns. Additionally, the development of cryptocurrency (i.e., bitcoin) began permitting cybercriminals to obtain untraceable ransom payments, driving up overall ransomware activity.





### **2015: Ransomware-as-a-Service (RaaS) Emerges**

At this time, the RaaS model debuted. RaaS refers to a dark-web business model that permits sophisticated cybercriminals to sell their ransomware software to willing buyers, who then use it to launch attacks and secure ransom payments. This model has since allowed cybercriminals of any skill level to execute ransomware attacks, leading to a surge in incident frequency.



### **2018-Present Day: Incident Frequency and Severity Surges**

Amid rising utilization of the RaaS model and the emergence of double and triple extortion techniques, ransomware incidents skyrocketed over the past few years. Today, large-scale attacks with major losses — such as WannaCry, Kasseya and Colonial Pipeline — have become all too common.

In this ever-changing cyber risk landscape, it's important now more than ever to take steps to address your unique ransomware exposures. Contact us today for the latest cybersecurity updates and solutions.



# Ransomware Case Studies

As ransomware attacks continue to rise in frequency in severity, it's important for organizations to have a clear understanding of these incidents and their potential consequences. In particular, reviewing past ransomware incidents can help organizations identify what went wrong, determine key takeaways and implement cybersecurity measures to prevent similar attacks within their own operations.

Here are some brief case studies of ransomware incidents that made headlines in recent years.



## City of Atlanta

In the spring of 2018, cybercriminals compromised several computer networks within Atlanta's City Hall to launch a ransomware attack. From there, the cybercriminals restricted access to a wide range of online platforms, municipal operations and databases — requiring more than \$50,000 in bitcoin to be paid in exchange for restoration. Nevertheless, the city of Atlanta refused to reward the cybercriminals and did not pay the ransom. As a result, the city took several months to recover from the incident, disrupting various government services for extended periods. In total, the incident is estimated to have cost both the city and its taxpayers nearly \$17 million.

Looking back, this incident highlighted the dangers of weak access controls and unpatched security software. After all, an audit performed just two months prior to the incident stated that there were between 1,500 and 2,000 total vulnerabilities identified within the Atlanta government's digital operations and technology — suggesting the city had become complacent regarding cybersecurity.



## Blackbaud

In June 2020, Blackbaud — a cloud software company that services a range of health care organizations, educational institutions and other nonprofits across North America and the United Kingdom — was targeted in a ransomware attack. Although Blackbaud provided the cybercriminal responsible for the attack with a ransom payment, this incident still led to a number of the company's customers having their sensitive data compromised.

In particular, the incident impacted an estimated 536 organizations and 13 million individuals throughout the United States, Canada and the United Kingdom. In the aftermath of the attack, Blackbaud was sued in a total of 23 putative consumer class action lawsuits, including 17 in U.S. federal courts, four in U.S. state courts and two in Canadian courts. Further, the company incurred costs of more than \$3 million in recovering from the attack between July and September 2020. Such an incident emphasized the potential supply chain exposures created by ransomware attacks, as well as the cybersecurity risks that can persist even after a ransom payment is made.



## **UVM Health Network**

In October 2020, the University of Vermont (UVM) Health Network — a six-hospital health care organization that serves more than 1 million patients throughout Vermont and upstate New York — discovered that its systems had been compromised by cybercriminals in a ransomware attack. This incident led to major disruptions across the organization's infrastructure, shutting down critical technology and delaying patient care.

As a whole, the attack is estimated to have cost UVM Health Network more than \$63 million. These costs greatly exceeded the organization's existing cyber insurance protection, as it was only insured for \$30 million. Upon reflection, this incident — which originally stemmed from an employee falling victim to a phishing scam — emphasized the importance of robust and routine cybersecurity training.



## **Colonial Pipeline**

One of the nation's largest pipelines was forced to shut down in early May 2021 after falling victim to a ransomware attack. The 5,500-mile pipeline is operated by Colonial Pipeline and carries refined gasoline and jet fuel from Texas to New York. This pipeline transports 45% of the east coast's fuel supplies. The attack — carried out by DarkSide ransomware — resulted in gas shortages along the east coast due to Colonial Pipeline halting its operations in an effort to contain the breach.

DarkSide reportedly stole 100 gigabytes of data from Colonial Pipeline and allegedly threatened to leak portions of it to the public unless a \$5 million ransom was paid. This method, known as double extortion, involves cybercriminals not only encrypting stolen data and making it inaccessible but also threatening to release it. Overall, this incident showcased the growing severity of ransom demands, the cybersecurity risks posed by aging infrastructure and outdated operating systems, and the value of backing up critical data.

For additional cybersecurity news and resources, contact us today.

# 5 RANSOMWARE THREATS TO KNOW

These days, cybercriminals are organized and well-funded. Unlike a lone threat actor, ransomware groups will reinvest a portion of their profits into hiring and training talented cybercriminals, making them more dangerous to organizations. As ransomware tactics evolve, it's important for organizations to be up to date on current ransomware techniques.



Here are five **ransomware threats** to know:



## Attacking the Cloud

Ransomware groups target known vulnerabilities in cloud software and applications. Sometimes they access the cloud through targeted attacks on individual devices or cloud accounts.



## Targeting Managed Service Providers

Compromising managed service providers enables cybercriminals to infiltrate multiple organizations in one attack.



## Attacking Industrial Processes

According to the FBI, several ransomware groups have created code to stop critical infrastructure and industrial processes.



## Targeting Supply Chains

Compromising software supply chains allows cybercriminals to gain access to multiple victim organizations in one breach.



## Attacking on Holidays

Cybercriminals are increasingly attacking on weekends and holidays when there are fewer IT and support personnel working.

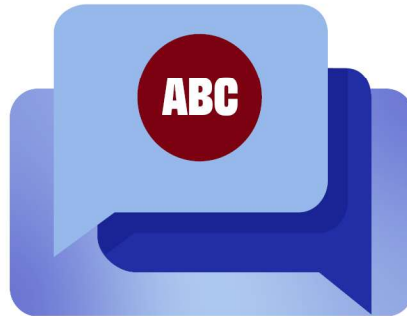


# 8 Tips to Avoid Email Phishing Scams

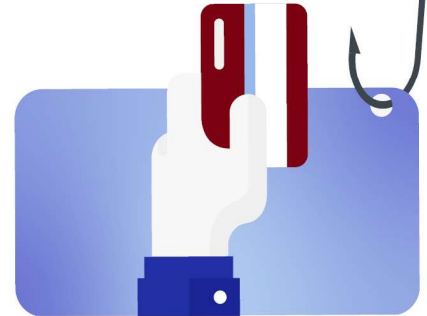
Every day, more than 3 billion phishing emails are sent out worldwide. These emails are tactics used by scammers to trick you into giving up sensitive information about you or your company. Here are eight tips to avoid email phishing scams:



**1. Verify the sender's email address.** Scammers may pretend to be your bank, a colleague or even a family member. Check any previous conversations with the sender or your address book to verify the email address.



**2. Look for spelling errors.** Various spelling or grammatical errors within an email can indicate fraudulent activity.



**3. Never give out sensitive information.** Most legitimate companies will avoid asking for personal information via email.



**4. Be wary of urgent messages.** People are more likely to give up sensitive information when pressured by a sense of urgency.



**5. Call to verify requests.** If you are skeptical of any requests made in an email, call the source directly to verify.



**6. Avoid opening unsolicited attachments.** Attachments can be embedded with malware—if opened, malware can steal sensitive information by gaining access to your computer or network.



**7. Verify hyperlinks.** Before opening a hyperlink, hover over the link text to verify the linked web address.



**8. Contact IT or security teams.** If unsure of an email's validity, report it to your IT department or security team to have them check for fraudulent activity.

This infographic is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice. © 2020 Zywave, Inc. All rights reserved.

# CYBER HYGIENE BEST PRACTICES

As cyberattacks become more frequent and severe, it's increasingly important for organizations to practice good cyber hygiene—habitual practices ensuring critical data and connected devices are handled safely—to minimize their exposure to risk. Some consequences of poor cyber hygiene include:



**Security breaches**



**Data loss**



**Software vulnerabilities**



**Antivirus weaknesses**

The following are essential parts of cyber hygiene:



**Passwords**—Users should create strong and complex passwords and avoid sharing passwords or using the same password across different accounts.



**Security software**—A high-quality antivirus software can perform automatic device scans to detect and remove malicious software and provide protection from various online threats and security breaches.



**Data backups**—Essential files should be backed up in a separate location, such as on an external hard drive or in the cloud.



**Firewalls**—Organizations should have a network firewall to prevent unauthorized users from accessing company websites, email servers and other sources of information.



**Multifactor authentication**—Important accounts should require multifactor authentication to limit the opportunity for cyber-criminals to steal data.



**Employee education**—Workforce cybersecurity education is essential to teach employees to identify phishing attacks, social engineering and other cyberthreats.

Daily routines, good behaviors and occasional checkups can make all the difference in ensuring an organization's cyber health is in optimal condition. For additional risk management guidance, contact us today.

# CHECKLIST | RANSOMWARE PREVENTION BEST PRACTICES

Presented by ToughComp

Date:

To protect your organization from becoming a victim of ransomware, the Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends using the following checklist.

Be Prepared		
1a.	It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important for backups to be maintained offline, as many ransomware variants attempt to find and delete any accessible backups. Keeping current, offline backups is critical because there is no need to pay a ransom for data that is readily accessible to your organization.	<input type="checkbox"/>
1b.	Maintain regularly updated “gold images” of critical systems in the event they need to be rebuilt. This entails maintaining image “templates” that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.	<input type="checkbox"/>
1c.	Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred. <ul style="list-style-type: none"><li>• <b>Note:</b> Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.</li></ul>	<input type="checkbox"/>
1d.	In addition to system images, applicable source code or executables should be available (i.e., stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly. Having separate access to needed software will help in these cases.	<input type="checkbox"/>
2a.	Create, maintain and exercise a basic cyber incident response plan and an associated communications plan that includes response and notification procedures for a ransomware incident.	<input type="checkbox"/>
2b.	Review available incident response guidance.	<input type="checkbox"/>

Ransomware Infection Vector: Internet-facing Vulnerabilities and Misconfigurations		
1.	Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface. <ul style="list-style-type: none"><li>• <b>Note:</b> CISA <a href="#">offers</a> a no-cost Vulnerability Scanning service and other no-cost assessments.</li></ul>	<input type="checkbox"/>
2a.	Regularly patch and update software and OSs to the latest available versions.	<input type="checkbox"/>
2b.	Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins and document readers—for known vulnerabilities.	<input type="checkbox"/>

3.	Ensure devices are properly configured and security features are enabled. For example, disable ports and protocols that are not being used for a business purpose (e.g., Remote Desktop Protocol [RDP]—Transmission Control Protocol [TCP] Port 3389).	<input type="checkbox"/>
4a.	Employ best practices for the use of RDP and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services and later propagate ransomware. See CISA <a href="#">Alert</a> AA20-073A, Enterprise VPN Security.	<input type="checkbox"/>
4b.	Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multifactor authentication (MFA) and log RDP login attempts.	<input type="checkbox"/>
5a.	Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the actions in 5b. and 5c. to protect their networks.	<input type="checkbox"/>
5b.	Disable SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on the part of existing systems or applications) that may break when disabled. <ul style="list-style-type: none"> <li>• <b>Note:</b> Remove dependencies through upgrades and reconfiguration. Upgrade to SMBv3 (or most current version), along with SMB signing.</li> </ul>	<input type="checkbox"/>
5c.	Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.	<input type="checkbox"/>

**Ransomware Infection Vector: Phishing**

1.	Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. Conduct organizationwide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.	<input type="checkbox"/>
2.	Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.	<input type="checkbox"/>
3.	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed sender policy framework and Domain Keys Identified Mail protocols, adding a reporting function that allows senders and receivers to improve and monitor the protection of the domain from fraudulent email.	<input type="checkbox"/>
4.	Consider disabling macro scripts for Microsoft Office files transmitted via email. These macros can be used to deliver ransomware.	<input type="checkbox"/>

**Ransomware Infection Vector: Precursor Malware Infection**

1a.	Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions. CISA recommends using a centrally managed antivirus solution. This enables the detection of both “precursor” malware and ransomware.	<input type="checkbox"/>
-----	--	--------------------------



1b.	A ransomware infection may be evidence of a previous, unresolved network compromise. For example, many ransomware infections result from existing malware infections, such as TrickBot, Dridex or Emotet.	<input type="checkbox"/>
1c.	In some cases, ransomware deployment is just the last step in a network compromise and is dropped as a way to obfuscate previous post-compromise activities.	<input type="checkbox"/>
2a.	Use the application directory to allow listing on all assets to ensure that only authorized software can run and all unauthorized software is blocked from execution.	<input type="checkbox"/>
2b.	Enable the application directory to allow listing through Microsoft Software Restriction Policy or AppLocker.	<input type="checkbox"/>
2c.	Use the directory to allow listing rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from PROGRAMFILES, PROGRAMFILES(X86) and SYSTEM32. Disallow all other locations unless an exception is granted.	<input type="checkbox"/>
3.	Consider implementing an intrusion detection system to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.	<input type="checkbox"/>

**Ransomware Infection Vector: Third Parties and Managed Service Providers**

1a.	Take into consideration the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting client organizations.	<input type="checkbox"/>
1b.	If a third party or MSP is responsible for maintaining and securing your organization’s backups, ensure they follow the applicable best practices outlined above. Using contract language to formalize your security requirements is a best practice.	<input type="checkbox"/>
2a.	Understand that adversaries may exploit the trusted relationships your organization has with third parties and MSPs. <a href="#">See</a> CISA’s APTs Targeting IT Service Provider Customers.	<input type="checkbox"/>
2b.	Adversaries may target MSPs with the goal of compromising MSP client organizations. They may use MSP network connections and access to client organizations as a key vector to propagate malware and ransomware.	<input type="checkbox"/>
2c.	Adversaries may spoof the identity of—or use compromised email accounts associated with—entities your organization has a trusted relationship with in order to phish your users, enabling network compromise and disclosure of information.	<input type="checkbox"/>

**General Best Practices and Hardening Guidance**

1a.	Employ MFA for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.	<input type="checkbox"/>
-----	--	--------------------------

1b.	If you are using passwords, use <a href="#">strong</a> passwords and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.	<input type="checkbox"/>
2a.	Apply the principle of least privilege to all systems and services so users only have the access they need to perform their jobs. Threat actors often seek out privileged accounts to leverage to help saturate networks with ransomware.	<input type="checkbox"/>
2b.	Restrict user permissions to install and run software applications.	<input type="checkbox"/>
2c.	Limit the ability of a local administrator account to log in from a local interactive session (e.g., “Deny access to this computer from the network”) and prevent access via an RDP session.	<input type="checkbox"/>
2d.	Remove unnecessary accounts and groups and restrict root access.	<input type="checkbox"/>
2e.	Control and limit local administration.	<input type="checkbox"/>
2f.	Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.	<input type="checkbox"/>
2g.	Audit user accounts regularly, particularly remote monitoring and management accounts that are publicly accessible. This includes audits of third-party access given to MSPs.	<input type="checkbox"/>
3.	<a href="#">Leverage</a> best practices and enable security settings in association with cloud environments, such as Microsoft Office 365.	<input type="checkbox"/>
4a.	Develop and regularly update a comprehensive network diagram that describes systems and data flows within your organization’s network (see Figure 1). This is useful in a steady state and can help incident responders understand where to focus their efforts.	<input type="checkbox"/>
4b.	The diagram should include depictions of covered major networks, any specific IP addressing schemes and the general network topology (including network connections, interdependencies and access granted to third parties or MSPs).	<input type="checkbox"/>
5a.	Employ logical or physical means of network segmentation to separate various business units or departmental IT resources within your organization and to maintain separation between IT and operational technology. This will help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. See Figures 2 and 3 for depictions of a flat (unsegmented) network and a best practice segmented network.	<input type="checkbox"/>
5b.	Network segmentation can be rendered ineffective if it is breached through user error or nonadherence to organizational policies (e.g., connecting removable storage media or other devices to multiple segments).	<input type="checkbox"/>
6a.	Ensure your organization has a comprehensive asset management approach.	<input type="checkbox"/>
6b.	Understand and inventory your organization’s IT assets, both logical (e.g., data, software) and physical (e.g., hardware).	<input type="checkbox"/>
6c.	Understand which data or systems are most critical for health and safety, revenue generation, or other critical services, as well as any associated interdependencies (i.e., “critical asset or system list”). This will aid your organization in determining restoration priorities should an incident occur.	<input type="checkbox"/>

	Apply more comprehensive security controls or safeguards to critical assets. This requires organizationwide coordination.	
6d.	Use the MS-ISAC Hardware and Software Asset Tracking <a href="#">Spreadsheet</a> .	<input type="checkbox"/>
7a.	Restrict usage of PowerShell, using Group Policy, to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows OSs should be permitted to use PowerShell. Update PowerShell and enable enhanced logging. PowerShell is a cross-platform, command-line, shell and scripting language that is a component of Microsoft Windows. Threat actors use PowerShell to deploy ransomware and hide their malicious activities.	<input type="checkbox"/>
7b.	Update PowerShell instances to version 5.0 or later and uninstall all earlier PowerShell versions. Logs from PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities. <ul style="list-style-type: none"> <li>• <b>Note:</b> PowerShell logs contain valuable data, including historical OS and registry interaction and possible tactics, techniques and procedures of a threat actor’s PowerShell use.</li> </ul>	<input type="checkbox"/>
7c.	Ensure PowerShell instances (use the most current version) have module, script block and transcription logging enabled (enhanced logging). <ul style="list-style-type: none"> <li>• <b>Note:</b> The two logs that record PowerShell activity are the “PowerShell” Windows Event Log and the “PowerShell Operational” Log. CISA recommends turning on these two Windows Event Logs with a retention period of 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs as large as possible.</li> </ul>	<input type="checkbox"/>
8a.	Secure domain controllers (DCs). Threat actors often target and use DCs as a staging point to spread ransomware network-wide. The following list contains high-level suggestions on how best to secure a DC: <ul style="list-style-type: none"> <li>• Ensure that DCs are regularly patched. This includes the application of critical patches as soon as possible.</li> <li>• Ensure the most current version of the Windows Server OS is being used on DCs. Security features are better integrated into newer versions of Windows Server OSs, including Active Directory security features. Use Active Directory configuration guides, such as those available from Microsoft, when configuring available security features.</li> <li>• Ensure that no additional software or agents are installed on DCs, as these can be leveraged to run arbitrary code on the system.</li> <li>• Access to DCs should be restricted to the administrators’ group. Users within this group should be limited and have separate accounts used for day-to-day operations with nonadministrative permissions.</li> <li>• DC host firewalls should be configured to prevent internet access. Usually, these systems do not have a valid need for direct internet access. Updated servers with internet connectivity can be used to pull necessary updates in lieu of allowing internet access for DCs.</li> </ul>	<input type="checkbox"/>
8b.	CISA recommends the following DC Group Policy settings (this is not an all-inclusive list, and further steps should be taken to secure DCs within the environment): <ul style="list-style-type: none"> <li>• The Kerberos default protocol is recommended for authentication, but if it is not used, enable NTLM auditing to ensure that only NTLMv2 responses are being sent across the</li> </ul>	<input type="checkbox"/>

	<p>network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible.</p> <ul style="list-style-type: none"> <li>• Enable additional protections for Local Security Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against the lsass.exe program to ensure an understanding of the programs that will be affected by the enabling of this protection.</li> <li>• Ensure that SMB signing is required between the hosts and the DCs to prevent the use of replay attacks on the network. SMB signing should be enforced throughout the entire domain as an added protection against these attacks elsewhere in the environment.</li> </ul>	
8c.	<p>Retain and adequately secure logs from both network devices and local hosts. This supports the triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred:</p> <ul style="list-style-type: none"> <li>• Set up centralized log management using a security information and event management tool. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact on the organization as a whole.</li> <li>• Maintain and back up logs for critical systems for a minimum of one year, if possible.</li> </ul>	<input type="checkbox"/>
9.	<p>Baseline and analyze network activity over a period of months to determine behavioral patterns so that normal, legitimate activity can be more easily distinguished from anomalous network activity (e.g., normal versus anomalous account activity). Business transaction logging—such as logging activity related to specific or critical applications—is another useful source of information for behavioral analytics.</p>	<input type="checkbox"/>

Source: CISA

# CHECKLIST | RANSOMWARE RESPONSE

Presented by ToughComp

Date:

Should your organization become a victim of ransomware, the Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends responding by using the following checklist.

Detection and Analysis		
1a.	Determine which systems were impacted and immediately isolate them.	<input type="checkbox"/>
1b.	If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.	<input type="checkbox"/>
1c.	If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.	<input type="checkbox"/>
1d.	<p>After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.</p> <ul style="list-style-type: none"><li>• <b>Note:</b> Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out only if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.</li></ul>	<input type="checkbox"/>
2.	Only in the event that you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.	<input type="checkbox"/>
3a.	Triage impacted systems for restoration and recovery.	<input type="checkbox"/>
3b.	<p>Identify and prioritize critical systems for restoration, and confirm the nature of data housed on impacted systems:</p> <ul style="list-style-type: none"><li>• Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation or other critical services, as well as systems they depend on.</li><li>• Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.</li></ul>	<input type="checkbox"/>

4.	Confer with your team to develop and document an initial understanding of what has occurred based on the initial analysis.	<input type="checkbox"/>
5a.	Engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to and recover from the incident.	<input type="checkbox"/>
5b.	Share the information you have at your disposal to receive the most timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders.	<input type="checkbox"/>
6a.	Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, collect any relevant logs and samples of any “precursor” malware binaries and associated observables or indicators of compromise (e.g., suspected command and control Internet Protocol (IP) addresses, suspicious registry entries or other relevant files detected). The contacts below may be able to assist you in performing these tasks.	<input type="checkbox"/>
6b.	Take care to preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).	<input type="checkbox"/>
7.	Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.	<input type="checkbox"/>
8a.	Research the trusted guidance (i.e., published by sources such as government, MS-ISAC, reputable security vendor, etc.) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.	<input type="checkbox"/>
8b.	Disable the execution of known ransomware binaries. This will minimize damage and impact on your systems. Delete other known associated registry values and files.	<input type="checkbox"/>
9.	Identify the systems and accounts involved in the initial breach. This can include email accounts.	<input type="checkbox"/>
10.	Based on the breach or compromise details determined above, contain any associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration. Securing the network and other information sources from continued credential-based unauthorized access may include disabling virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.	<input type="checkbox"/>
11.	<p>In the event you learn server-side data is being encrypted by an infected workstation, quick identification steps are to:</p> <ul style="list-style-type: none"> <li>• Review Computer Management &gt; Sessions and Open Files lists on associated servers to determine the user or system accessing those files.</li> <li>• Review file properties of encrypted files or ransom notes to identify specific users who may be associated with file ownership.</li> <li>• Review the TerminalServices-RemoteConnectionManager event log to check for successful remote desktop protocol (RDP) network connections.</li> <li>• Review the Windows Security log, server message block (SMB) event logs and any related logs that may identify significant authentication or access events.</li> <li>• Run Wireshark on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., “smb2.filename contains cryptxxx”).</li> </ul>	<input type="checkbox"/>
12a.	Conduct an examination of existing organizational detection or prevention systems (e.g., antivirus, Endpoint Detection & Response, IDS, Intrusion Prevention System) and logs. Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.	<input type="checkbox"/>

12b.	<p>Look for evidence of precursor “dropper” malware. A ransomware event may be evidence of a previous, unresolved network compromise. Many ransomware infections are the result of existing malware infections such as TrickBot, Dridex or Emotet:</p> <ul style="list-style-type: none"> <li>• Operators of these advanced malware variants will often sell access to a network. Malicious actors will sometimes use this access to exfiltrate data and then threaten to release the data publicly before ransoming the network in an attempt to further extort the victim and pressure them into paying.</li> <li>• Malicious actors often drop manually deployed ransomware variants on a network to obfuscate their post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromise.</li> </ul>	<input type="checkbox"/>
13a.	Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.	<input type="checkbox"/>
13b.	Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc.	<input type="checkbox"/>
13c.	Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use of PowerShell scripts).	<input type="checkbox"/>
13d.	Identification may involve the deployment of endpoint detection and response solutions, audits of local and domain accounts, examination of data found in centralized logging systems or deeper forensic analysis of specific systems once movement within the environment has been mapped out.	<input type="checkbox"/>
14.	Rebuild systems based on a prioritization of critical services (e.g., health and safety or revenue-generating services), using preconfigured standard images, if possible.	<input type="checkbox"/>
15.	Once the environment has been fully cleaned and rebuilt (including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms), issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility. This can include applying patches, upgrading software and taking other security precautions not previously taken.	<input type="checkbox"/>
16.	Based on established criteria, which may include taking the steps above or seeking outside assistance, the designated IT or IT security authority declares the ransomware incident over.	<input type="checkbox"/>
17a.	Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.	<input type="checkbox"/>
17b.	Take care not to reinfect clean systems during recovery. For example, if a new Virtual Local Area Network has been created for recovery purposes, ensure only clean systems are added to it.	<input type="checkbox"/>
18.	Document lessons learned from the incident and associated response activities to inform updates to—and refine—organizational policies, plans and procedures and guide future exercises of the same type of incident.	<input type="checkbox"/>
19.	Consider sharing lessons learned and relevant indicators of compromise with CISA.	<input type="checkbox"/>

Source: CISA



# CYBER RISKS & LIABILITIES

## Ransomware Considerations for Board Members

Organizations of all sizes and sectors are facing increased cybersecurity risks. Specifically, ransomware attacks—which leverage malware to compromise a victim’s data and demand them to make a large payment to recover it—have quickly become a rising threat across industry lines.

In fact, recent research found that these types of attacks have surged by 150% in the past year alone, with the average amount paid by victims jumping by over 300%. Such attacks have also become more sophisticated over the years as cybercriminals have developed a wide range of different ransomware-use techniques.

In light of these advancing cyber concerns, it’s important for board members to be actively involved in developing and promoting effective workplace cybersecurity measures—especially as it pertains to ransomware attacks. By involving senior leadership in such initiatives, organizations can foster a culture of cybersecurity awareness and bolster their preparedness against cyberthreats.

Here are five key questions that board members should discuss to help their organizations stay resilient against ransomware attacks.

### 1. How can our organization better detect ransomware threats?

Before a ransomware attack can occur, a cybercriminal has to gain access to their target’s network, systems or data. Once a cybercriminal gains this access, an extended length of time—also known as “dwell time”—typically passes before the ransomware is deployed and the attack actually begins.

With this in mind, organizations that are able to detect potential ransomware threats during dwell time rather than at the onset of an attack can stop such incidents before they even start. The following measures can help

board members ensure the earliest possible detection of ransomware concerns within their organizations:

- Keep updated records of all workplace technology to understand where ransomware threats could arise.
- Equip all workplace technology with antivirus and malware detection software. Update this software regularly.
- Have critical technology, systems and data consistently monitored for suspicious activity. Make sure the employees in charge of these monitoring procedures are properly trained to do so.
- Establish thresholds for when employees should notify senior leadership of ransomware threats.
- Provide all employees with clear ransomware reporting protocols.

### 2. What can our organization do to minimize the damages in the event of a ransomware attack?

When ransomware attacks occur, it’s vital for impacted organizations to do everything they can to limit the damages. In particular, board members should prioritize these procedures:

- Keep data encrypted. This practice will make it significantly harder for cybercriminals to compromise data during a ransomware attack.
- Restrict employee access to workplace technology, systems and data. Only allow access on an as-needed basis.
- Require employees to use proper credentials and multifactor authentication when accessing workplace technology, systems and data.

# CYBER RISKS & LIABILITIES

- Consider keeping different workplace networks separated to prevent cybercriminals from gaining full access after attacking a single network.

### 3. Does our organization have an effective cyber incident response plan in place?

Cyber incident response plans are one of the best tools for helping organizations react appropriately and mitigate losses amid cyberattacks. Board members should work closely with workplace leaders across departments to develop sufficient cyber incident response plans for their organizations. Generally speaking, an effective cyber incident response plan should outline:

- Who is part of the cyber incident response team (e.g., board members, department leaders, IT professionals, legal experts and HR specialists)
- What roles and responsibilities each member of the cyber incident response team must uphold during an attack
- What the organization's key functions are and how these operations will continue throughout an attack
- How any critical workplace decisions will be made during an attack
- When and how stakeholders should be informed of an attack (e.g., employees, customers, shareholders and suppliers)
- What federal, state and local regulations the organization must follow when responding to an attack (e.g., incident reporting protocols)
- When and how the organization should seek assistance from additional parties to help recover from an attack (e.g., law enforcement and insurance professionals)

Take note that cyber incident response plans should be evaluated and updated regularly to ensure effectiveness. Various activities can be implemented to assess cyber incident response plans—including tabletop exercises and penetration testing.

### 4. Does our organization's cyber incident response plan adequately address ransomware attacks?

Cyber incident response plans should address a wide range of possible attack circumstances. That being said, it's important for board members to ensure that ransomware attack scenarios are properly accounted for within their cyber incident response plans.

Specifically, board members must determine whether or not their organizations will make ransom payments to cybercriminals—particularly when the compromised data is sensitive in nature or critical to operations. Keep in mind that cybersecurity experts typically advise against complying with ransom demands, seeing as there is a chance that cybercriminals could take the ransom money and not recover the compromised data or leverage it in future attacks.

Further, board members must ensure their organizations are prepared for the lengthy recovery process that often accompanies ransomware attacks. In some cases, it can take several weeks or months to recover compromised data. During this time, board members must have plans for keeping their organizations functional and minimizing reputational damages.

### 5. Are all data backup protocols within our organization sufficient to protect against ransomware threats?

Backing up important data can help organizations maintain access to key files and information during cyber incidents. However, poor data backup protocols can easily be exploited by cybercriminals, subsequently resulting in ransomware attacks. As a result, board members should ensure their organizations follow these data backup security procedures:

- Conduct data backups on a routine schedule. Consider backing up critical data more frequently.
- Store data backups offline and in a separate location from other workplace systems and networks.
- Only allow trusted and qualified employees to perform data backups.

For more risk management guidance, contact us today.

# CYBER RISKS & LIABILITIES

## Ransomware-as-a-Service Explained

Ransomware attacks—which entail a cybercriminal deploying malicious software to compromise a device (or multiple devices) and demand a large payment be made before restoring the technology for the victim—have become a significant concern for organizations across industry lines. In fact, the latest research provides that these attacks have increased by nearly 140% in the past year alone, with the median ransom payment demand totaling \$178,000 and the average overall loss from such an attack exceeding \$1 million.

A key contributor to this surge is the recent debut of Ransomware-as-a-Service (RaaS). Put simply, RaaS refers to a dark web business model that permits sophisticated cybercriminals to sell their ransomware software to willing buyers (usually less skilled cybercriminals), who then utilize the software to launch an attack and secure a ransom payment.

The RaaS model poses a serious threat to organizations of all sizes and sectors, as it allows cybercriminals of any skill level to execute ransomware attacks on their targets. Review the following guidance to learn more about the RaaS model, its impact on organizational cybersecurity and best practices for addressing RaaS concerns.

### What Is RaaS?

Although its purpose is to sell a harmful product, the RaaS model operates quite similarly to a normal business model. First, knowledgeable ransomware developers generate malicious software to be sold. In order to be attractive to buyers, this software must carry a high likelihood of penetration and a minimal risk of discovery.

Once the software has been created and is ready for distribution, it gets launched as a multi-end user

infrastructure. RaaS developers then seek potential customers by using typical business marketing methods throughout the dark web—such as advertisements and online forums. Some developers are more selective in who they offer their software to, requiring customers to demonstrate certain technological skills or cybersecurity knowledge, while others are not as strict.

When RaaS developers secure buyers, these customers are usually provided with access to not only the ransomware software itself, but some form of a product portal as well. This portal may include detailed instructions for software implementation, user reviews, support forums and special discounts or offers for future purchases from the developer. Customers may receive permanent access to the software they buy, or only be given an allotted amount of time to utilize it—similar to a rental agreement.

Depending on the developer, RaaS purchases can be a one-time sale or a monthly subscription service. In some cases, RaaS developers don't actually sell their software, but rather recruit other cybercriminals who are willing to launch attacks using the developers' software in exchange for a percentage of the resulting ransom payment. This commission-based partnership is also known as an affiliate program.

Regardless of whether RaaS developers have customers or affiliates, once these cybercriminals receive the developers' software, they can use it to execute ransomware attacks on their targets—potentially resulting in widespread disruption, damaged or destroyed data, reputational repercussions and significant financial fallout for the affected organizations. Well-known RaaS incidents include WannaCry, Cerber, MacRansom, Philadelphia, Atom, Hostman and FLUX.

# CYBER RISKS & LIABILITIES

## The Impact of RaaS

Prior to the emergence of RaaS, cybercriminals needed to possess extensive software knowledge and coding capabilities in order to pull off a ransomware attack. In other words, only the most sophisticated cybercriminals could successfully launch such attacks and obtain ransom payments from their victims.

However, the introduction of RaaS to the dark web has allowed cybercriminals of practically any skill level and very little technical ability to accomplish this feat with a simple purchase—contributing to a rapid increase in the frequency of ransomware attacks as a whole.

In addition to attack frequency, cybercriminals involved in RaaS models have become more confident in the strength of their malicious software—thus motivating them to ramp up their ransom payment demands. This is particularly true in the scope of RaaS affiliate programs. Because affiliates only receive a portion of the overall ransom payment following an attack, an elevated payment demand provides them with a larger profit.

That being said, the RaaS model has played a major role in increasing both the frequency and cost of ransomware events in recent years, compounding the expected consequences that affected organizations will face for an already severely damaging form of attack.

## Addressing RaaS Concerns

The best way to minimize the growing threat of RaaS concerns at your organization is to make ransomware prevention and response measures a top priority. Remember that ransomware attacks are commonly deployed via phishing emails, deceptive links, dangerous websites, harmful attachments and malicious programs. With this in mind, here are some best practices for combatting ransomware attacks:

- **Secure your systems**—First, it's important to take steps to protect your organizational IT infrastructure from potential ransomware exposures. This may entail:
  - Using a virtual private network (VPN) for all internet-based activities (e.g., browsing and sending emails)
  - Installing antivirus software on all workplace technology
  - Implementing a firewall to block cybercriminals from accessing your organization's VPN
  - Restricting employees' access to websites that aren't secure
  - Establishing email filters to keep phishing messages from reaching employees' inboxes
  - Encrypting sensitive data on all organizational devices and routinely backing up this information
  - Limiting which employees receive administrative controls to prevent inexperienced staff from mistakenly downloading a malicious program
  - Regularly updating all organizational devices and security programs to ensure effectiveness
  - Developing a cyber incident response plan that adequately considers ransomware scenarios and practicing this plan with staff
- **Educate your employees**—Next, be sure to train your employees on how to prevent and respond to a ransomware attack. Give your staff these tips:
  - Avoid opening or responding to emails from individuals or organizations you don't know. If an email claims to be from a trusted source, be sure to verify their identity by double-checking the address.
  - Never click on suspicious links or pop-ups—whether they're in an email or on a website. Similarly, avoid downloading attachments or software programs from unknown sources or locations.
  - Only browse safe and secure websites on organizational devices. Refrain from using workplace devices for personal browsing.
  - If you suspect a ransomware attack, contact your manager or the IT department immediately for further guidance.

For additional risk management guidance and insurance solutions, contact us today.

# CYBER RISKS & LIABILITIES

## Double Extortion Ransomware Attacks

In recent years, ransomware attacks have steadily been on the rise. These incidents—which entail cybercriminals compromising a device or server and demanding a large payment be made before restoring the technology (as well as any data stored on it) for the victim—are one of the most damaging cyberattack methods, incurring an average of \$1 million in total losses per incident.

As these attacks become increasingly common, numerous ransomware techniques have also emerged. Specifically, double extortion ransomware attacks are now a potential cybersecurity concern for organizations across industry lines. This technique follows a similar protocol to that of a typical ransomware attack, but comes with an extra threat—the victim must pay a ransom not only to regain access to their technology and data, but also to keep that data from being uploaded publicly online.

Double extortion ransomware attacks are particularly concerning, seeing as these incidents can further pressure organizations to comply with ransom demands in order to keep their data private. Review the following guidance to learn more about how double extortion ransomware attacks work and what your organization can do to prevent such an attack.

### How Double Extortion Ransomware Attacks Work

To outline the general framework of a double extortion ransomware attack, this technique starts out like most other ransomware incidents, in which a cybercriminal first gains access to their target's device or server—often via phishing scams, nonsecure websites or malicious attachments. From there, the cybercriminal is able to compromise the victim's technology and encrypt data stored on it. Then, the cybercriminal delivers their ransom demand and accompanying consequences for noncompliance.

Contrary to a typical ransomware incident, however, these consequences are twofold. That is, failing to pay the ransom could result in the cybercriminal both permanently restricting the victim's access to their technology and sensitive data, as well as sharing this data publicly on the internet. Although double extortion ransomware attacks can occur at any organization, these incidents are most common within establishments that store a considerable amount of sensitive data. This includes health care facilities, financial institutions, government organizations and large retail businesses.

Double extortion ransomware attacks can be significantly more damaging for affected organizations than typical ransomware incidents. This is because even if organizations have protocols in place (e.g., storing data in multiple secure locations) that allow them to recover their compromised information without paying a ransom, they may still be pressured to do so in order to keep their data from going public. After all, a data breach can lead to further ramifications—including reputational damages, regulatory fines and class action lawsuits.

What's more, cybercriminals who conduct double extortion ransomware attacks are known to demand higher ransom payments, sell or trade stolen data to other attackers for future extortion attempts and still move forward with sharing data publicly even after the ransom is paid (whether on purpose or by accident)—making these attacks all the more damaging.

### Preventing Double Extortion Ransomware Attacks

When it comes to combatting double extortion ransomware attacks, it's important to prioritize standard ransomware prevention measures. This includes conducting routine employee training on how to detect potential ransomware risks (e.g., suspicious emails or attachments), implementing policies that prohibit



# CYBER RISKS & LIABILITIES

browsing nonsecure websites on organizational servers or devices, and installing adequate security features on all workplace technology (e.g., a virtual private network, antivirus programs, data encryption software, email spam filters, an internet firewall and a patch management system).

In addition to these key prevention measures, the best course of action for reducing double extortion ransomware attack risks is to establish an effective cyber incident response plan for your organization. This plan should explicitly address double extortion ransomware attack scenarios and outline steps that employees should take to limit the damages during such an event.

Lastly, it's vital to secure appropriate insurance coverage for ultimate peace of mind in the event of a ransomware attack. A dedicated cyber insurance policy can offer much-needed support and resources when an attack occurs, minimizing the potential damages and financial impact on your organization.

For additional risk management guidance and insurance solutions, contact us today.



# CYBER RISKS & LIABILITIES

## Preventing Ransomware Exposures From Remote Desk Protocol

Remote desk protocol (RDP)—which is a network communications protocol developed by Microsoft—consists of a digital interface that allows users to connect remotely to other servers or devices. Through RDP ports, users can easily access and operate these servers or devices from any location. RDP has become an increasingly useful business tool—permitting employees to retrieve files and applications stored on their organization's network while working from home, as well as giving IT departments the ability to identify and fix employees' technical problems remotely.

Unfortunately, RDP ports are also frequently being leveraged as a vector for launching ransomware attacks, which entail a cybercriminal deploying malicious software to compromise a device (or multiple devices) and demand a large payment be made before restoring the technology for the victim. In fact, a recent report from Kaspersky found that nearly 1.3 million RDP-based cyberattacks occur each day, with RDP reigning as the top attack vector for ransomware incidents.

Don't let RDP contribute to a costly ransomware incident for your organization. Review the following guidance to learn more about how ransomware attacks can occur via RDP and best practices for minimizing the likelihood of such an incident.

### Ransomware Attacks via RDP

RDP-based ransomware attacks usually stem from organizations leaving their RDP ports exposed to the internet. Although doing so can seem more convenient for employers in the scope of remote work operations, internet-exposed RDP ports are easy for cybercriminals to identify and offer a clear access point for deploying harmful attacks.

The typical process of an RDP-based ransomware attack is as follows:

1. **Scanning**—First, a cybercriminal utilizes a port-scanning tool to search the internet for any exposed RDP ports. These scanning tools are often free and relatively simple to operate for attackers of varying skill levels.
2. **Gaining access**—After identifying an exposed RDP port, the cybercriminal then gains access to the targeted server or device by using stolen credentials. Attackers can secure these credentials by either purchasing them on the dark web or implementing a brute-force tool that can rapidly input a series of usernames and passwords until the correct combination is found.
3. **Disabling security features**—Once the cybercriminal has accessed the targeted server or device, they attempt to make it as defenseless against an attack as possible by disabling any existing security features (e.g., antivirus software, data encryption tools and system backup capabilities).
4. **Executing the attack**—From there, the cybercriminal is able to steal sensitive data and deploy a ransomware attack on a vulnerable server or device. Some attackers even install backdoors during this step to allow for easy access during future attacks.

Like other ransomware incidents, RDP-based attacks can result in devastating ramifications for the impacted organization—including business interruption issues, reputational damages and large-scale financial loss.

# CYBER RISKS & LIABILITIES

## Strengthening RDP Against Ransomware

Although RDP-based ransomware attacks have become increasingly common, there are several ways for you to bolster your organization's RDP security and lessen the risk of such an incident impacting your operations.

Consider the following best practices:

- **Close your RDP connection.** First and foremost, ensure that your RDP connection is not open to the internet.
- **Establish a virtual private network (VPN).** To keep your RDP port from being exposed to the internet, be sure to establish a VPN. This will allow remote employees to securely access your organization's RDP port, while also making the port far more difficult for cybercriminals to locate online.
- **Elevate authentication protocols.** Because cybercriminals require login credentials to properly execute an RDP-based ransomware attack, make sure you have effective user authentication protocols in place. Specifically, encourage employees to develop unique passwords for all of their devices and accounts. These passwords should be an appropriate length, refrain from using common words or phrases, and contain several special characters. In addition to strong passwords, consider requiring multifactor authentication for RDP port access as an extra layer of protection.
- **Implement login attempt limits.** To stop cybercriminals from being able to deploy brute-force tools to secure login credentials during an attack, update RDP port protection features to detect when multiple failed login attempts have occurred in a short period of time. Establish a limit on how many incorrect logins can occur before the user is blocked from further attempts—therefore halting an attack.
- **Utilize adequate security software.** Ensure all workplace technology is equipped with top-rated security software—including antivirus programs, a firewall, data encryption features and a gateway server—to deter attempted attacks. Update this software on a regular basis.
- **Restrict employee access.** Be sure to uphold the principle of least privilege by only providing

employees with RDP access if they absolutely need it to conduct their work tasks. These employees should be trusted and trained in appropriate RDP usage. After all, granting extra employees unnecessary RDP permissions simply creates additional security gaps.

- **Have a plan.** Lastly, make sure your organization has an effective cyber incident response plan in place that addresses RDP-based ransomware attack scenarios. This plan should promote the backup storage of any critical data in multiple secure locations (both on-site and off-site) to minimize potential losses. Practice this plan regularly with staff and make updates as needed.

For additional risk management guidance and insurance solutions, contact us today.

---

# CYBER RISKS & LIABILITIES

## Endpoint Detection and Response Explained

Endpoint detection and response (EDR) is a cybersecurity solution that continuously monitors security-related threat information and endpoint data to detect and respond to ransomware and other kinds of malware. It provides visibility into security incidents occurring on endpoints—such as mobile devices, desktop computers, laptops, embedded devices and servers—to prevent damage and future attacks. This article discusses the importance of EDR solutions, how they work and the types of threats they can detect.

### The Importance of EDR Solutions

According to the Identity Theft Resource Center, nearly 294 million people were impacted by 1,682 data breaches at U.S. corporations in 2021. As cyberthreats grow more sophisticated and frequent, and remote work more common, these advanced attacks have become more difficult to identify in real time. Therefore, it's important for organizations to prioritize cybersecurity measures that can deflect, analyze and respond to the constant barrage of cyberattacks. EDR solutions can provide a number of features that improve an organization's cybersecurity risk management, including:

- **Improved visibility**—EDR solutions continuously collect data and analytics before compiling them into a single, centralized system. These insights can give security teams full visibility into the state of a network's endpoints from a single console.
- **Rapid investigations**—Since EDR solutions automate data collection and processing, security teams can gain rapid context regarding incidents and take steps to quickly remediate them.
- **Remediation automation**—Security teams can allow EDR solutions to automatically perform

certain incident response activities based on predefined rules, enabling them to block or rapidly remediate incidents.

- **Contextualized threat hunting**—The continuous data collection and analysis provided by EDR solutions can allow threat hunters to identify and investigate potential signs of an existing issue.

### How Do EDR Solutions Work?

EDR solutions offer advanced threat detection, investigation and response capabilities—including incident data search and investigation triage, suspicious activity validation, threat hunting, and malicious activity detection and containment—by constantly analyzing events from endpoints to identify suspicious activity. These tools provide continuous and comprehensive visibility into what is happening in real time by recording activities and events taking place on endpoints and all workloads. By generating alerts, security teams can uncover, investigate and remediate issues. The primary functions of an EDR security system include:

- Monitoring endpoints and collecting activity data
- Analyzing data to identify threat patterns
- Using behavioral analysis to detect anomalies
- Removing or containing identified threats
- Notifying security personnel
- Researching identified threats and searching for suspicious activities

Overall, EDR solutions can be used to shorten response times for incident response teams and eliminate threats before damage is done.

# CYBER RISKS & LIABILITIES

## What Types of Threats Do EDR Solutions Detect?

EDR is an integral part of an organization's complete information security posture. It can detect the following threats to a network:

- Malware, including spyware, ransomware, viruses and bots
- Misuse of legitimate applications
- Stolen user credentials
- Suspicious user activity and behavior
- Fileless attacks during which malicious software is not installed and therefore more likely to be missed by antivirus tools

## Conclusion

EDR solutions are helpful in protecting both the enterprise and the user while also adding value to a company's integrated approach to cybersecurity. Furthermore, they are frequently required by insurance underwriters in order to obtain cyber insurance. For more risk management guidance, contact us today.

---

# CYBER RISKS & LIABILITIES

## Extended Detection and Response Explained

Extended detection and response (XDR) is a security solution that offers organizations end-to-end visibility, detection, investigation and response across multiple security layers. Unlike endpoint detection and response (EDR), XDR provides a holistic view of threats across the entire technology landscape rather than only those within managed endpoints. This article explains what XDR is and how it works, outlines the benefits of XDR and discusses how it compares to EDR.

### What Is XDR and How Does It Work?

XDR uses data collected across multiple security layers to provide IT and security teams with real-time, actionable threat information. By utilizing extended visibility, analysis and response across endpoints, workloads, users and networks, XDR can help organizations reduce blind spots, detect threats faster and jump-start threat remediation. Essentially, XDR helps security teams:

- Recognize advanced and hidden threats
- Detect and follow threats in and across various systems
- Improve the time it takes to detect and respond to threats
- Improve the threat investigation process

There are several components of XDR that provide organizations with a wider grasp of threats via the following:

- **An analysis of internal and external traffic**—XDR can identify cybersecurity threats even after they've bypassed system perimeters.
- **Integrated threat intelligence**—XDR learns from attacks on other systems to detect similar events in its own environment.

- **Machine learning-based detection**—XDR can detect zero-day and nontraditional threats that bypass signature-based methods.

### The Benefits of XDR

XDR adds value to organizations by combining multiple security offerings into one incident detection and response product. Benefits of XDR include:

- **Greater visibility and context**—Threats that utilize legitimate software, ports and protocols can often slip past system defenses undetected. With XDR, security analysts can see threats on any security layer. It can also offer insights into how an attack happened, who was affected and how it spread.
- **Improved prioritization**—As cyberthreats become increasingly frequent, it can be difficult for IT and security teams to keep up with security alerts. XDR can help prioritize threats by grouping related alerts across the framework and presenting the most important ones.
- **Enhanced automation**—XDR's automation abilities allow IT teams to handle a large volume of data and consistently execute complex processes.
- **Faster detection and response**—Since XDR is continuously monitoring the technology landscape, it enables organizations to detect and respond to threats faster than before.
- **More sophisticated responses**—XDR can tailor specific systematic responses and leverage other control points to minimize the overall impact of the affected endpoint.

# CYBER RISKS & LIABILITIES

## **How Does XDR Compare to EDR?**

XDR is an evolution of EDR—a cybersecurity solution that continuously monitors security-related threat information and endpoint data to detect and respond to ransomware and other types of malware. However, EDR can only detect and respond to threats inside managed endpoints, which limits the scope of threats that can be detected. In contrast, XDR goes beyond the capabilities of EDR by analyzing all security layers and offering organizations a more holistic view of threats.

## **Conclusion**

In an increasingly complex threat landscape, XDR solutions can provide organizations with flexible and efficient security enforcement and remediation. For more risk management guidance, contact us today.

---



# CYBER RISKS & LIABILITIES\_

## Patch Management Explained

Patch management is the process of acquiring and applying software updates to a variety of endpoints, including mobile devices, computers, servers and embedded devices. Installing patches regularly is necessary to correct errors, help protect data and optimize system functions. This article provides information on how a consistent approach to patching and updating software can limit exposure to various exploits.

### What Are Patches?

Patches modify operating systems and software to improve security, fix bugs and improve performance. They are created by software developers and address vulnerabilities attackers may target.

### Why Is Patch Management Necessary?

Patch management is necessary for the following reasons:

- **Security**—Hackers look to exploit cybersecurity weaknesses. Installing patches fixes software vulnerabilities and therefore reduces an organization's cybersecurity risks.
- **Compliance**—Regulatory bodies or government agencies may require organizations to adhere to patch management standards. Meeting those requirements can help businesses avoid sanctions, fines or penalties.
- **Feature improvements**—In addition to addressing security issues and fixing bugs, patches can also offer feature and functionality improvements to help software run smoothly
- **Minimize downtime**—With the enhancements that patches provide, programs may run more efficiently.

This can increase production by helping minimize downtime and improving the user experience.

### How Is Patch Management Performed?

The patch management process can be carried out by a company's IT team, an automated patch management tool or a combination of both. Steps in the patch management process include:

- **Identifying IT assets (inventory) and their locations**—Taking stock of IT assets and where they are located is a crucial first step in the patch management process. This is especially important as employees increasingly work remotely.
- **Identifying critical systems and vulnerabilities**—Being aware of critical systems and identifying and tracking vulnerabilities are also key aspects of patch management. It is important to take note of existing security features (e.g., firewalls and antivirus software) and what they are protecting against. With this information, an IT team can more readily determine which systems need to be patched when vulnerabilities are discovered or reported.
- **Testing and applying patches**—Before applying the patches to all systems, it is best to test them on a representative subset of IT inventory. This can help ensure the updates will not create unforeseen issues. Once testing is complete, begin rolling out the patches to the rest of the assets. It is advisable to do this in batches, as this can help identify potential issues before they become too widespread.

# CYBER RISKS & LIABILITIES\_

- **Tracking progress and maintaining records**—During the rollout, it is advisable to keep track of the progress being made. After the patches have been successfully installed, it is essential to keep accurate documentation that notes which assets have been updated.

## **Conclusion**

Having a comprehensive patch management process not only increases a company's cybersecurity posture and helps keep the business running smoothly, but it also is a practice frequently required by insurance underwriters in order to obtain cyber insurance. Contact us today for more information.

---



# COVERAGE INSIGHTS

## Common Components of a Cyber Insurance Policy

In recent years, organizations of all sizes and sectors have become increasingly reliant on workplace technology and digital systems to conduct their operations. Nevertheless, utilizing such technology carries additional exposures and liabilities. That's why it's crucial to secure adequate cyber coverage.

Having a cyber insurance policy in place can provide protection against financial losses that may result from a range of cyber incidents, including data breaches, ransomware attacks and phishing scams. Especially as these kinds of incidents continue to surge in both cost and frequency, organizations simply can't afford to ignore the importance of cyber coverage.

Specific cyber insurance offerings differ between carriers. Furthermore, organizations' coverage needs may vary based on their particular exposures. In any case, cyber insurance agreements typically fall into two categories—first-party coverage and third-party coverage. It's best for policyholders to have a clear understanding of both categories of coverage in order to comprehend the key protections offered by their cyber insurance. This article outlines the primary components of a cyber insurance policy.

### First-party Coverage

First-party cyber insurance can offer protection for losses that an organization directly sustains from a cyber incident. Types of first-party coverage include:

- **Incident response costs**—This coverage can help pay the costs associated with responding to a cyber incident. These costs may include

utilizing IT forensics, hiring external services and restoring damaged systems.

- **Data recovery costs**—Such coverage can help recover expenses related to reconstituting data that may have been deleted or corrupted during a cyber incident.
- **Business interruption loss**—This coverage can help reimburse lost profits or additional costs incurred due to the unavailability of IT systems or critical data amid a cyber incident.
- **Contingent business interruption loss**—Such coverage can assist with expenses stemming from business interruptions caused by a third-party cyber incident (e.g., a supplier, vendor or utility).
- **Cyber extortion**—This coverage can help pay costs associated with hiring extortion response specialists to evaluate recovery options and negotiate ransom payment demands (if applicable) during a cyber incident.
- **Reputational damage**—Such coverage can help recover lost revenue related to higher customer churn rates and reduced sales resulting from poor publicity following a cyber incident.
- **Financial theft and fraud**—This coverage can help reimburse direct financial losses stemming from the use of workplace technology to commit fraud or theft of securities, money or other property.



- **Physical asset damage**—Such coverage can assist with expenses resulting from the destruction of hardware or other physical property due to a cyber incident.

### Third-party Coverage

Third-party cyber insurance can provide protection for claims made, fines incurred or legal action taken against an organization due to a cyber incident.

Types of third-party coverage include:

- **Data privacy liability**—This coverage can help recover the costs of dealing with third-party individuals who had their information compromised during a cyber incident. These costs include notifying impacted individuals, offering credit-watch services and providing additional compensation.
- **Regulatory defense**—Such coverage can help pay fines, penalties and other defense costs related to regulatory action or privacy law violations stemming from a cyber incident.
- **Multimedia liability**—This coverage can help reimburse defense costs and civil damages resulting from defamation, libel, slander and negligence allegations associated with the publication of content in electronic or print media. Multimedia liability coverage can also offer protection amid copyright, trademark or intellectual property infringement incidents.
- **Network liability**—Such coverage can help recover expenses related to third-party liability concerns that may arise from a cyber incident affecting IT networks. Network liability coverage can also provide protection in the event that cybercriminals pass through IT networks to attack other parties (e.g., customers, investors or suppliers).
- **Technology errors and omissions liability**—This coverage can reimburse costs associated with third-party claims alleging technical service or product failures, including claims filed in response to a cyber incident.

### For More Information

Overall, it's evident that cyber insurance has become increasingly vital for organizations across industry lines. By securing proper coverage and understanding the key elements of their policies, organizations can stay properly protected against various cyberthreats.

For additional insurance guidance and solutions, contact us today.

**WORKERS COMPENSATION**  
Non Renewed?  
High Premiums?  
State Fund?  
**(212) 390-8772**  
info@toughcomp.com  
**TOUGHCOMP**  
BEFORE THE LAST REPORT  
www.toughcomp.com