# 20 Steps to Prevent a **Ransomware Nightmare**

The phrase “ransomware” conjures all sorts of terrifying associations—from networks being locked down by a shadowy organization to hackers breaking encryption protocols to infiltrate your computer.

**The threat looms even larger for big networks or organizational IT systems. Ransomware attacks can shut down network access, block internal operations, and seriously damage a company’s reputation. Attacks like those launched last year against Colonial Pipeline and Kaseya have shown that no company is safe. The Colonial Pipeline attack cost the company $4.4 million (some of which was recovered), while the Kaseya attackers initially demanded $70 million.**

**Organizations must invest time and effort in training employees on the safe use of corporate software, implement reliable security and data storage systems, and maintain flexible network configuration tools.**

## WHAT IS RANSOMWARE?

Ransomware is a malware created with the purpose of locking down a system and exacting a ransom from the person or company in order to re-gain access to the system. This malware works by hacking the network and cryptographic processes, resulting in the most important files being locked and encrypted so that further system operation is paralyzed.

Unfortunately for end users, as computer technology has increased, so too have the power of tools used by these malicious actors. When ransomware first appeared, symmetric encryption mechanisms were used, for which decrypting tools worked quite well. Modern malicious programs use asymmetric encryption methods, so decryption becomes very difficult.

The success of individual ransomware has led to this attack technology being adopted by hacker groups around the world. Ransomware is offered as a service (RaaS) available for ordering on the dark web. Ransomware has also found its way into the arsenal of groups employing the “advanced persistent threat” (APT) attack, which targets the network infrastructure of companies. The APT technique involves a variety of covert attacks, most of which are not easy to detect right away. The minimum period for their detection is usually one to two weeks, and during this time cybercriminals can cause serious damage.


Colonial Pipline Network

The situation is complicated by the fact that modern ransomware increasingly has the ability to access and distribute sensitive network data before it is encrypted by the computer. Thus, attackers can also threaten an organization with the disclosure of data. As a result, the organization is exposed to the risk of a double extortion attack, as hackers may return demanding more data and threatening the release of what they have already stolen.

## HOW RANSOMWARE WORKS

Ransomware, like any other malware, breaks into networks using traditional types of infiltration:

- Emails and messages in instant messengers with suspicious links, social engineering methods (baiting, honey traps, scareware), phishing, and malicious sites.
- Software and remote desktop protocol vulnerabilities. With the transition to remote work and reliance on remote desktop software, the number of malicious emails jumped by 600% in the first few months of the pandemic alone.[1] Similarly, as organizations move to hybrid set-ups or cloud storage systems, vulnerabilities associated with the cloud are being exposed.

Without the use of a network segmentation policy (more on this below), attackers are free to roam the network, infecting endpoints and servers, and to demand a ransom for regaining access to data.

Email attacks, which allow ransomware to enter a network, are difficult to stop. Attackers can trick even experienced users into clicking on an expected link (such as a financial report) or on a photo purporting to come from someone employees know. It may even be a document that appears to have been forwarded by the boss. These could be emails sent to millions of potential victims, or targeted messages to a specific person in a specific organization. The latter is usually combined with social engineering methods, with the help of which cybercriminals collect the necessary information about the victim in advance. These attacks depend on the weakest link in the security chain: the fallible human element. Therefore, organizations must take all necessary training measures to minimize potential attacks.

After a successful attack, the attackers inform their victims that their data is encrypted. To access the decryption key, the victim must make an immediate payment, often in cryptocurrency, which obscures the attacker's identity. You will know that you are a victim of ransomware if a pop-up window appears on your desktop or a readme.txt file that reads something like this: "**Your files have been encrypted and are now inaccessible. You will lose all your information on X date if you do not pay X amount in bitcoins.**" There may also be a postscript such as: "**IMPORTANT! All your files are encrypted with RSA-2048 and AES-256 algorithms.**"


Thankfully, since the cryptocurrency does not hide the wallet address, attackers can sometimes be detected. For example, in the United States they were able to return part of the ransom after the ransomware attack on the Colonial Pipeline company in May last year, committed by the DarkSide hacker group.[2] This is not the norm, however, and companies should not expect to get their ransom payment back.

If a company does not pay within the initial period (usually 48 to 72 hours), attackers are not shy about increasing the ransom and often threaten to delete or compromise data. Of course, in such cases, you can turn to cybersecurity specialists in the hope that they will find a way to recover data. Such options are possible but unlikely.

Modern ransomware also often contains data extraction tools, so sensitive information such as usernames and passwords can simply be stolen.

For all these reasons, the best practice is to proactively prevent ransomware from intruding into the network. And because the breaches in the network mostly happens through unsuspecting users, one of the main tasks in preventing these attacks is training personnel.

Equally important is email and network security, and the network must include a reliable backup program. Fresh copies of the data, which can always be returned in the event of a destructive cyberattack, must be created at least daily.

## Here are some critical steps organizations must take to effectively evade ransomware and its aftermath:

1. **Create offline backups**
   While regular cloud and virtual backups are useful, if you don't keep your data backed up offline, you run the risk of losing that data. The solution means regularly backing up to a safe place, keeping multiple copies, and monitoring that the backups match the original. The latter is important because if the backup copy that is being restored was created after a cyberattack, then it will also be infected.

2. **Improve employee cybersecurity awareness**
   Raising employee awareness about ransomware is one of the most important ways to improve cybersecurity. Companies should conduct both general and personal briefings regularly, because a successful attack needs only one misstep in order for the entire organization to be compromised.

3. **Customize the display of the file extension**
   Employees must be trained not to double-click on executable files (files with the extension .exe), from any source. However, Windows hides file extensions by default, allowing malicious executables like "ransom.doc.exe" to look like a Word document named "ransom.doc." This is a simple setting change, but setting extensions to always show up will go a long way in countering these kinds of threats.

4. **Set up spam filters**
   Cybercriminals send millions of malicious emails to random organizations and users, but an effective spam filter that constantly adapts to new threats can stop more than 99% of such messages from reaching employees' mailboxes.

5. **Block executable files**
   Filtering .exe and other suspicious extensions from emails (attachments or hyperlink) can prevent certain malicious files from being forwarded to employees.

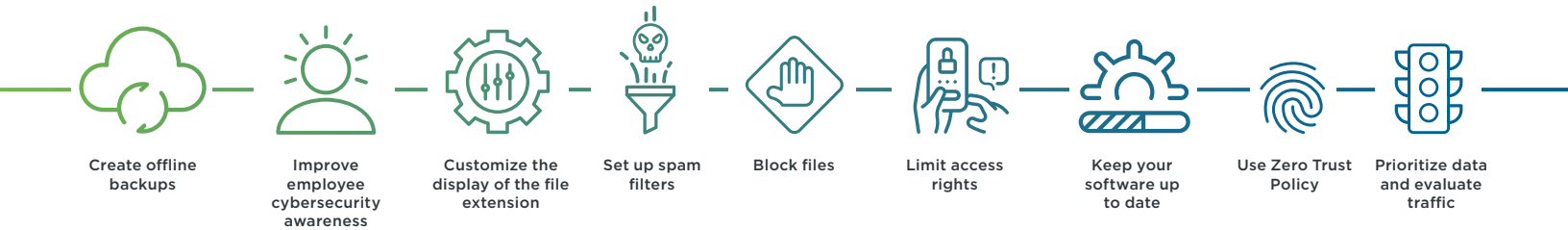
6. **Block JavaScript Files**
   Ransomware is sometimes distributed in ".zip" archives which contain malicious JavaScript files. They are usually disguised as text files with names such as "readme.txt.js" and are often seen simply as "readme.txt" but with a script icon for the text file. You can address this vulnerability simply by disabling Windows Script Host.

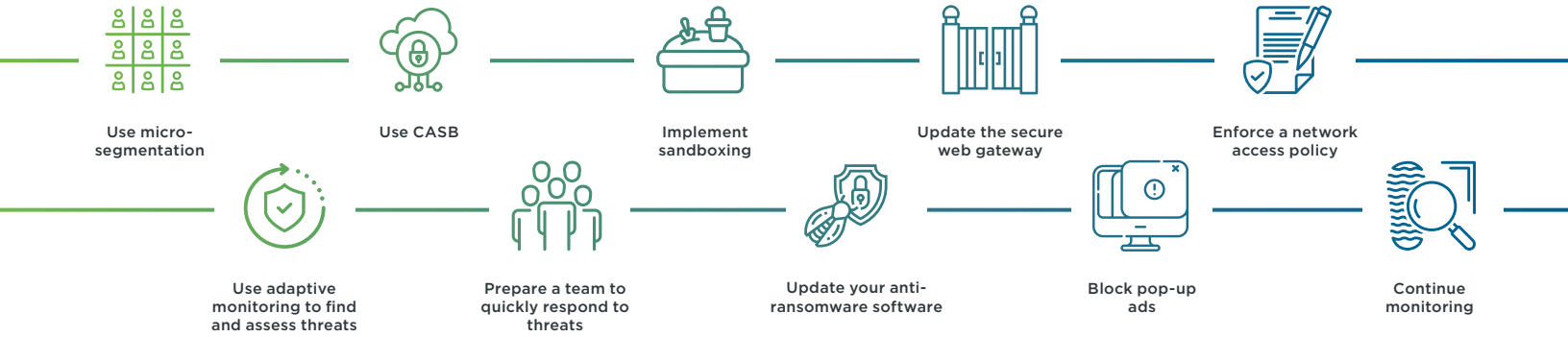
7. **Limit access rights**
   Ransomware can only encrypt files that are available to a specific user on the system, unless they contain code that can elevate user privileges as part of an attack. Care must be taken to ensure that changing access rights is not possible without confirmation.

8. **Keep your software up to date**
   All software must be kept up to date, as updates almost always include the latest security patches to address previously discovered vulnerabilities. 2020's SolarWinds attack is a good example of this preventative approach, as organizations that updated the SolarWinds Application in a timely manner were able to prevent cyberattacks as a consequence of the breach of the SolarWinds application network infrastructure.[3]

9. **Use Zero Trust Policy**
   Zero Trust provides more reliable control over the network, which increases the chances of blocking ransomware. Thus, if a user with limited access initiates a cyberattack, its consequences can be minimized with prompt actions by the organization's cybersecurity specialists.

10. **Prioritize data and evaluate traffic**
    Identifying the most valuable data and network elements gives cybersecurity professionals and company leaders an idea of how attackers can infiltrate your network. This will give your team clear indications of which parts of the network infrastructure need additional protection or restrictions.






11. **Use micro-segmentation**
    A micro-segmentation policy ensures that a user is only granted access to the applications, database, and directories that they need. Micro-segmentation is the ideal solution for blocking attempts to compromise an entire network. Implementing strict application layer policies, segmentation gateways, and next-generation firewalls (NGFWs) can prevent ransomware from accessing the most valuable network segments.

12. **Use adaptive monitoring to find and assess threats**
    If there is even the slightest potential of attacks on the most sensitive segments, organizations need to constantly monitor data and processes, using adaptive technologies. This includes sequentially assessing traffic for critical applications, data, or services to actively look for threats and viruses.

13. **Use CASB**
    Cloud access security broker (CASB) services can help manage your organization's cloud infrastructure. CASBs provide additional transparency, data security, and threat mitigation while protecting your data backed up to the cloud.

14. **Prepare a team to quickly respond to threats**
    In the event of hacking attempts or a successful attack, your team must be ready to promptly restore systems and data. This work includes preliminary assignment of roles and preparation of an attack response plan.

15. **Implement sandboxing**
    Sandbox testing is a common technique for cybersecurity professionals when examining new or unrecognized files. Sandboxes are environments that are disconnected from the corporate network to safely test files.

16. **Update your anti-ransomware software**
    Regular network and endpoint security software updates are critical. This is especially important for existing intrusion detection and prevention systems (IDPS), antivirus, and antimalware.

17. **Update the secure web gateway**
    All email on the network typically goes through a secure web gateway (SWG). By updating this server regularly, you can monitor email attachments, websites, and files for malware. This data can help you inform your staff about what attacks can be expected in the near future.

18. **Block pop-up ads**
    All devices and browsers must have extensions that automatically block pop-up ads. Such ads are a serious threat if not blocked.

19. **Enforce a network access policy**
    If you have a remote workforce and your company doesn't have a clear policy on which devices are allowed to access the network, it might be time to take immediate action. The unregulated use of various connected devices poses unnecessary risk to your network. When gaining remote access to a corporate network, company employees should install all the necessary security software (antivirus, EDR, a reliable firewall, etc.) on their PCs and laptops to minimize the risk of ransomware attacks.

20. **Continue monitoring**
    The entire IT system and all related footprints need to be monitored for signs of suspicious behavior. This involves monitoring across all your servers, network, endpoints, applications, and users. Round-the-clock monitoring with an active defence strategy can help you respond at an early stage of intrusion.

## RANSOMWARE IN RECENT YEARS

Researchers from the Beazley Group note that until four years ago, reports from customers about ransomware attacks were infrequent. At the time, these cases usually involved data encryption, but not access or exfiltration. Today, however, the frequency of ransomware attacks has increased significantly, and the additional threat of data leakage makes such attacks much more destructive. As early as 2019, ransomware variants like Ryuk and Sodinokibi were increasingly being launched in tandem with banking trojans like Trickbot and Emotet. And cybercriminals are getting smarter every day; in some cases, the attacks resulted in the suspension of hundreds of clients' operations.

At the same time, the goals of these attacks were not random. The criminals calculate the probability of receiving a ransom from the attacked company, and the damage that a company may experience if the entire client base and business were to disappear due to the attack. Consequently, ransomware attacks on healthcare businesses are on the rise, due to the sensitive nature of patient data and the critical impact on their care. According to Beazley research, companies in the healthcare sector were the most affected (35% of the total) from ransomware attack, followed by financial institutions (16%), educational institutions (12%), professional services (9%), and retailers (7%). And the total number of attacks increased by 130% in 2020 compared to 2019.

Ransomware has become one of the biggest cybersecurity threats in the world.[5] As early as 2016, the total amount of ransom demanded from ransomware creators approached the annual criminal turnover of $1 billion—and that's just in the U.S. As with Beazely research, Malwarebytes also considers healthcare and financial services to be the most vulnerable to ransomware.

IBM research has determined that

- **only 38% of government employees are trained to prevent ransomware attacks**,

and

- **only 29% of small businesses have experience with ransomware**.[6]

Additionally,

- **81% of the total number of ransomware attacks occur in corporate infrastructure**,

and

- **62% of attacks occur in small and medium-sized businesses**.[7]

These statistics demonstrate existence of a widespread, equal-opportunity threat that continues to grow.

ACCORDING TO

**BEAZLEY RESEARCH,[4]**

companies most affected from ransomware attack were

**35%**
Healthcare

**16%**
Financial Institutions

**12%**
Educational Institutions

**9%**
Professional Services

**7%**
Retailers

And the total number of attacks

**INCREASED BY**

**130%**

in 2020 compared to 2019.

## WHAT TO DO IF YOU BECOME A VICTIM OF RANSOMWARE

No one is immune from these attacks, and even the best-laid plans can have security gaps. If your organization is a victim of such an attack, here are some things to remember.

First, focus on getting your organization back to normal by restoring systems from backups. This may take several days, and it's important to remember that any changes made since the last backup before the attack will be lost. Find out when your data was corrupted to make sure you are restoring from a malware-free backup copy.

It may be possible to restore files on individual systems using the built-in file versioning service. This approach essentially allows you to "go back in time" to restore them to an unencrypted state. Some ransomware variants block this possibility, so this method may not work. If your attacking version of ransomware was implemented with ad-hoc encryption, it may be possible to recover data. Security vendors release decryption tools that automatically generate keys and decrypt files for compromised ransomware. Check to see what may be available for your particular instance.

Unfortunately, these "free" solutions may not always solve the problem, and it may be necessary to have the conversation about whether your organization is willing or able to pay the ransom. While it is obviously not ideal, it is good to know that in the end, 99% of all payments to intruders lead to obtaining the necessary decryption key and restoring all data. Do keep in mind, however, that paying criminals encourages their actions, making future attacks more likely. Decryption is also slow, and in many cases it is only partially obtained; part of the damaged data often cannot be restored.

As you consider your organisation's situation, vulnerabilities, and security protocols, take the time to consider these points. Ultimately, network security is only as good as the weakest link, and prevention is much easier than dealing with the consequences.

Give us a call or visit our website to learn more about how we can help you brave this internet-driven business world. To learn more about how SDG can help your organization secure its cyber assets, visit **www.sdgc.com**.

WHAT TO DO IF YOU BECOME A VICTIM OF RANSOMWARE

1. Get your organization back to normal by restoring systems from backups
2. Check to see what decryption tools may be available for your particular instance
3. If the "free" solutions aren't solving the problem, have the conversation about whether your organization is willing or able to pay the ransom

AS YOU CONSIDER YOUR ORGANISATION'S **situation, vulnerabilities, and security protocols,** take the time to consider these points. Ultimately, network security is only as good as the weakest link, and prevention is much easier than dealing with the consequences.

## ABOUT SDG

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.

RESOURCES


1. https://apnews.com/article/virus-outbreak-europe-technology-pandemics-medical-research-c7e7fc7e582351f8f55293d0bf21d7fb
2. https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack
3. https://www.coalitioninc.com/blog/december-2020-solarwinds-breach-what-you
4. https://www.beazley.com/Documents/2020/beazley-breach-briefing-2020.pdf
5. https://go.malwarebytes.com/OstermanRansomwareSurvey.html
6. https://www.ibm.com/downloads/cas/74JKYWZQ
7. https://docs.broadcom.com/doc/internet-security-threat-report-volume-24-en



SDG

Contact Us: solutions@sdgc.com

- 55 North Water Street
  Norwalk, CT 06854
- 203.866.8886
- sdgc.com