SpinOne

Ransomware Prevention Guide for Enterprise

- The cost of ransomware
- Should you pay the ransom?
- Ransomware prevention measures
- Action plan in case of a ransomware attack

Like a terrible disease epidemic, ransomware infects and destroys any data in its path. Its victims can potentially never recover from an infection. Much like protecting your physical health, you want to understand how to prevent such a damaging infection of your data.

As is the case in preventing a disease epidemic, the old adage, “an ounce of prevention is worth more than a pound of cure” certainly applies. Preventing a ransomware infection is much more desirable than having to recover from one. In this post, we will take a look at ransomware trends, costs, targets, and how a ransomware infection can be prevented.

SpinOne

Contents

01

RANSOMWARE

SaaS Data Protection Guide

Why Ransomware is the Fastest Growing Malware Threat

In 2019, Trend Micro found a 77% surge in ransomware attacks during the first half of 2019 from the previous year. Even though fewer ransomware families are detected, the statistics suggest cyber criminals are using existing ransomware variants to infect unsuspecting victims and doing so more pervasively.

There are two important reasons that ransomware is increasingly being used by cyber criminals – it is extremely effective, and lucrative. With its ease of use, effectiveness, and likeliness that a victim will pay the ransomware, it has become a favorite tool among attackers.

There are even Ransomware-as-a-Service offerings on the dark web providing would-be criminals with all the tools they need for carrying out a successful ransomware attack, specific to a particular industry or business entity with little effort.

What is equally alarming is ransomware is not only targeting on-premises environments but also cloud environments as well. Whether it is synchronized files from on-premises to cloud environments or the risk of encryption of cloud email, ransomware is a real threat to your data.

How much can ransomware cost your business?

The Cost of Ransomware

The cost of ransomware is tremendous. It can encompass many different costs, both tangible and hidden, for businesses that are infected. What do these costs include?

1. Ransom Payment

The first obvious and tangible cost of ransomware is the actual ransom demanded by an attacker. Ransom payments are generally demanded in the form of untraceable cryptocurrency such as Bitcoin. Just the ransom payment alone can be tremendously expensive. Hackers demanded bitcoins totaling $14 million to restore computers in 110 nursing homes managed by Wisconsin-based IT company Virtual Care Provider (VCPI). This was the amount demanded for restoring 80,000 computers and servers across many different states.

Other examples:

- Jackson County Georgia – paid $400,000 to hackers to restore access
- City of Riviera, Florida – paid $600,000 to attackers to bring systems back online

2. Cost of downtime and recovery operations

Even if the ransom demanded is not paid, the costs due to a ransomware infection can be tremendous. As is often the case, the cost of restoring files from backups can amount to more than paying the ransom. This is due to some restore operations and impairment lasting for days if not weeks depending on the scope of the ransomware infection.
A case in point, the city of Baltimore was hit with ransomware earlier this year. Hackers demanded bitcoins worth around $76,000. The city opted not to pay the ransom demanded. This has resulted thus far in costs exceeding $18.2 million. These costs for Baltimore include the cost to restore systems and making up for lost or delayed revenue.
Another costly example is the ransomware attack on Norsk Hydro, a Norwegian aluminum and energy giant. Total costs so far of the ransomware infection total some $71 million. This includes restore operations and downtime as a result of their cleanup efforts.

3. Intangible costs associated with lost customer confidence and damaged business reputation

As significant as the other costs associated with a ransomware infection may be, the intangible costs related to lost customer confidence and damaged business reputation can be extremely costly as well. In IBM's Cost of a Data Breach Report 2019 cited the following:

- Lost business is the biggest contributor to data breach costs
- The average cost of lost business in 2019 was $1.42 million
- Data breach costs can impact your business for years – 67% of the cost comes in the 1st year of the breach, 22% accrued in the 2nd year, and 11% of costs occurred more than two years after a breach.

Global Averages for a Data Breach

The following statistics are cited in IBM's Cost of a Data Breach Report 2019 as the global averages for a data breach event.

- Average total cost of a data breach - $3.92M
- Average size of a data breach – 25,575 records
- Cost per lost record - $150
- Time to identify and contain a breach – 279 days
- Highest country average cost of $8.19M – United States
- Highest industry average cost of $6.45M – Healthcare

When you look at the totals for data breach events, it is evident, ransomware is an extremely costly risk to your business. Between the initial damage inflicted on your data, the threat of data leak to the Internet, and the loss of business as a result of damaged customer confidence, the net effect on your business can be major.

02

RANSOMWARE TYPES THAT TARGET ENTERPRISE

SaaS Data Protection Guide

Attackers are using targeted attacks more than ever to net very large sums of money from various enterprise environments that hold valuable data prizes. There are certain ransomware variants that have shown themselves to be favorites among cyber criminals for infecting enterprises with ransomware. Let’s take a look at three ransomware variants that have been heavily used in ransomware attacks so far in 2019.

Ryuk

Ryuk was derived from Hermes ransomware code. It is effectively used in “big game hunting” which targets large environments with large ransoms.
It has been extremely lucrative. In fact, according to current totals known, Ryuk has netted over 705.80 Bitcoins across many different transactions for a total of more than $3 billion. This is quite a feat as it was only first discovered in mid-august 2018.
Ryuk ransomware was connected to attacks on DCH Health Systems in Alabama, Pitney Bowes, State of Louisiana, and Virtual Care Provider infections just to name a few.

RobinHood

The RobinHood ransomware is a newer ransomware variant that is becoming well known for its use in infecting city networks. RobinHood is said to be closely linked with the Eternal Blue tool. Eternal Blue is a U.S. National Security Agency tool that was leaked by the hacker group “Shadow Brokers” in 2017 . It exploits a vulnerability in Microsoft’s Server Message Block (SMB) protocol. RobinHood is thought to be using this exploit tool among others for compromise.

RobinHood is not known to leak data to the Internet if no payment is made. But it is known to increase the ransom amount after 4 days of being infected without paying, charging as much as $10,000 in penalties each day the victim does not pay the ransom. Another unique characteristic of RobinHood is that it tries to infect as many PCs as possible on the network and pushes out ransom notes under different names on the infected machines.
RobinHood was linked with the attack on the City of Baltimore this year where city services were disrupted. Service disruptions due to the ransomware attack included payments to city departments and real estate transactions. Hackers demanded 13 Bitcoins.

SamSam

The SamSam ransomware is named after the group responsible for its development and use. SamSam has been used very effectively in highly targeted attacks on mainly U.S. targets. SamSam's specialty is breaking into networks and encrypting multiple computers across an organization and then demanding a very high-value ransom, totalling in the millions. The SamSam ransomware was believed to be behind the attack on the City of Atlanta and the Colorado Department of Transportation.

Maze

Maze ransomware demands a ransom and also threatens releasing your sensitive data if the ransom is not paid. Maze ransomware was first seen in the wild since May 2019 and is becoming increasingly active.
It stands to reason that Maze will only be the first of many ransomware strains to come that may use data leak scare tactics as leverage to force victims to pay the ransom.

BitPaymer

The BitPaymer ransomware has been linked with various ransomware infections in 2019. This includes the Billtrust and German manufacturer, Pilz, ransomware infections. Bitpaymer ransomware infections are typically known to be higher ransom demands that other ransomware variants. Ransoms demanded average $110,000 USD (50 BTC).
It is known for being used for highly targeted attacks on mid-large sized organizations. BitPaymer encrypts files with the .lock extension along with deleting all shadow copies of your files. The decryption tool provided by BitPaymer once the ransom is paid is known to not be very reliable. This means there is a good chance your files are gone even if you pay the ransom.
When it comes to paying a ransom demanded by today’s ransomware variants, should you pay it?

03

SHOULD YOU PAY THE RANSOM?

SaaS Data Protection Guide

According to many law enforcement experts, including the FBI, you should not pay the ransom. It has been noted that paying a ransom demand only encourages this type of cybercrime and funds it. However, for many small, medium, and even large businesses, the consequences of having unreachable data due to ransomware encryption can be disastrous.

When ransomware infects your enterprise environment, there are really only two ways to recover your data:

1. Restoring from backup
2. Paying the ransom

It can go against every fiber of moral-based decision making based on “what’s right”, however, some businesses have made the decision to pay the ransom. Why?

Why do businesses pay the ransom?

1. Ransom Payment

Restoring from backup is certainly preferable to paying the bad guys for the damage they have inflicted. However, many have found themselves in a position where the ransomware has also infected their backups along with production business-critical data. Ransomware today can actually look for backup files along with user data. Hackers know if they can encrypt backup files, they have a better chance to have the ransom paid.
If backups exist in network shares that are accessible to ransomware, these can be encrypted along with any other data. You must protect your backups at all costs.

Often, a ransomware infection can expose flaws in an organization's backup methdology of business-critical systems. These can include:

- Backups are not scheduled regularly
- Backups are failing so data was not copied correctly
- Backups are not tested on a regular basis
- Backups are not copied offsite for additional protection

2. The cost of downtime is too high.

Restore Time Object (RTO) is a term used in data protection that describes the amount of time that is acceptable to the business to be without business-critical data. During this time, they may be able to operate in a degraded state.

If the business has decided upon an RTO of 24 hours and restoring data infected by ransomware would take significantly longer, perhaps an entire week, paying the ransom becomes a simple business decision.

3. Cybersecurity insurance will offset the ransom.

Another factor that can weigh into making the decision to pay the ransom demanded by ransomware is having cyber security insurance. Since cyber security insurance can help your business offset the cost of paying a ransomware demand, many businesses opt for paying the ransom instead of restoring data.

Does paying the ransom guarantee getting all your data back?

Many ransomware decryption keys provided after paying the ransom have failed to retrieve all data.
Kansas Heart Hospital in Wichita, KS, was hit with ransomware that held several non-critical systems hostage with a ransom. Even though patient data and other business-critical systems were unaffected by the ransomware, the hospital officials decided to pay a "small amount" that was demanded for the ransom.
However, after paying the initial ransom demand to the hackers, they did not send the decryption key/tool as promised and demanded even more money as a ransom. This helps to emphasize the risky nature of dealing with cyber criminals and paying the ransom amounts demanded.

A summary of potential dangers of paying a ransom demand includes:

- Attackers may not send a decryption key
- They may have a poorly written or implemented decryption process and damage files
- They may deliver a larger ransom demand after receiving the initial payment

04

RANSOMWARE PREVENTION METHODS

SaaS Data Protection Guide

As mentioned in the outset, preventing ransomware is certainly much more desirable than having to recover from a ransomware infection even if you have the means to do so. What are some effective ransomware prevention methods?

Have effective backups of business-critical data

Backups are arguably the single most effective means of preventing, protecting, and recovering from a ransomware infection. This should be given priority among other means of protection.

Educate end users

Help them identify suspicious and potentially malicious emails, files, web sites, or other resources.

Implement good email phishing/SPAM filtering

Filter out obvious malicious SPAM emails with infected links, attachments, and other files.
There is no question that ransomware found in SPAM/phishing emails are one of the main threat vectors for a ransomware infection. In fact, one report shows that business email compromises are 23% of cyber insurance claims.

Implement endpoint security

Endpoint security is a necessity and can help to prevent a widespread infection of multiple endpoints with ransomware. Endpoint security includes antivirus, anti-malware, and anti-ransomware solutions that scan and protect your end user clients.

Use firewalls

Block known malicious connections and IP addresses. Firewalls can read from IP threat lists which can help block malicious source network traffic, including those used by ransomware.

Use least privilege access

Ransomware can exploit overprovisioned privileges and access levels to spread across network environments. Having least privileged access in place helps to minimize the damage that can be caused. Least privileged access means that users only have the absolute minimum required level of permissions to access resources on the network.

Use application whitelisting

With application whitelisting, legitimate programs such as your business applications have to be explicitly allowed to run. This helps to ensure that ransomware executables and other malicious code will not be approved to run if it makes its way to an end user workstation.

Secure or disable Remote Desktop connections

RDP vulnerabilities, like “Bluekeep” have been responsible for many widespread ransomware infections. RDP vulnerabilities allow attackers to compromise and take control of remote RDP servers. If RDP connections exposed to the Internet are required, make sure RDP servers are patched, use two-factor authentication to authenticate to RDP, and restrict access as much as possible via network or other means.

Logically and physically separate your networks

When ransomware infects a network environment it tries to spread laterally across all other connected devices. Having your network segmented and logically/physically separated helps to limit this potential widespread infection.

05

ACTION PLAN IN CASE OF RANSOMWARE ATTACK

SaaS Data Protection Guide

What to Do If Infected with Ransomware

What do you do if ransomware makes it past the defense mechanisms and preventative measures you have put in place? The following are a few recommended actions you should take when you become aware of a ransomware infection.

- **Isolate the infected device immediately** – You want to take the device off the network as soon as possible. One of the quickest and easiest ways is simply disconnecting the network cable.
- **Isolate devices that are not infected** – If a device has not been affected by ransomware, isolating it from the network can be a great way to ensure it is protected while the ransomware infection is contained and remediated.
- **Secure Cloud Drives and synchronization access –** You should disable synchronization of OneDrive or Google Backup & Sync for all users.
- **Verify backup systems and isolate those ASAP** – Many variants of modern ransomware are looking for backup files. If they can wipe out your ability to restore, there is a greater likelihood they will receive the ransom. Take your backup systems off the network or isolate them completely. Verify backup file integrity and backup repositories.
- **Enforce password changes of network accounts** – As a proactive measure in case sensitive data or passwords have been leaked, enforce a password change of all accounts across the board.
- **Contact Law Enforcement** – It is recommended to contact the Federal Bureau of Investigation (FBI) or your local law enforcement authorities when you learn of a ransomware attack. They can help assist with working the event as a criminal investigation as well as offering other assistance as needed such as providing recovery resources and in some cases, technical assistance.

- **Implement your business-continuity (BCP) and disaster recovery (DR) plan** – The BCP and DR plans are a set of procedures and processes documented before a disaster happens that help prioritize activities in order to keep the business running and restore access to affected systems. Part of the DR plan is restoring backups. In the case of ransomware, restoring backups allows recovering any files that have been affected by the ransomware encryption process.

- **Consider the risks of paying the ransom** – As we have already covered, paying the ransom can be risky. As noted, you may not get your data back, a higher ransom may be demanded after you pay the first one, and it can encourage cybercriminals to attack you again in the future.

07

ANTI-RANSOMWARE SOFTWARE

SaaS Data Protection Guide

What is anti-ransomware software? There are many solutions on the market today that feature anti-ransomware capabilities. These are found in both paid and free variants. Many of the anti-ransomware tools available include a range of features like the following:

1. Ransomware behavior detection – scanning and “learning” file behaviors – Since ransomware’s primary activity on your system is encrypting files, anti-ransomware detects unusual changes in your files including encryption processes and can stop the process before it progresses.

2. File protection – Protects files from suspicious processes that attempt to make changes to your file system.

3. Recover files – Anti-ransomware solutions can either catch the encryption process before it encrypts a single file, or detect the encryption and revert the process.

07

MAKE THE BEST CHOICE

SaaS Data Protection Guide

SpinOne – The Best Option for RansomCloud Protection

SpinOne is a unique cloud-to-cloud backup and cybersecurity solution. It provides a cybersecurity and backup solution rolled into a single cloud protection suite. This means you can manage both your cybersecurity initiatives and backups of cloud data from a single pane-of-glass dashboard.
It makes use of a Machine Learning (ML) enabled cybersecurity that detects and responds to anomalous behavior in your cloud environment.
As prevention is the recommended way to deal with ransomware, SpinOne provides many powerful cybersecurity features to help prevent ransomware from infecting your files to begin with. These include:

- **A dedicated Ransomware Protection module** – With the ransomware protection module, SpinOne detects any anomalous behavior, blocks the source of the file behavior anomalies and reverts any changes made to files automatically.
- **Risky Apps Protection** – With risky apps protection, SpinOne provides an effective way to block apps that exhibit risky behavior or start to show signs of being malicious in intent or activity
- **Insider Threat Protection** – This helps to give visibility to either an employee with unscrupulous intent or a compromised account.
- **Brute force login protection** – Often attackers trying to drop ransomware in your environment will make use of brute force attempts to find credentials for compromise. SpinOne provides brute force login protection and reporting so you have visibility to any potential attempt to breach security.
- **Active alerting and reporting** – Real time alerts and reporting are great ways to gain visibility to security issues in your environment. SpinOne provides real time alerting and reporting on your cloud environment and security events as they happen.

In addition to the cybersecurity features, SpinOne provides enterprise backups of your cloud data, including the following services:

- **G Suite** – Gmail, Drive, Team Drives, Contacts, Calendar, Photos, and Sites
- **Office 365** – Email, OneDrive, Calendar, People, and SharePoint

One of the great features with SpinOne is the ability to store your cloud backups in a public cloud of your choosing. This helps you to satisfy the offsite backup requirement for your business-continuity and disaster recovery strategy. It also helps to ensure your backups are not located in the same public cloud where your production data is housed.

You can choose from Azure, GCP, and AWS for storing your cloud backups.

Concluding Thoughts

Ransomware is an ever-growing threat to your data, both on-premises and in the cloud. By protecting your environment with various layers of security, you can greatly reduce the chances of having data damaged by ransomware.

As we covered, there are many practical steps to take to prevent a ransomware infection such as enforcing good cyber “hygiene” by educating your users and using effective email filtering and endpoint security. Remember to not neglect your cloud environments when protecting your valuable data assets.

Knowing what to do in the case of a ransomware infection is important as well. Acting quickly and decisively can help prevent the spread of a ransomware infection throughout your environment and can help contain the damage. Practical steps involve isolating both infected clients and those that aren’t infected. Additionally, it is a good idea to isolate backup systems.

When it comes to cloud environments, using solutions that provide both cybersecurity and data protection for your environment is key to ensuring your data is protected. SpinOne provides both means of protecting your data in a unique solution that leverages Machine Learning to fight ransomware.

By doing your due diligence in preventing a ransomware infection both on-premises and in the cloud as well as protecting your data with effective backups, you can rest assured knowing your data is safe even though the danger of ransomware is lurking at every corner.

SpinOne

ABOUT SPINONE

SpinOne is a multi-tenant platform created by Spin Technology and designed to simplify the complexity of cloud data security. As an all-in-one platform, SpinOne combines three solutions that make business data bulletproof from the security breach and insider threats: SpinSecurity, SpinAudit, and SpinBackup.

SpinOne is trusted by over 1,500 organizations worldwide including HubSpot, Vopak, IBT Industrial Solutions. We have more than 1,200,000 business users in more than 100 countries.

Try SpinOne Free →

Spin Technology Inc

2100 Geng Rd Suite 210

Palo Alto, CA 94303, USA

USA and Canada Toll Free:

+1-888-883-2993
(9am to 5pm PST)

EU, CIS and Asia:

+48-22-602-2440
(7am to 4pm GMT)