peters & associates
simplify solve succeed

Ransomware Guide

Table of Contents

About Peters & Associates

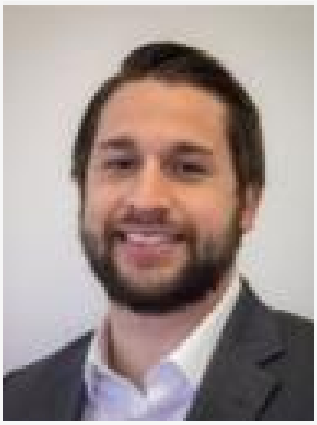
Who We Are

Peters & Associates is a Chicago-based leader in delivering technology and cybersecurity support services as well as project-based technology implementations. Although local to the Chicagoland area, Peters & Associates is nationally recognized as a leader in the industry by our 12 Gold & Silver Microsoft competencies and our CompTIA Security Trustmark+ designation amongst other vendor certifications we currently hold.

We are a family-owned business that has been providing information technology consulting services since 1981. The key to Peters & Associates success and longevity in the marketplace is our commitment to focusing on the customers' business needs and aligning a technology solution to meet those needs.

To learn more about Peters & Associates, go to www.peters.com.

About the Author



Adam has been at Peters & Associates for nearly 8 years in roles that span service delivery, marketing, and technical education. In his current role, Adam is responsible for the development and alignment of Peters & Associates support, managed services, and managed security services. In this capacity, Adam is tasked with partnering with clients to identify their unique challenges and developing a support and security plan to address those challenges. Adam holds bachelor degrees in Management & Organizations and Marketing from the University of Iowa.

Contact Us

info@peters.com

1801 S. Meyers Road, Suite 120

Oakbrook Terrace, IL 60181

Phone: (630) 832-0075

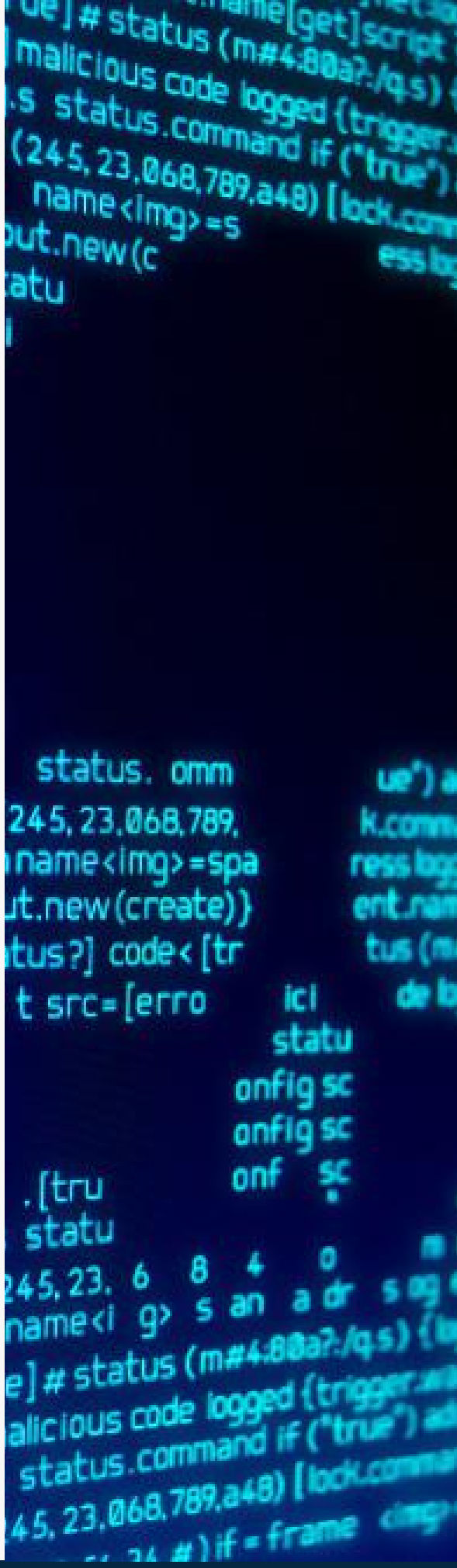
peters & associates
simplify solve succeed

Introduction

Over the last 5 years ransomware has grown in both frequency and sophistication. From municipal government, to hospitals, to schools, to small and medium-sized businesses (SMBs), ransomware has impacted most sectors of public and private industry. It seems like every week brings a new report of an organization fighting through a ransomware attack. There is no greater testament to this than Peters & Associate's long-running (almost 4 years!) "This Month in Cybersecurity" webinar series, which covers security issues and mitigation tactics that are applicable to SMBs and is never short on material.

The fact is, every organization is a target. It doesn't matter if the association is profit-generating or not. Attackers know that access to your computer systems is crucial to the function of your group. When their systems are compromised, most organizations will do whatever they can to regain access. This is why attackers know that they don't need to attack the largest, highest-revenue organizations; successful attacks on smaller businesses can prove just as profitable.

What has spurred the deluge of ransomware attacks in the last few years? Well, like most things in this world, there isn't a single explanation. Throughout this guide, we'll explain some of the reasons why the scourge of ransomware has been on the rise, what organizations can do to try to prevent ransomware, how to plan for a ransomware incident, and how to respond when ransomware strikes. But first, we're going to start with the basics: What is ransomware? Read on to learn more.



What is Ransomware?

Ransomware is a piece of malicious software (malware) that prevents an organization from accessing their files unless the organization pays a ransom. Typically, the victim organization's files are encrypted using the Advanced Encryption Standard (AES). The level of encryption is not easily broken. The attackers provide an organization a limited number of days to pay the ransom to decrypt the files or the files will remain locked.

How is Ransomware Spread?

There are many ways that organizations become infected. Among the most common ways is via malicious attachments or links in email messages. Each strain of ransomware has different characteristics, but the main functions are generally the same. Once the ransomware has infected a device in your environment, it gets to work. The ransomware encrypts all of the files on the device and network file shares that the user has access to. The more access and permissions that a user has, the more damage can be done. Often times, the ransom demand is not made nor the infection known until the malware encrypts as many files as possible. What are the most common ways that ransomware is spread?

Phishing Attacks

Traditional phishing attacks are emails that attempt to trick the victim into clicking on a malicious link opening an infected attachment. Some phishing attempts also trick the user into entering their network credentials, which allows the attacker access to the network so more information can be exploited. Newer attacks noticed by security researchers involve attackers injecting malicious links into a victim's calendar. When the user clicks to join the conference call that they can't recall setting up, their system and, usually, their credentials, are compromised. In addition to general phishing attempts, some targets may be "spear-phished." Spear-phishing is the deliberate targeting of an individual. For instance, an attacker may use LinkedIn to learn the identity of the CFO and a new member of an organization. Then, the attacker will spoof the CFO's email with an urgent request to the employee. Many unsuspecting people have fallen victim to this. Other phishing attacks involve phone calls pretending to be the IT department or financial institution and attempt to direct the user to a malicious site, these are less common though.

Drive-by Downloads

This method of ransomware infection occurs when a user goes to a malicious website. In many cases, that's enough for the malware to be installed to the user's device. This is increasingly common with software download and video streaming sites, but has also been seen via malicious ads on other sites.

Infected USB Drives

This form of malware infection has been around for a long time and has been used for other types of attacks aside from ransomware. Typically, an attacker will drop a USB drive in a public place – the company lobby, the parking lot, the sidewalk – or the attacker will mail a USB drive under the guise of a recognized vendor. Either way, once the victim plugs the USB drive into the computer to see what's on it, the infection begins.

How is Ransomware Becoming More Sophisticated?

Just like any legitimate software developer, ransomware developers know that they need to continue to enhance their software to dodge new detection and prevention technologies, make ransom payment more likely, and exploit new vulnerabilities.

We'll dive into the business of ransomware later in this guide, but we'll cover the recent evolution of methods and technology here. One of the newest trend that we've encountered is the targeting of backups before launching the ransomware attack. In some cases, an attacker has gained access to an environment, located the backup server, and deleted all backups before the launch of the ransomware attack. In other cases, ransomware strains have been developed to target specific backup solutions to encrypt first. As we'll explain in depth later, reliable backups are a critical factor to successfully recover from a ransomware attack. Keeping a set of backups offline and offsite can help to minimize the damage in these new attacks.

In addition to developing more sophisticated software, attackers have also become smarter about their timing. Most ransomware attacks that we've encountered begin late on a Friday or on the weekend. This is because the victim organization's employees are less likely to be logged in and less likely to recognize that an attack is occurring. Thus, the ransomware software has more time to encrypt files in the environment.

Payments for Ransomware

If an organization is unprepared for a ransomware attack, the cost of recovering the data can be astronomical. Just this year (2019) the Baltimore City government was hit with ransomware. They declined to make the $76,000 ransom payment, but total recovery costs were estimated at over $18 million dollars. With numbers like that, it's no wonder that many organizations are tempted to pay the ransom.

Should You Pay the Ransom?

This is an organizational decision, but there are some pros and cons to consider, along with some statistics. Let's start with the pros:

- If you do not have reliable backups to recover from, paying the ransom is likely less expensive than recovery. While ransom demand payments are increasing, examples like Baltimore City government show that other costs can be higher.
- Depending on the scope of the infection and your time to restore from backups, you may have your data back more quickly.
- Your cyber insurance provider may require it in order to receive coverage. While the FBI recommends not paying cyber criminals, insurance providers have other motivations.

Now for the cons:

- Not all organizations that pay, get their data back or get all of their data back. For instance, the ransomware strain Estimates are that roughly 40% or organizations pay the ransom and that 96% of those organizations receive a decryption tool. However, some strains of ransomware are less reliable in the success of that tool and 4% pay and don't receive the tool at all.

- After paying, you still have all of the negative aspects associated with the breach. Loss of public trust, the cost to recover, potential loss of customers, and more.

- By paying the cyber criminal, it encourages the attacker to target others or target you again. As a whole, the cyber criminal industry is propped up by these payments. The more people that pay, the more resources will be devoted to developing better strains of ransomware. Additionally, you've just proven to a cyber criminal that you are willing to pay the ransom. Very little will stop them from targeting you again. Of course, after the attack you should invest heavily in beefing up your cyber security plan, but resources can be limited in these circumstances.

The Business of Ransomware

Total ransomware costs for 2021 are predicted to be $6 trillion annually. Ransomware is big business for cyber criminals. While the big companies and breaches make the most headlines, small and medium sized business are much more frequently targeted. According to a 2019 study conducted by Beazley Group, 71% of ransomware attacks are against small and medium sized business.

What Do Hackers Want from Me?

Like we mentioned in the introduction, if you're a small or medium sized business, you are not being specifically targeted because of the name on the side of your building. Most people would agree on that, which is why it makes it especially hard to make business owners understand this next part – you are still being targeted! Attackers use sophisticated tools to identify vulnerabilities across the web. If your organization has a web presence and email addresses, you are in somebody's database and someone is trying to phish your employees or exploit other vulnerabilities. The organizations that become victims are generally those with the weakest security practices.

The Evolution of Ransomware

We're not going to dive into every strain of ransomware that exists, there are other great internet resources for that. What we'd like to emphasize here is that ransomware is becoming more and more sophisticated and more accessible to bad actors. A few years ago, attackers had to put in some effort to develop a new strain of ransomware and initiate a successful attack. Now, the barriers of entry are extremely low for someone that wants to distribute ransomware.

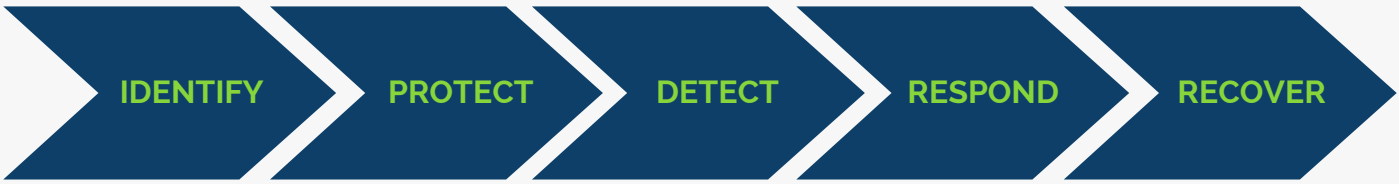
Entire enterprises have been built to develop ransomware, recruit distributors, and even support victims through the ransom payment. The way these enterprises operate would be hard to distinguish from a legitimate business – complete with bonus plans and incentives.

Ransom Negotiation

Another industry that has cropped up around ransomware is ransom negotiators. Often times a cyber criminal is willing to negotiate for a lower payment. There are third party organizations that will negotiate on your behalf to reduce your ransom payment and remove you from dealing with the cyber attackers directly. Victim arrangements with these ransomware negotiators are generally coordinated through your insurance carrier or law firm.

Securing your Organization from Ransomware

As you can see, ransomware is as pervasive and dangerous as ever. What can organizations do to protect themselves? If you're familiar with Peters & Associates, you likely know that we adhere to and promote the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF). The NIST CSF views security from five angles: Identify, Protect, Detect, Respond, and Recover. When we develop a security strategy, these elements should be understood and addressed. So, how does the NIST CSF apply to ransomware? Let's take a look.



Identify

Identify is presented on the left-most side of our diagram because the decisions that you make in every other phase are dependent on the systems, people, and data sets that are prioritized during the Identify phase. Remember, your organization is not being targeted because you have information that the attacker deems valuable. You're being targeted because you value your data and your business and, if you have no other options, you might be willing to pay the ransom. So, what are some of the people, systems, and data sets that you might choose to prioritize in securing from ransomware? Here are some common ones:

PEOPLE	• C-Suite • Human Resources Employees • Strategic Partners • Internal Application Owners	Employees with responsibility for the most sensitive data and systems are sure targets.
SYSTEMS	• Email • Human Resources Systems • Financial Systems • Core Line of Business Applications	Email is the most common attack vector while critical systems are the most likely targets.
DATA	• Regulated Data (Health Care, Personally Identifiable Information) • Intellectual Property	Regulated Data is commonly sold. Intellectual property can be sold or held hostage.

Protect

The Protect phase of the NIST CSF contains a lot of the traditional elements that we think of when we think about security technology. It's a combination of Process and Technology that work together to keep your organization as secure as possible. There are myriad ways to slice up your computing environment, I prefer to think about this Protect phase as layers of security. Individual layers could be compromised – no person, process, or technology is perfect – but, when properly implemented, more layers give an organization a greater chance of preventing a data breach. Which of these protection processes and technologies has your organization embraced to combat ransomware?

PROCESS	• System Patching • Password Management • Employee Security Awareness Training	→ Exploiting unpatched systems and unsuspecting employees are the most common ransomware tactics.
TECHNOLOGY	• Multi-Factor Authentication • NextGen Anti-Malware • NextGen Firewalls • Internet/DNS Protection • Security cameras and keycard access systems • Advanced Email Security	→ Securing employee login credentials, perimeter access, and devices is vital defense against ransomware.

Detect

One of the most overlooked components of a sound cyber security strategy is detection. The metric used in the industry is known as "dwell time." That is, the amount of time from when an attacker first infiltrates a network to when the victim organization recognizes that they've been breached. According to one report, average dwell time as of the second quarter of 2019 was 798 days for small and medium-sized businesses. That's over two years of an attacker having access to the victim's network. For ransomware specifically the average dwell time was significantly lower (43 days) since ransomware notifies the victim of the attack to seek payment. Because of the increase in quantity and severity of cyber attacks, detection methods are rising to the foreground in security strategies. Given how quickly ransomware spreads, what methods can an organization leverage to detect ransomware?

Monitoring for Anomalous Behavior

Watching for unusual user account behavior can indicate compromise early on in a ransomware attack. As we've noted before, the initial breach of an organization could occur days or weeks before the attacker deploys the ransomware. During this time the hacker probes the network for information that could be extracted, other vulnerabilities, and opportunities to launch attacks against the victim organization's partners. There are automated tools that can help in this effort, but organizations can also schedule frequent checks of indicators of compromise. For instance, Peters & Associates assists our customers by checking for mailbox logins from foreign mailboxes on a daily basis.

NextGen Anti-Malware

While Anti-Malware is definitely a "Protect" mechanism, it also operates as a detection mechanism when it identifies suspicious software on a machine. The difference between NextGen Anti-Malware and traditional Anti-Malware is that newer solutions are designed to combat "Zero Day" threats. That is, threats that have not yet been discovered by security researchers. Traditional Anti-Malware solutions are "signature-based," meaning that malware is cataloged as it is discovered. NextGen Anti-Malware provides a more proactive approach to preventing and detecting security threats.

NextGen Firewall

NextGen Firewall's also serve a "Protect" and "Detect" purpose. NextGen firewalls are able to evaluate traffic and connections at a deeper layer than older model firewalls can. This makes them better suited to identify suspicious traffic or traffic coming from suspicious locations, more easily. While firewalls are unlikely to identify ransomware itself, it can help identify a breach before the ransomware payload is launched.

Internet/DNS Protection

DNS protection is the last line of defense when it comes to a ransomware attack. DNS protection provides filtering and monitoring at a layer above your network. Routing all of your internet traffic (offsite workstation and on-prem devices alike) allows DNS protection to identify dangerous traffic attempting to leave and enter the environment. This can prevent ransomware software from communicating with the attacker's infrastructure for instruction.

Security Awareness Training

Security Awareness Training strengthens your defenses by teaching your employees to identify threats. While this helps to protect your organization, a well-trained and incentivized staff can also help to detect a breach. For instance, notifying IT of strange activity on their account or recognizing that they should not have clicked a link.

Respond

The fourth component of the NIST CSF is Respond. Like detection, response is too frequently overlooked. Too often organizations don't think about how they will respond to a cyber security incident until they are already breached. Organizations that have mastered the Response phase have developed a clear incident response plan, educated their staff on its components, and tested its effectiveness. There are several components to a well written incident response plan, which we won't fully flesh out in this guide. Specifically, for ransomware, there are numerous questions and scenarios that need to be discussed prior to a ransomware infection.

Will we pay the ransom?

- We'll explore this further in another section, but have the discussion before hand.
- Setup a Bitcoin account prior to an incident so that you don't waste valuable time during a crisis.

Who do we need to notify?

- This is why the first stage, Identify, is so important. If you have regulated data or customer data that is impacted by ransomware, you have a responsibility to report and possibly certain steps to follow.

Will we pursue a forensic investigation?

- If you are dealing with regulated data or require a forensic investigation of how the breach occurred, you need to take steps to preserve data before recovering data.

What is your response plan and priority?

- Part of your Incident Response Plan should be a course of actions specific to a ransomware infection. This should include disconnecting the impacted machines from the internet as soon as possible and beginning to collect data to determine the scope of the infection.
- Depending on your data sets and applications, you may want to prioritize specific systems for review.

Recover

Recovery is the most important component of preparing for and mitigating a ransomware incident. As we mentioned during our discussion on the Protect phase, we believe that more layers of security can put your organization in a better position to prevent a ransomware infection. However, these security layers can fail. That's when you need to fall back on your Disaster Recovery Plan.

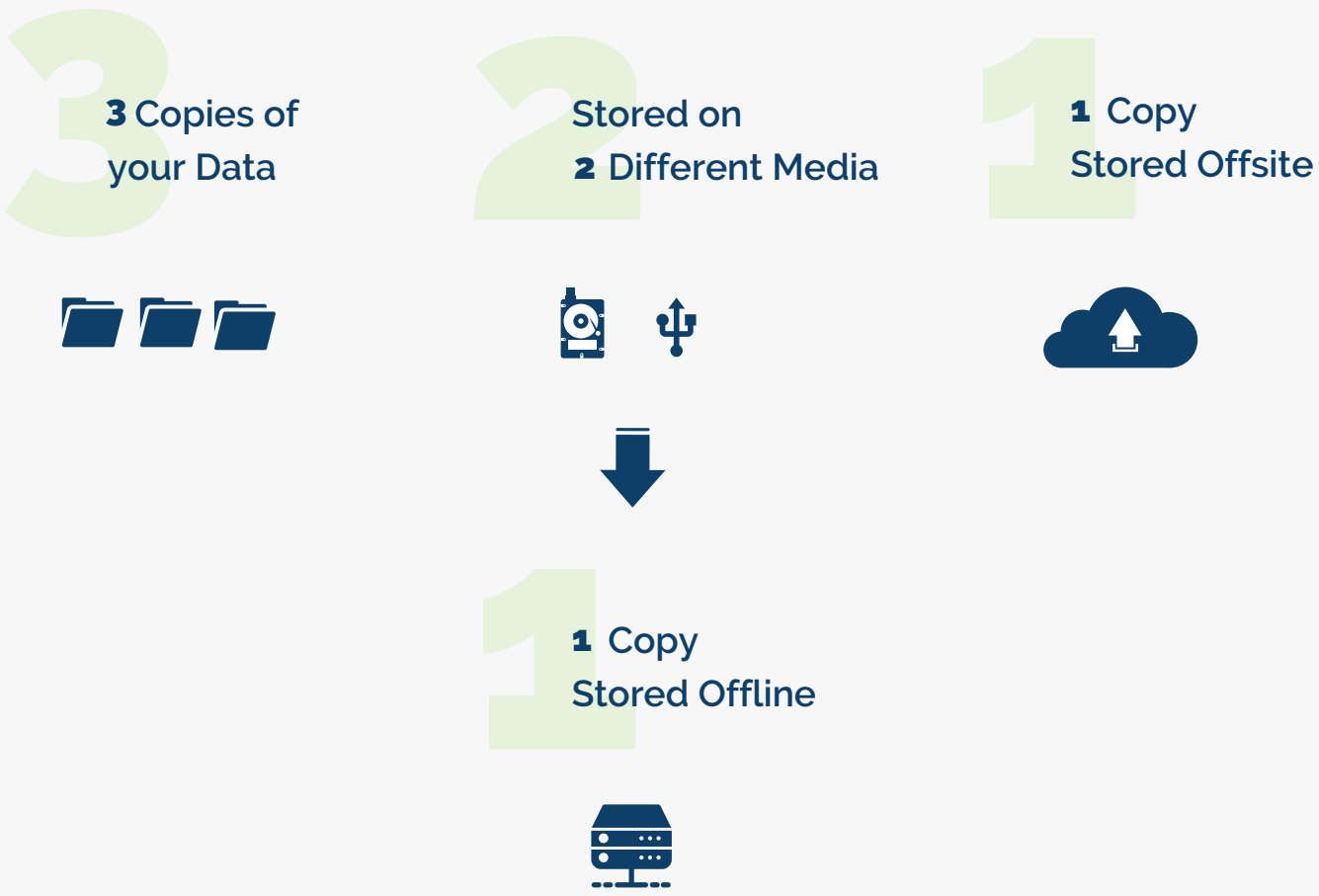
A Disaster Recovery Plan is an organization's documented process for how they prepare for and respond to a loss of data. The circumstances under which data is lost are myriad, it could be flooding or a fire in the physical data center, it could be hardware or human failure, or it could be ransomware. Why is a Disaster Recovery Plan so important for ransomware?

Ransomware is difficult to recover from; the encryption is unbreakable with current technologies. If a significant portion of your environment is impacted, your only options may be to pay the ransom or restore from your last clean backup. Further complicating the issue, there are new strains of ransomware that target your backups or attackers that have accessed your environment could delete your backups before beginning the attack. Because of this, organizations need to consider new methods and standards for backing up their data.

A well-thought out plan includes details on what servers are being backed up, where the servers are being backed up to, how frequently backups are taken, how long backups are retained, how long data restoration takes, how backup data is being secured (encryption), and how backup data is tested.

Backup is one important component of the Disaster Recovery Plan. There are additional considerations when it comes to recovery. Primarily, what is the order of recovery. In the Identify stage, we determined which systems and data sets are most important to our organization. In the event of a ransomware attack that compromises these systems, our recovery efforts need to prioritize those systems. Additionally, there are technical considerations that can determine the order of recovering servers. For example, Active Directory will need to be up and running before any systems that rely on Active Directory. As most organization know, the longer your primary systems are out of commission, the more productivity and money you lose.

So, what does a sound backup strategy look like? The diagram below details the 3-2-1 plan, with a slight modification. The 3-2-1 plan describes a process for backing up your data in a way that protects it from hardware failure, natural disaster, or other incidents. We have updated this plan to include regular offline backups (also known as cold backups) to secure data from new types of ransomware and backup deletion. Here is our version of the 3-2-1-1 backup plan.



What Do I Do During a Ransomware Outbreak?

We've just detailed several recommendations for building a security strategy to prevent or reduce the impact of ransomware attacks. However, if you haven't built that plan yet and you're infected with ransomware, what do you do? Here are a few simple steps that will suit most, but not all, situations.

1. **Disconnect from the Network**

Take every impacted workstation or server offline. Hopefully you've recognized this early, but taking the machine offline is the best way to stop the spread of the infection. Don't forget to turn off the WiFi capabilities for your wireless devices.

2. Review and Protect Backups

Review your backups to determine your last clean backup copy. That is, when was the last time that you took a backup of your environment that was not infected. Modern backup solutions can save you time by testing for this before restoration. During this time, you'll also want to ensure that the backups were not compromised by the ransomware or deleted prior to the attack starting. If backups are compromised, your options become a lot more limited.

a. Set your BIOS clock back

This won't work with all types of ransomware, but some strains use the BIOS clock to countdown the time to payment, and sometimes increase the ransom over time. Setting the clock back might buy you more time to review your options.

b. Look for a Decryptor

As the ransomware crises has worsened, some security researchers have developed tools to assist victim organizations. A number of these researchers have compiled encryption keys for common types of ransomware. This decryption key can be used to recover your files without paying a ransom.

c. Discuss paying the ransom

Refer to our earlier section on ransomware payment. Your cyber insurance provider may require that you make this payment.

If all of the options above fail, your organization will be in a tough spot. Restores can be attempted using Windows System Restore, but most strains of ransomware prevent that. You can also attempt to boot into Safe Mode and run some anti-virus tools via an external drive. However, most of these attempts will be fruitless. The best way to address ransomware is to build a plan ahead of time.

How Can Peters & Associates Help Your Organization?

Peters & Associates has been assisting our customers with ransomware and other security issues for over 3 decades. Over that time, we've developed a number of tactics for preventing and mitigating data breaches and infections. Here are three ways that we can help your organization today.

Build a Plan

Our team of project managers, engineers, and virtual CIOs have deep experience in evaluating the security maturity level of our clients and developing a security strategy that is optimized for your organization. Small and medium sized businesses can't afford the same security solutions as large enterprises, but we can help build a cost-effective solution that meets your needs.

In addition to building a general security strategy plan, our team can help with specific policies that we mentioned throughout this guide. We've developed Incident Response Plan or Disaster Recovery Plans for hundreds of clients.

Managed Services

Our managed services offerings adhere to the NIST CSF from the ground up. While we have some specific managed security service offerings like our PULSE Managed SIEM, all of our managed services include security elements. The goal is to build layers of security for our clients.

System Hardening

Peters & Associates can also assist our clients that don't have managed services through system hardening exercises. This includes projects to review the security of your firewall configuration or, more commonly these days, your Office 365 configuration. Did you know that auditing is turned off by default in Office 365? Our team can conduct security reviews, vulnerability scans, and penetration tests to help ensure that our client's environments are secure.

Do you still have some burning questions on cyber security and education? Reach out to us, we're here to help.

Contact Us

peters & associates
simplify solve succeed