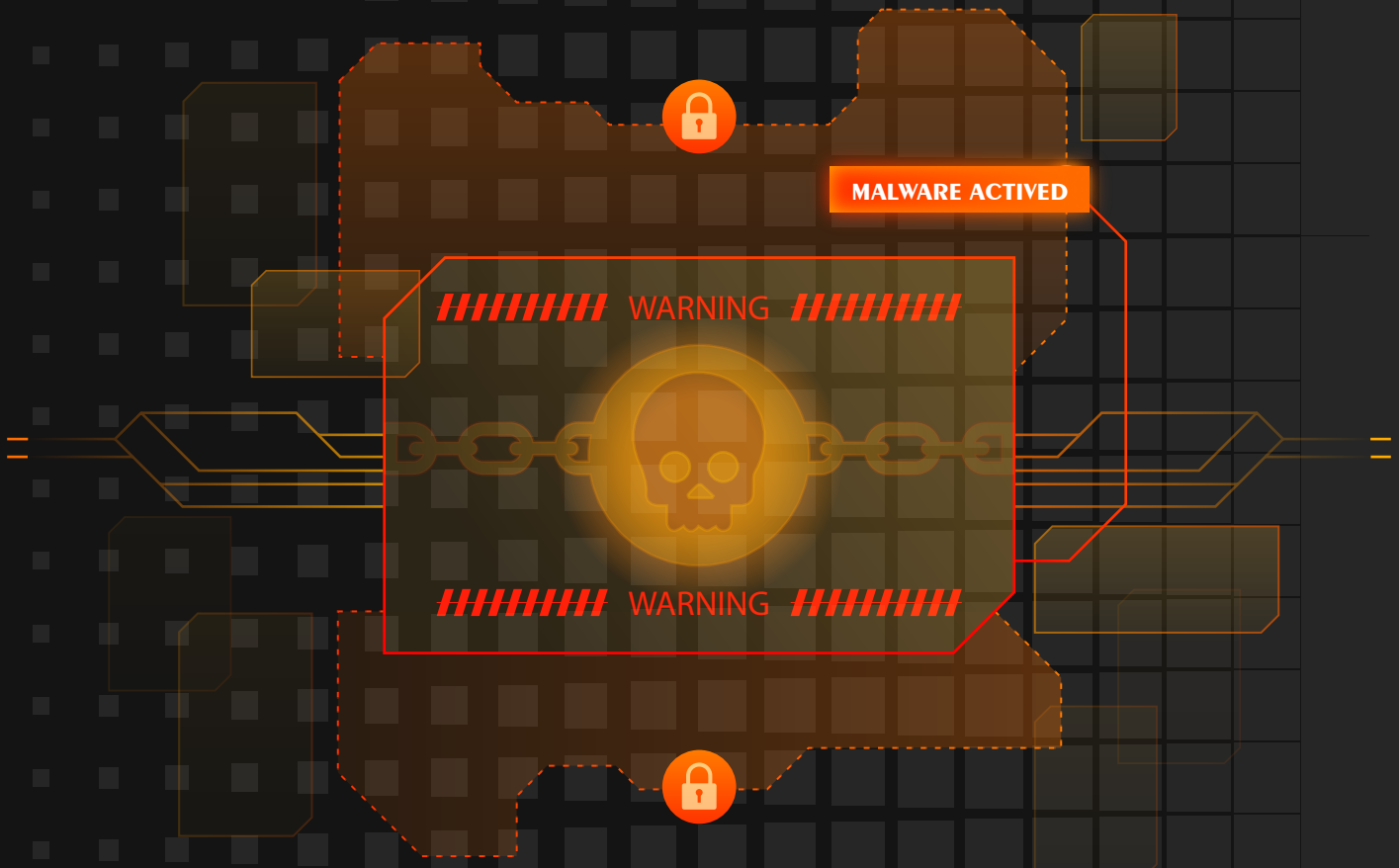
PROTECTED HARBOR

# THE COMPLETE GUIDE

# RANSOMWARE PROTECTION FOR SMB's




2022

Digital transformation has altered businesses' operations, bringing a new set of cyber risks. Traditionally, small to medium-sized companies pay less attention to cybersecurity because they assume they are safe and tend to feel as though they don't have any sort of sensitive data that attackers are after.

However, the ransomware changes the game. It has become a growing concern in a rapidly evolving cyber threat landscape. SMBs (Small and Small-Medium Businesses) are particularly vulnerable as they lack the proper resources to protect themselves. According to the Statista Research Department, 236.1 million ransomware attacks occurred worldwide during the first half of 2022.

As ransomware spreads, it continues to get more lucrative and more sophisticated. According to a recent study, the average ransom demand has increased to $750,000. As an SMB owner, you can't afford to pay that huge loss.

What does all this mean to SMBs? All organizations should keep ransomware and cybersecurity at the forefront of their minds to protect themselves. Given this, we have gathered information regarding ransomware and how your business can proactively take precautions to avoid an attack, plus help you address the growing ransomware threats.

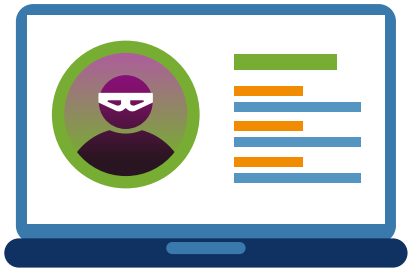
# Part 1: What is Ransomware?

Ransomware is a type of malware used to encrypt your company's data. At first glance, you may believe that your data has been deleted, but on the contrary, it's actually been locked and hidden away from you. The attacker, in this case, is the only person who knows the code to let you back in. Now, how do you get the attacker to let you back in? There's no exact way to guarantee re-entry; there's only hope on the victim's end. The victim will pay the requested ransom to the attacker and hope that they deliver the correct code for you to unlock your files. If they give the victim the wrong code, then, unfortunately, the victim is out of luck.


The data hostage fee from a ransomware attack can range from hundreds to thousands of dollars. More often than not, most companies can still not access their data due to the hackers either demanding an additional ransom or providing the wrong codes.

A ransomware attack can present itself in various ways, such as a pop-up showing your encrypted data and telling you that you need to pay the attacker's desired ransom to get them back. Moreover, it can infect your system or device in various ways.

# HERE ARE SOME STANDARD METHODS USED BY CRIMINALS



MALICIOUS FILE ATTACHMENTS & INFECTED FILES

DRIVE-BY DOWNLOADING

EMAILS CONTAINING FAKE INVOICES

UNPATCHED SOFTWARE VULNERABILITIES

**Ransomware** infections generally appear after criminals convince users to download malicious files, attachments, or applications from malicious emails. This prompts the script to run on a victim's device, initiating downloading of the payload. It eventually leads to the encryption of victims' data and, in turn, locking them out.

# Types of Ransomware

**"As ransomware criminals improve their malware payloads and related extortion schemes, a new attack will occur every two seconds."** ~ Cybersecurity Ventures

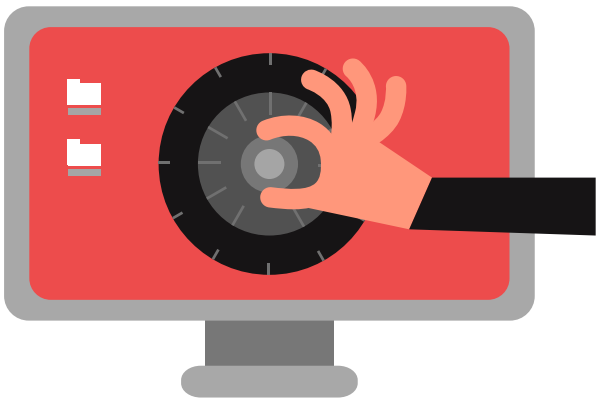
One of the most contentious issues in the IT industry is ransomware. This comes from the widespread effect of the WannaCry ransomware, which devastated thousands of businesses worldwide. Ransomware is constantly changing, making it challenging to keep up with the many strains.

Ransomware can be distributed via infected websites, emails, or malicious links. Once installed, it encrypts your files and holds them for ransom until you pay the specified amount. Ransomware is designed to be un-installable, leaving you at the mercy of your attacker and forcing you to pay their ransom to get your files back.

**Here are some common types of ransomware attacks you need to look out for-**

## WannaCry

In 2017, a ransomware assault known as WannaCry, previously affecting more than 150 nations. WannaCry infects a Windows machine and then encrypts the contents on your hard drive to prevent any user from accessing them. Then, the attacker will request a bitcoin ransom to unlock the files.



## Locky

Locky is one of the oldest forms of ransomware and was first discovered in February 2016. It's also one of the most effective because it encrypts the victim's files rapidly and spreads through phishing emails that contain an attachment that appears to be an invoice or other business document.

## Maze

Maze, another ransomware similar to Locky, was first discovered in 2017. The similarity between these two viruses lies in how their saved files appear on the screen. For example, if a Locky ransomware attacked you, the file would be saved as an extension. Locky; however, if it is a Maze ransomware, the file will appear as an extension. Maze. Maze also spreads via spam emails, though it usually requires you to open an attached file for it to infect your computer with malware.

## NotPetya

According to early reports, NotPetya is a ransomware variation of Petya, a strain initially discovered in 2016. However, researchers now think that NotPetya is a type of malware called a wiper whose only goal is to destroy data rather than demand a ransom.

## Scareware

Scareware is phony software that demands payment to fix problems it claims to have found on your computers, such as viruses or other issues. While some scareware locks the computer, others saturate the screen with pop-up notifications without causing any file damage.

## Doxware

Doxware or leaks threaten to publish confidential information about individuals or businesses online, scaring their victims into paying the ransom to stop this from happening. Police-themed ransomware is one variant. It poses as law enforcement and informs users that it has discovered illicit internet conduct and that they can avoid jail time by paying a fine.

## Petya

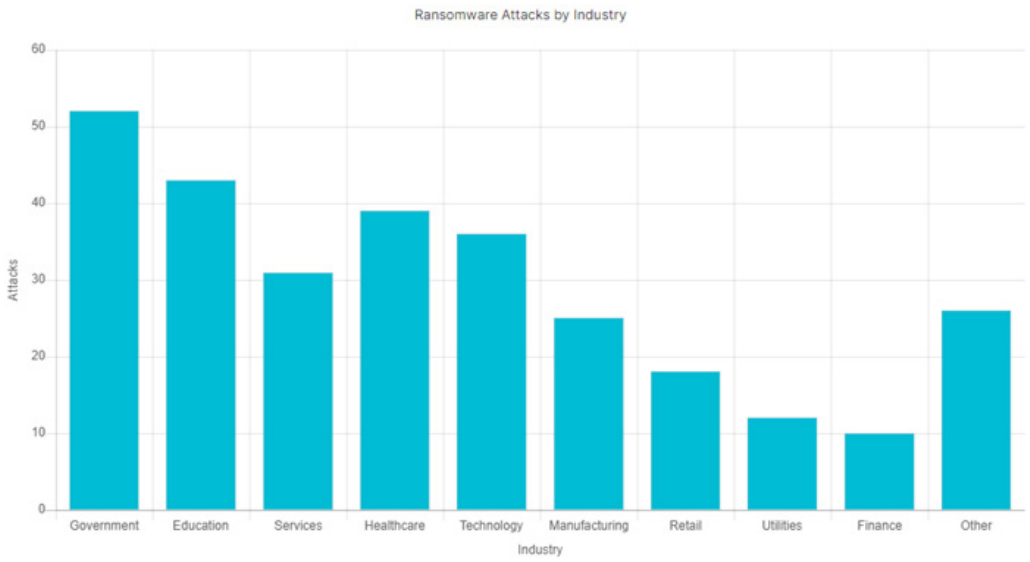
The Petya ransomware encrypts whole computer systems, in contrast to several other varieties. The master boot record is overwritten by Petya, which prevents the operating system from booting.

## Ryuk

Ryuk uses drive-by downloads or phishing emails to infiltrate computers. It employs a dropper, which installs a trojan and creates a permanent network connection on the victim's computer. When creating an Advanced Persistent Threat (APT), attackers can start with Ryuk and add tools like keyloggers, perform privilege escalation, and undertake lateral movement. On every other system, the attacker's access to, Ryuk is installed.

# Part 3: Damage Caused by Ransomware

For thousands of enterprises worldwide, the frequency and size of ransomware attacks are becoming a significant worry. Threat actors encrypt data belonging to various institutions worldwide, including private corporations, healthcare facilities, and governments, by taking advantage of security flaws.




The fact that some businesses agree to pay the ransom and keep the attack a secret drives ransomware operators to become even more inventive in their attacks and demand payments in the tens of millions of dollars range. Victims frequently do it out of fear of the negative social consequences.

# How Many Ransomware Attacks in 2021?

The number of ransomware attacks rose by 78% in 2021. Overall, two out of three organizations were affected. According to a collaborative analysis led by Cyber Security Works, there were 288 vulnerabilities linked to assaults in 2021, up from 223 the year before. The development of ransomware-as-a-service is primarily to blame for this increase in the reach and sophistication of attack methods. Making ransomware deployment less complex increases its accessibility.

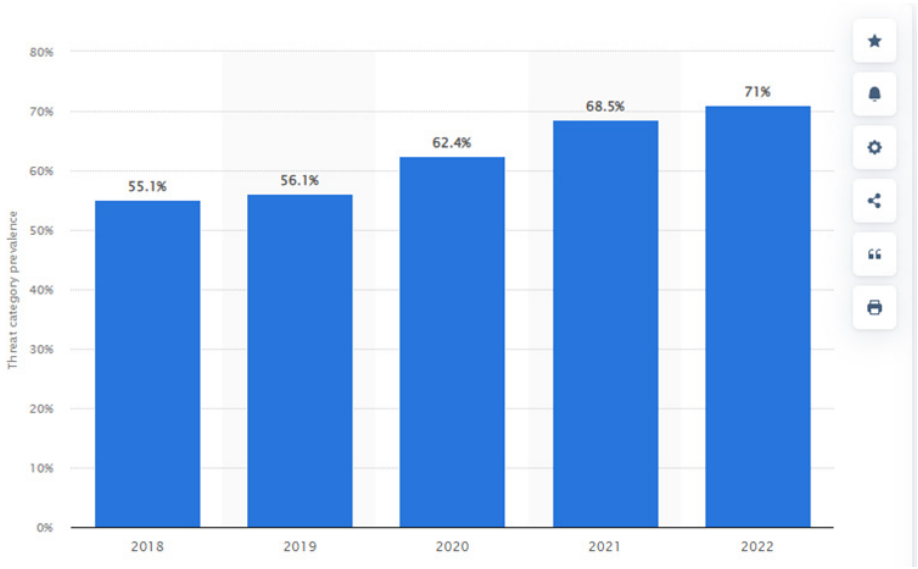

# How Does Ransomware Affect Small Businesses?

"As of 2022, ransomware damages will reach $20 billion annually."
~ CyberSecurity Ventures

Cybercriminals have historically targeted essential institutions, including governments, hospitals, and colleges. They knew these institutions might be rendered inoperable by an attack and had the money to pay a ransom.

But nowadays, 82% of ransomware assaults target small enterprises.

About 70% of organizations experienced ransomware attacks in 2022. This was the highest figure recorded thus far and rose from the preceding five years. Each year, more than half of all poll participants said their employer had fallen victim to ransomware.




**Ransomware attacks can be devastating to a small business. Some of the most common effects include the following:**

## Business Loss

Ransomware attacks can cause significant losses for companies that rely on their computer systems to conduct daily operations. These losses include lost productivity, revenue, customer satisfaction, and increased security costs.


## Reputational Damage

Public perception can affect any business, but it's essential for small businesses that rely on local support and word-of-mouth recommendations from customers and community members.

## Ransom Payment

If a ransomware attack hits your small business, the hackers will often demand a ransom. They usually require a certain amount of money to be paid in bitcoin, making tracking the payment extremely difficult. The hackers may also threaten to trash your data or expose it publicly if you do not comply with their demands.



## Regulatory Fines

Due to the nature of the attack, many businesses are unsure how they will be penalized by regulators when they report their data breach. Some states allow companies to report cyber-attacks after they occur, while others require them to report incidents within 24 hours of discovering them. While the penalty for non-compliance varies state by state, there's no doubt that it would be much better for your business if you could avoid any fines.

# Part 4: How to Protect Your Business?

**"Install security software and keep it up to date with security patches. Many ransomware assaults employ earlier versions for which security software countermeasures are available." ~** Steven Weisman, a professor at Bentley University.

The best way to protect your business from ransomware is to prevent it from happening in the first place. This means that you should be taking steps to ensure that your systems are secure and that the data they contain is protected.


## There are several different ways to do this

### AirGap Backups

An airgap backup is a copy of your data stored on a physical device that isn't connected to your network or the internet.

**How Does It Help?**

When an isolated system needs data, air gaps commonly deliver it via storage methods like USBs, firewires, or other removable media devices that transport data without an internet connection. This aside, AirGap also divides backups onto a separate VLAN (Virtual Local Area Network) to perform the backup from a hypervisor (software that creates and runs virtual machines) backchannel and not through a client-facing network.

**How to Do It?**

This backup server does not interact directly with clients. As previously stated, AirGap segments its backups onto a separate VLAN and is isolated, so it cannot talk to any virtual network your client may be on. What's great about how this works is that if your client were to download a malicious file accidentally, it would not destroy the entire backup network, as the infection cannot spread through the software since this backup has already been isolated.

# Protect Your Network

Firewalls are one of the best ways to protect your network and assets. They are often overlooked as a security solution but are extremely important. Firewalls monitor network traffic and stop anything it deems to be a threat. They're one of the most critical security solutions every business should have.

## Content filtering

Monitoring network traffic and blocking content that matches predefined policies.

## Deep Packet Inspection

Though similar to content filtering, DPI (Deep Packet Inspection) goes one step further. DPI sits between the client's machine and any internet traffic that goes in or out of their system; it captures the content being looked at and scans for any malicious content. If detected, DPI will hold the virus before it ever reaches your system.

## Public blacklists

A list of known bad actors or attackers maintained by public entities. It ensures quicker remediation of offenses and proactive blocking of offenders.

## Geo-blocking

IP addresses are registered based on region. Blocking these regions is possible if the area is known to conduct cyberattacks.

## Email filtering (in and out)

Third parties scan emails, including attachments, for malicious content or emails from bad actors. It is then possible to stop these attacks before they reach your infrastructure or leave it.

# Computer & System Maintenance

Computer and system maintenance includes examining the computer's performance, ensuring that automated system monitoring tools are correctly installed and configured, spotting potential security threats, and regularly backing up data.

### How Does It Help?

Your computer is a crucial part of your digital network and communication, so it has to have hardware and software that are specifically tailored to your office's computing requirements. The maintenance method is a component of a more comprehensive policy that defines what, how, and when the necessary changes can be made.

### How to Do It?

Schedule monthly operating system updates and bi-monthly firmware/driver updates. Our monitoring system for quality assurance then verifies these actions. Making a system correction, a system restoration, or a hardware component replacement might also be essential.

# 4. Network Segmentation

Network segmentation is the process of creating multiple networks within your organization. By doing so, you can ensure that no single network contains all of your clients, servers, or infrastructure appliances.

**How Does It Help?**

Segmenting different functions within a network will prevent an attack from spreading from a device previously used by a client to any underlying critical infrastructure, like a backup. This restricts any lateral movement of an attack.

**How to Do It?**

Each client is configured with a dedicated VLAN (Virtual Local Area Network). These VLANs each have a unique network, which cannot access other clients or infrastructure appliances. Each VLAN has its firewall rules, so if an attacker gets into one client's network, they cannot access other clients' data or infrastructure devices.

# 5. Least Privilege Access and Data Security

Regarding information security, the Principle of Least Privilege (PoLP) refers to the situation when a user is only given the bare minimum of network access or authorization. The user can only carry out their duties or other necessary tasks thanks to this.

**How Does It Help?**

Less privileged access minimizes a network's attack surface. A compromised user account can only harm the user's data with direct access. If a regular or standard user has too much access to your data, when their account is compromised, it can do far more damage.

**How to Do It?**

User accounts are not allowed admin access, and permissions are strictly delegated. This ensures that attackers cannot do much damage even if your system is hacked because they cannot access critical systems like databases or servers.

# 6. Staff Training & Phishing Tests

Educate your employees about standard phishing emails and other threats leading to ransomware infections. Test them by sending them simulated phishing emails periodically.


**How Does It Help?**

Most attacks originate from uneducated users. Teaching users technical skepticism is critical in preventing intrusion.

**How to Do It?**

Hold quarterly or bi-annual training seminars with your staff and teach them what to look for when it comes to a potentially dangerous email. Conduct interactive training methods to show them what is out there and how it can be detrimental to your company. Also, try to implement security solutions that prevent malware from being installed on your systems in the first place (anti-virus software and firewalls).

# 7. Multi-Factor Authentication

The most effective way to protect your business from ransomware is to implement Multi-Factor Authentication (MFA) solutions. Most organizations are aware of the need for MFA to log into their corporate networks, but they may not realize how crucial it is in protecting against ransomware attacks.

**How Does It Help?**

It prevents someone with the correct username and password from gaining access by requiring a second layer of verification.

**How to Do It?**

At the client's request, we implement 2FA (Two Factor Authentication) in terminal server environments, requiring a user to enter this second verification code before working in the data center environment.

## 8. Proactive Monitoring

Proactive monitoring monitors a broader set of business systems beyond critical ones. This allows us to see if anything suspicious is happening on your network before it becomes a problem. It also lets us know when changes in privileges or permissions may indicate that someone has gained unauthorized access to your network infrastructure.

**How Does It Help?**

It allows staff to act before an issue begins to impact clients by defining thresholds that alert before it affects the user. This can be used to monitor mission-critical conditions or to predict future problems by looking at trends in historical data.

**How to Do It?**

We feed into picking the right tool and serving insights to stakeholders and your team so you can have a cohesive, scalable monitoring strategy and prevent issues beforehand. We monitor the network, servers, VMs, and out-of-band management using custom thresholds tuned over years of management.

# Part 5: Best DIY Software for Protecting Against Ransomware

Suppose you have fewer than five employees or are a lone proprietor. Perhaps you should wait a little while before investing in managed cybersecurity or IT services. During this time, you may be able to implement some fantastic DIY software to protect your organization unless you are subject to government compliance regulations (healthcare, legal, medical, or education).

Keep in mind that, aside from the minor offices, a DIY method is occasionally not cost-effective when calculating the total cost of cybersecurity.

## 1. Malwarebytes

Malwarebytes' free version of this tool will scan your computer for threats, and it can remove most of them. The paid version offers more features, including a real-time scanner that protects you from malware as you surf the web.

## 2. CryptoPrevent


CryptoPrevent blocks ransomware before it can do any damage to your files. It also has a self-defense mode that prevents ransomware from spreading to other computers on the network.

## 3. Windows Defender

Windows Defender is built into Windows, so downloading anything is not needed. If you're using an older version of Windows, you'll have to download the software from Microsoft. The updates in Windows Defender work almost daily with new patches and fixes. It will help if you run updates on it monthly - although we prefer you do it every week - to stay up-to-date and secure.

## 4. SpamHero

SpamHero is an excellent tool for businesses that want a simple way to block spam and malicious emails. It has been around for years and has earned quite a reputation for being effective at stopping malicious emails from getting through. Since Spamhero is a paid email filtering service, it's worth it. If you want to opt for this service, Protected Harbor can help you get a discount on their services, where we would, in turn, receive a credit.

## 5. Duo 2FA

With user-friendly features for safe access, robust authentication, and device monitoring, Duo 2FA (Two-Factor Authentication) apps and access solutions can simplify security resilience for your business. This tool is perfect for stopping brute-force attacks.

## 6. Macrium Reflect

Macrium Reflect is a powerful software tool that allows you to create backups of your entire computer system, including its operating system and applications. The program has an intuitive interface that allows anyone to use it without training.

## 7. Snort

Snort is a free and open-source Network Intrusion Detection System (NIDS) and Network Intrusion Prevention System (NIPS) developed by Sourcefire, now part of Cisco Systems. Snort is one of the most widely used IDS/IPS systems, with over 1 million monthly downloads and over 800,000 registered users.

## 8. Squid

Squid is one of the best free software to protect your business from online threats like ransomware, spyware, and phishing. Squid is a free and open-source web proxy cache. It supports caching and forwarding for HTTP, HTTPS, and FTP protocols. Enterprises have used Squid for various purposes, from Internet service provisioning to website acceleration to circumventing censorship to anonymizing private information.

# Part 6: How a Managed IT Service Provider Can Help

Many businesses have installed next-generation firewalls, spam filters, and anti-virus software. Although these tools will help them keep an eye on their network activities, it is up to the IT team to respond to malicious attacks and fix compromised devices. Bringing in an experienced team to help with the rise in threats can provide a level of service beyond what firms currently have and at a lower cost.

Companies like Protected Harbor provide various benefits like cost-saving and advanced protection beyond off-the-shelf solutions. And better IT performance for organizations. They will ensure that your business is protected from outside threats with well-tested, proven, and integrated technology.

Ransomware is constantly improving, becoming stronger and faster with each passing moment. Protecting your business and your clients are more likely than not your company's top priority. It also Protected Harbors.

Protected Harbor has helped support businesses' cybersecurity and compliance management programs for the past decade. From implementing required security controls and automating the data collection needed for compliance reporting to assisting with audits and reports to regulatory authorities, outside teams like Protected Harbor bring years of actionable experience to strengthen your company.

Our team stops ransomware before it even has a chance to try and harm your infrastructure. With making backups and recovery your top defense against these hackers, we also offer a blend of offensive and defensive security expertise and 24/7/365 monitoring of your systems. We help protect your employees from falling for the simplest to the most complex malicious activity while offering full safety measures for your most desirable data.

Protected Harbor is a family-owned, managed IT service partner for companies and organizations throughout the tri-state. We take responsibility for the technology and applications that keep your business moving forward. We turn IT into a competitive advantage by eliminating outages, speeding up systems, improving productivity, and lowering costs.

We pride ourselves on our customer's happiness. That's why we ensure our 24/7/365 customer service is second to none. Whenever you need us, we're always here. Got a problem at 2:00 am? A live person will answer your call and resolve the issue before sun-up.
Our approach to customer service goes beyond just solving problems and closing tickets. We aim to connect on a human level, getting to know you and your business so we can function like an extension of your team.

That is why over 90% of our business comes from client referrals, and we have a 98% customer retention rate. Protected Harbor is the last I.T. company you will ever have to hire

**Call today for a free cybersecurity assessment and IT Audit at 201-957-1616**

E&F
ESBIN & FEINMESSER PLI

# Introduction

Esbin & Feinmesser, PLLC is a boutique law firm that prides itself on offering legal and advisory services that match those of large corporate firms while crafting a more personal experience for its clients. Being in practice for over 20 years, they have a lot to protect. Partner Scott Esbin explains, “as a law firm, we're just inherently conservative about putting our data and files in somebody else’s hands. There's a whole host of rules that we have to abide by in terms of client confidence and security. Law firms can be brought down ultimately, and lawyers could theoretically be sanctioned if they're not careful about how they treat their data.” With all the news in 2019 of the cyber-attacks on corporate giants like  Facebook and Citibank, his firm’s security was heavily on his mind. Esbin knew that they would likely close the business when client confidence was lost. He would have to have many very tough conversations with clients and employees.

## AT A GLANCE

- Ransomware attack shut down this lawfirm and put them on the defensive.
- Refused to pay $200k ransom
- 4.8 terabytes of data recovered
- Decresed I.T. costs by 50%

# Challenges

Despite the trend at the time toward cloud-based storage, Esbin wasn’t convinced it was the proper course for his firm. He found an IT provider he thought could help.
The vendor seemed like a good fit for Esbin & Feinmesser initially, but things began to shift over time. There was no cohesive, intentionally-developed plan to achieve the organization’s goals and satisfy its security needs. The proposed solutions were often a quick-fix of new software with more equipment.

Esbin & Feinmesser housed their data in the office to circumvent Esbin's fears about cloud technology. They had more machines in the office than employees. There was way too much volume with no design, so it was not enough to keep the business safe—and those choices cost Esbin dearly. "We had to pay for our licenses. We had to pay for people to come in. We had to pay for hardware when a computer would bust. It was expensive. I would have spent $50,000 - $100,000 more on computers and, licensing, other costs." Esbin recalls.
Then in March of 2020, what Esbin had always feared, happened...

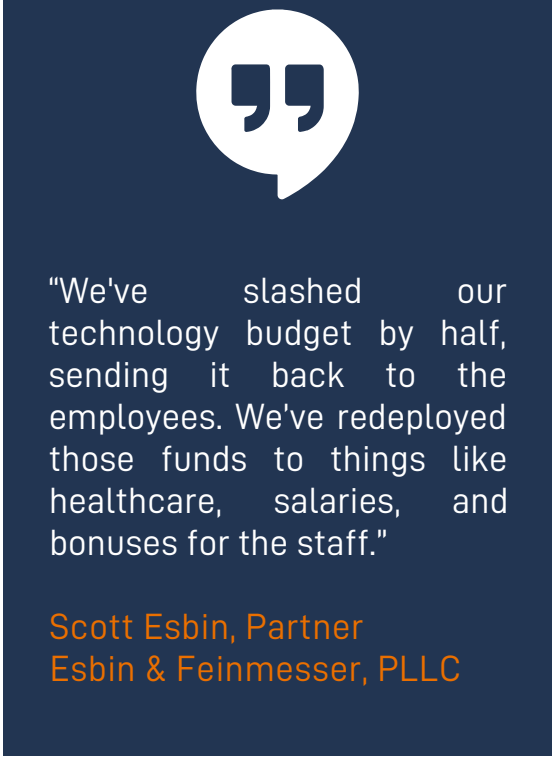
## Challenges (continued)

"We got hacked," Esbin shared. "We couldn't access email. We couldn't access our servers. It was like somebody came in and put a giant padlock on all of our stuff. We still, to this day, don't know exactly how it happened. We think it was a bad attachment somebody opened." Rather than giving in to the ransom of $200,000.00 USD, Esbin immediately knew he needed a new IT provider that could help him regain access to his business. Still, more than anything, he needed better protection so this could not happen again. Keeping the servers in his office did not prevent intruders, but he still had doubts about cloud-based storage. Protected Harbor sat down with Esbin and listened to his concerns. He worried if his data was safer sitting next to him in the office or the cloud. How could the firm stay safe? How can he make sure this doesn't happen again? How could he keep an employee from making a mistake that may take down the company?

## Solutions

Protected Harbor calmed these fears quickly by explaining how the process would work, why cloud-based storage was safer, and how they would protect him from future attacks with monitoring and redundancies. Then they worked as a team to put the pieces of Esbin & Feinmesser back together. Nick Solimando, Director of Technology at Protected Harbor, said he believes "ransomware hit the servers in our client's office. It got down to cryptic system files to the point where servers wouldn't even function properly and wouldn't boot up properly. None of their file shares were functional." Fortunately, none of their data was leaked and some of the data were not infected so severely that Protected Harbor could look at those files. The equipment, on the other hand now essentially scrapped metal. Solimando illustrated Esbin & Feinmesser's new security measures saying, "Our goal is to put clients in a protective bubble. We don't want you to worry about the IT—so you can focus on your business."

Protected Harbor always starts with an audit of the client's current system and what their needs are. But this migration was unique because. Esbin came with only pieces of data, and the plans were down. So
Protected Harbor analyzed the entire picture to see what was salvageable and asked Esbin what functions were most important for recovery. "We have a lot of unique programs that we use that are proprietary," Esbin immediately answered. "They're unique to us; we own them. If I don't have them, I don't operate." In the end, Protected Harbor worked with Esbin's
programmers to reconnect and successfully integrate the custom application. Protected Harbor was able to recover 4.8 terabytes of data and only 200 gigabytes were ultimately lost. They managed to retrieve a
suitable backup file about two months old, but it was valid and able to be restored. Out of roughly ten years' worth of data, Esbin was only missing a fraction of data, but their system was restored, and they could continue operating.




## Solutions

Protected Harbor even worked with end-users to recreate their environments so that their files and access were back to normal after less than a month. As Esbin & Feinmesser's systems returned online, they needed to be fully protected. "We put them in a virtual environment in our data center and gave him his dedicated virtual network. So it's just him in there, nothing else. He's segregated and isolated." Solimando elaborated. Malware scanning and monitoring are a part of Protected Harbor's default environment. The monitoring services are comprehensive and prevent threats instead of reacting to them. Esbin now benefits from constant monitoring for things like RAM, CPU, and disk space to ensure everything is performing as it should. If it's lagging, Protected Harbor is already looking into it and resolving the issue before the end-user is impacted.

Known malicious IP addresses, attack vectors, and even whole countries are blocked out, not allowing anything to penetrate the network. Redundant internet, firewalls, switches, virtualization nodes, backup architecture, and mechanisms help prevent errors and maximize uptime. If there is an issue, the backup files are completely inaccessible from where the admin users are. “Most likely, the ransomware they got hit with before would never even reach the server today,” Solimando assures. “It would get stopped by one of the protections upstream from them. If it got through all of that, we would be able to recover them inside of a day, probably less than 12 hours.”

## THE RESULT

Today Esbin is grateful that the hack happened when and how it did. He quotes, "'Fear is the mind-killer.' It's a line from a movie called Dune, but I think that's probably the biggest lesson I've learned from this.

I think that we were lucky that we got hacked. It's true because having what we have now works better than anything we've had in the past."

The lesson cost was high, but Esbin recognizes that the infiltration they experienced could have been much worse. Fortunately, none of his client data was taken or accessed. It was locked away, so they could not access it without Protected Harbor's services.

Esbin has a new confidence level as he knows his business is adequately protected. He has the support he needs, and when his company grows or changes, Protected Harbor will design a solution for him based on his individual needs.

There's always someone to answer Esbin's calls, even for help with the simple things that cause significant problems, like figuring out how to print on both sides of the page. He's received all the personal service and hands-on assistance he needs.

The cost savings with Protected Harbor is also significant. Esbin was pleased that while he's reduced his IT costs by roughly 50%, he has gained security, expert assistance when needed, and more peace of mind.