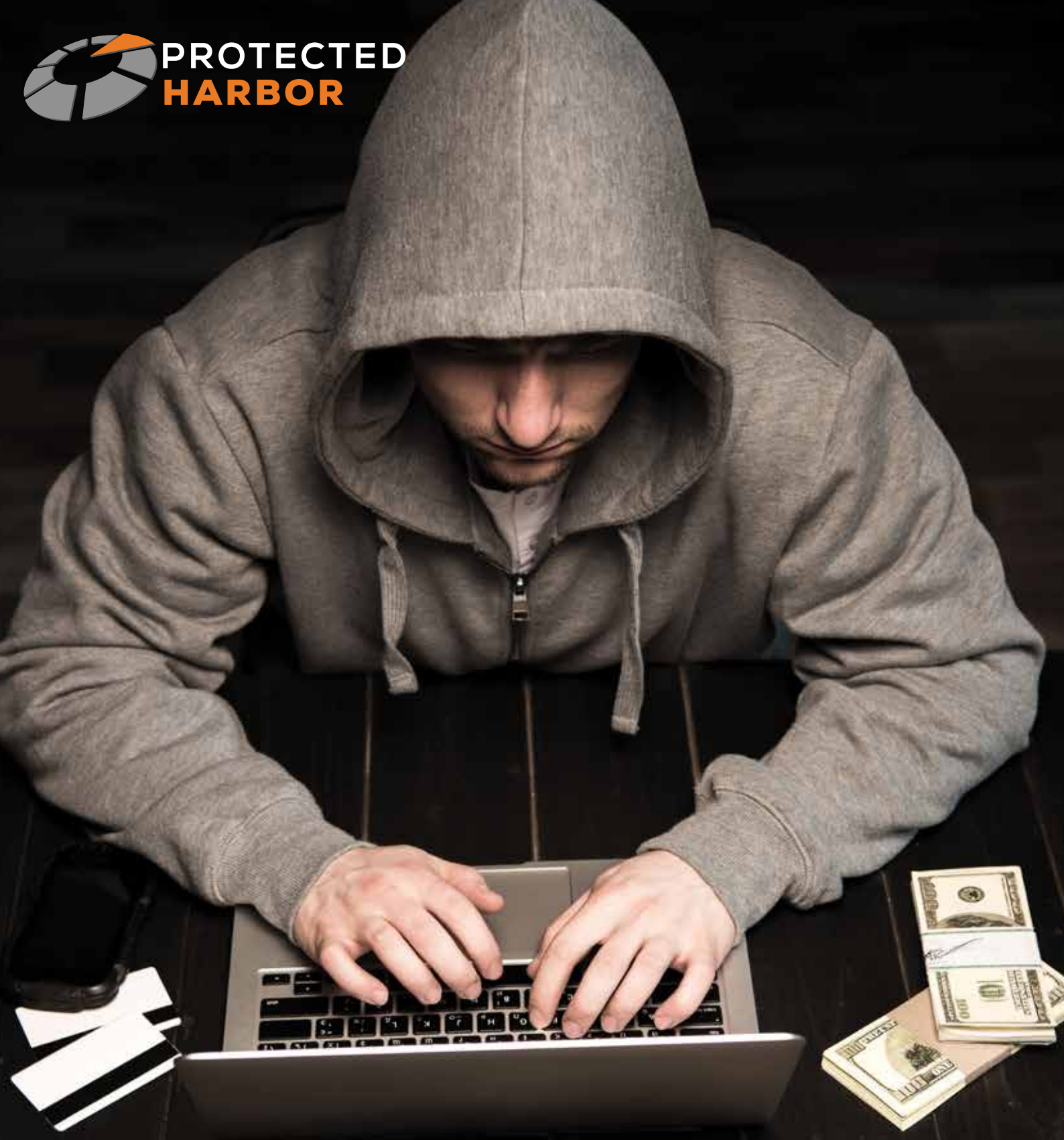
PROTECTED HARBOR



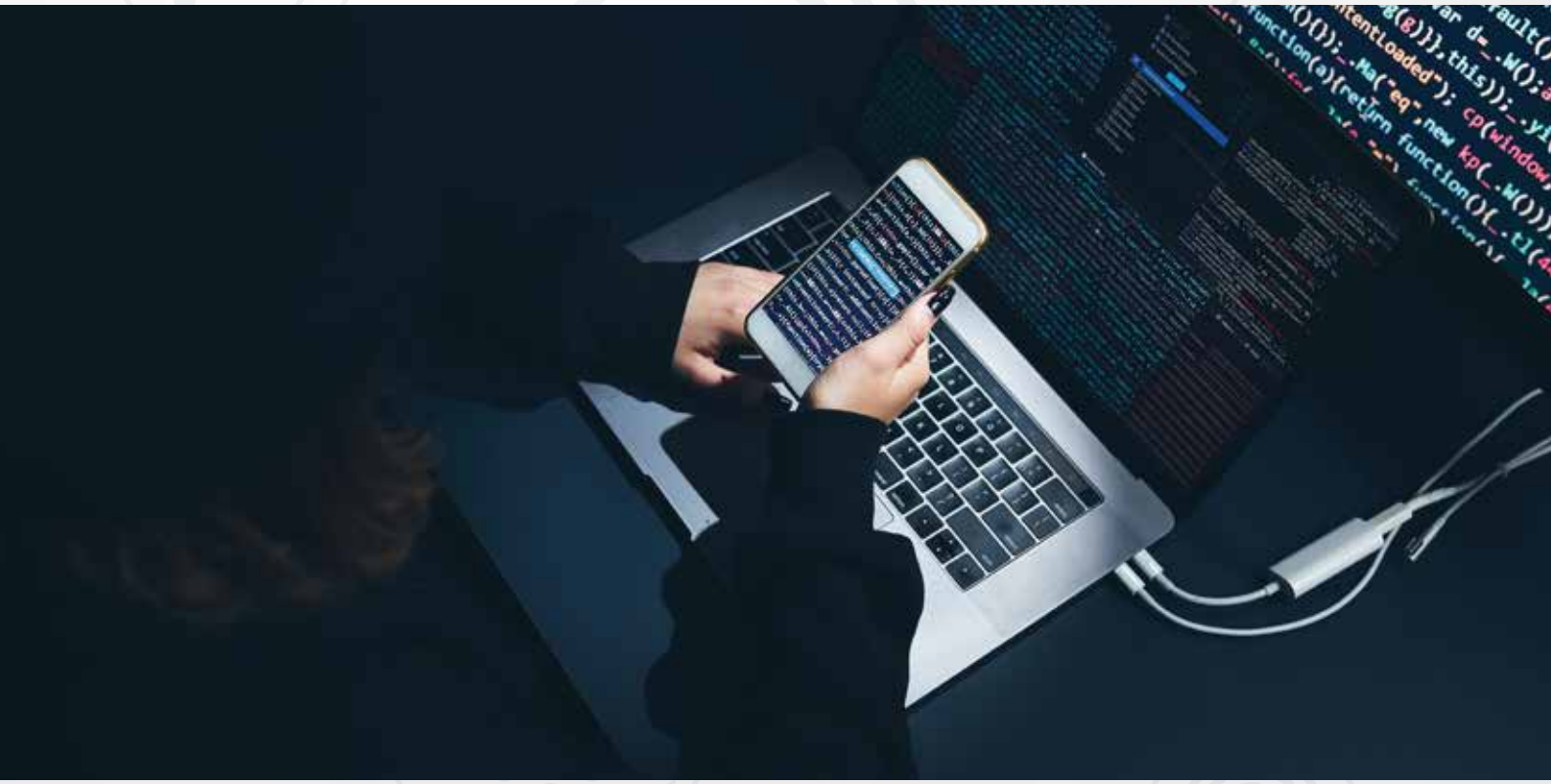
TOP LAW FIRM CYBER ATTACKS THROUGHOUT HISTORY

INTRODUCTION

Experts believe we are on the verge of a cybersecurity catastrophe. Hackers and scammers are at an all-time high with the frequency and sophistication of their cyber-attacks. Criminals have never had easier than today's technology to try and exploit potential victims' security flaws. Various individuals as well as organizations are being attacked, and law firms are no exception.

According to a survey conducted by the American Bar Association (ABA), the number of law firms that had experienced a cybersecurity breach in 2020 has increased from 26% in 2019 to now 29%. This means that enhancing cybersecurity is more of a necessity than ever before, especially for law firms with high-profile clients like Google.

The threats posed by hackers and other hostile actors are becoming more widely recognized in the legal community. These criminals attack law firms of all sizes, including those on the larger scale finding that law firms aren't responding quickly enough to the growing threat.



WHY WILL LAW FIRMS CONTINUE TO BE A PRIME TARGET?

The answer to this is simple: law firms hold sensitive information about their clients, and they store this information in databases that can be accessed or stolen by hackers.

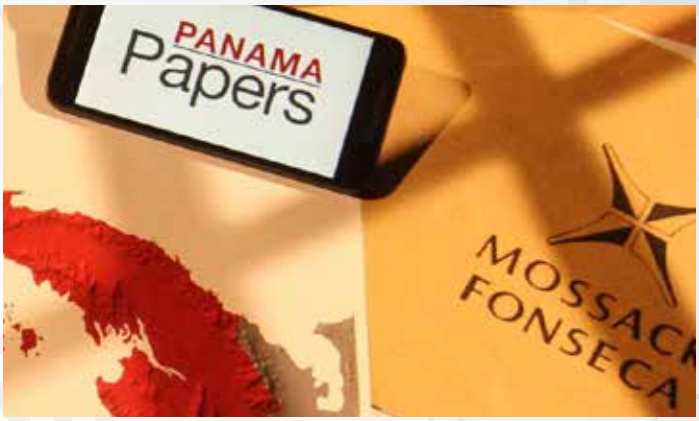
Cybercriminals target law firms to sell sensitive client information on the Dark Web or use it to try and extort clients. Furthermore, law firms often handle large amounts of money and confidential documents making them prime targets for phishing scams and ransomware attacks.

FAMOUS TOP LAW FIRM CYBER-ATTACKS

Let's take a look at some of the most well-known law firm security breaches in the world:

MOSSACK FONSESCA & THE PANAMA PAPERS

The Panama Papers have been described as one of the biggest leaks in journalism history. The leak revealed how some of the world's wealthiest people have been using tax havens in order to hide their wealth. The revelations led to protests in Iceland and more than 10 high-profile resignations, including that of Iceland's prime minister.



According to reports, the breaches included 11.5 million classified records from the 1970s to late 2015. Mossack Fonseca told the BBC their firm had been hacked by servers based abroad and that it was working alongside Panamanian authorities to investigate the incident and made no other comments in regard to the situation.

The Panama Papers also led to protests across Iceland and other countries where people called for transparency over political leaders' financial interests.

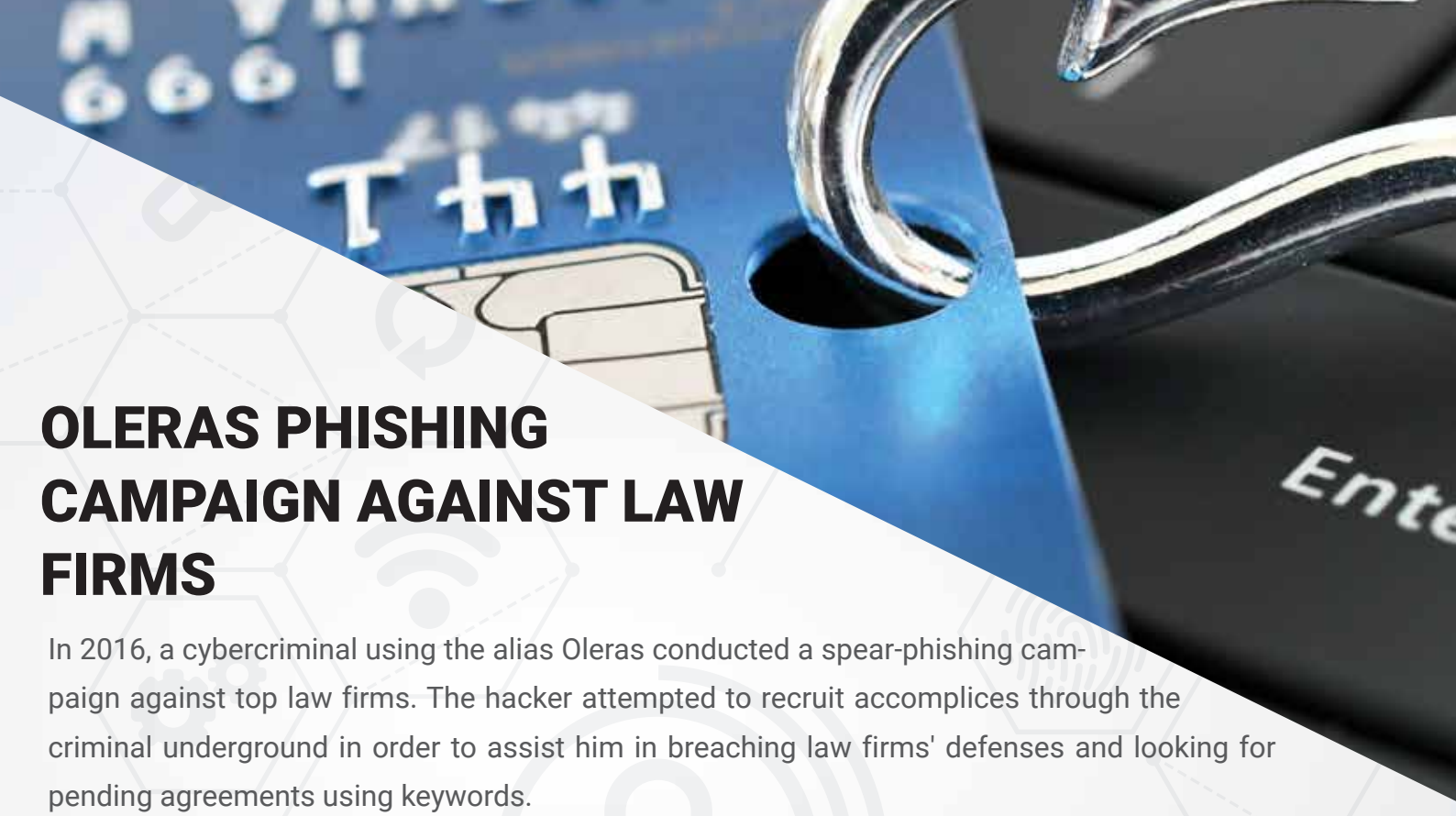
JP MORGAN CHASE

The JP Morgan Chase cyber security incident in 2014 was one of the most publicized data breaches to date. The attack involved the theft of sensitive personal information belonging to more than 76 million households and seven million small businesses through a sophisticated breach on its servers.

It was the hack heard 'round the globe due it’s success in breaking the world’s largest bank. Names, addresses, phone numbers, email addresses, and private, internal user information was hacked in more than half of all U.S. households in 2014.

The hackers even gained "root" rights on more than 90 of the bank's servers. Root rights or rooting grants a hacker to access to any Android operating systems. This gives the hacker access to manipulate any software codes or to install new software that, for example, this bank wouldn’t normally do. This allowed them to move money and terminate accounts.

The final hacker was apprehended in 2016 in New York, but their wire fraud and money laundering totaled more than $100 million between the years 2014 and 2016.



OLERAS PHISHING CAMPAIGN AGAINST LAW FIRMS

In 2016, a cybercriminal using the alias Oleras conducted a spear-phishing campaign against top law firms. The hacker attempted to recruit accomplices through the criminal underground in order to assist him in breaching law firms' defenses and looking for pending agreements using keywords.

Oleras presented a strategy to run keyword searches in law firm computer networks for papers that included merger information, offering a hacker $100,000 plus extra 45,000 rubles ($564). But first, the hacker would have to gain access to the law firm's computer networks. Oleras is said to have advised spear-phishing assaults on employees who had submitted their names, email addresses, and social media account information.

The scheme started with an email first sent to the firm's client that included malware. Once opened, the malware would collect information about the user and send it back to Oleras. Then Oleras would use that information to access the law firm's network and transfer funds from trust accounts into his accounts.

The firm recovered most of its money, but not before paying a $5 million ransom to Oleras for his silence.

UPMC PATIENTS

A group of hackers managed to breach the email accounts of multiple doctors in order to gain access to sensitive patient medical data.

CJH (Charles J. Hilton, P.C. Attorney at Law) sent UPMC (University of Pittsburgh Medical Center) a breach report in December 2020, confirming that the people who broke into the email accounts did have access to patient data. The data utilized by CJH to offer its contracted billing-related legal services to UPMC was among the patient information compromised in the assault.

The breach has exposed personal data of patients. However, it's unclear how many patients were affected by this attack, but experts believe it could be millions.

MOSES AFONSO RYAN LTD & THE RANSOMWARE ATTACK

According to a lawsuit filed in U.S. District Court, an unknown person or possibly group kept a Providence law practice hostage for months by encrypting their files and demanding a $25,000 ransom in anonymous cyber money for recovery access.

The firm's billing system and documents were specifically blocked, making it impossible for clients to pay and vital financial information to be accessible.

Because the value of the encrypted material was so high, the legal firm's officials decided to give in to the hackers' demands. They paid the hackers in Bitcoins, but they did not supply the decryption key and went on to demand more money.

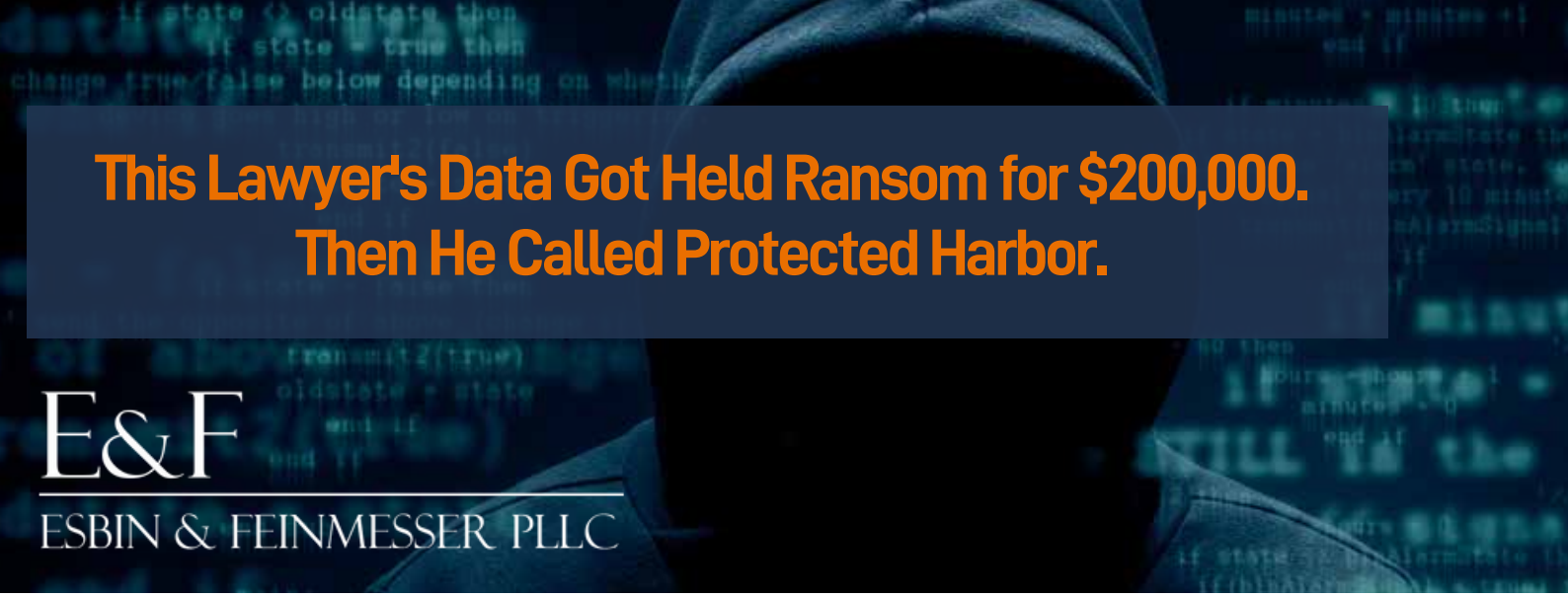
The law firm made arrangements to buy more bitcoins in return for various tools to recover its records, hoping that the insurer would reimburse them for all of their costs. They unfortunately did not.

CONCLUSION

It's vital to remember that cybercriminals stand to gain a lot by harming your business, and their chance of being discovered is low. The perpetrators are rarely apprehended, and some businesses never recover.

Both large and small law firms are at risk. When a security breach occurs, the only thing a company can do is notify their clients and try to determine how much information was compromised.

Prevention should be preferred over damage control, though some businesses think otherwise. Don’t become a victim. Take the proper steps to ensure that you know how data loss can occur and what you can do to protect your networks, databases, and staff accounts from being next on the hit list.



This Lawyer's Data Got Held Ransom for $200,000. Then He Called Protected Harbor.

E&F
ESBIN & FEINMESSER PLLC

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 weighing heavily on his mind. Esbin knew that in the event of an attack, he would be faced with many tough conversations not only with his employees but with his clients. If he were to lose his clients confidence, it would be likely that he would have to close his business for good.

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. Though keeping the servers in his office did not prevent intruders, 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 collaborated 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 was not infected severely so that Protected Harbor could still look at those files. The equipment, on the other hand was 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."

> "We've slashed our technology budget by half, sending it back to the employees. We've redeployed those funds to things like healthcare, salaries, and bonuses for the staff."
>
> Scott Esbin, Partner
> Esbin & Feinmesser, PLLC

Protected Harbor always starts with an audit of the client's current system and what their needs are. 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 small fraction worth of data. Their system was restored, and they are still operational.

Solutions (continued)

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 their 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 hackers 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.

ABOUT PROTECTED HARBOR

Protected Harbor provides customized data center infrastructure management and appli-cation migration support to businesses looking to scale their technology and bottom line. With over 15 years of service and a 99.99% uptime record, our team is fully committed to creating, maintaining, and managing the high-est quality application operations environment experiences. Your uptime is our focus. Our 90+ Net Promoter Score, and 95% client retention rate back up that claim.

Our Protected Data Center is an integrated suite of managed services focused on the uptime of your appli-cation at the lowest possi-ble cost, regardless of location, and cloud pro-vider. From infrastructure design to network operations including security, storage, connec-tivity, remediation, monitoring, and more. Protected Data Center provides end-to-end support to secure deployments of complex enterprise applica-tions to protect your tech-nology infrastructure investments.

Like everyone else, we o er Cybersecurity, Enterprise Networking, Infrastructure Design, Network Con guration, Monitoring, Customized Protected Cloud, Change Management, & Protection & Recovery.Unlike everyone else, we listen, learn, think, and do not blindly deploy. Focusing on durability and uptime, we design a custom architecture solution integrated with a seamless migration process. The entire time we keep your business up and running with our proprietary application outage avoidance methodology (AOA) providing redundancy and high availability.Protected Data Center features a global helpdesk with level 1, 2 & 3 support, 24/7 NOC, a Tier 3 Data Center, best-in-breed CMDB solutions, and years of experience & knowledge from working with leading technology companies.

PROTECTED HARBOR

Protected Harbor, Inc., 60 Dutch Hill Road, Suite 16, Orange-
burg, NYSuite 16, Orangeburg, NY
Email: sales@protectedharbor.com
Phone: +1 201-957-1616