PROTECTED HARBOR

Because IT Matters

TREND REPORT

2023 LAW FIRM DATA BREACH

TABLE OF Content

INTRODUCTION

The legal industry has changed drastically over the years due to a combination of both the pandemic as well as the rise of cybercriminals trying to infiltrate cyber infrastructures.

With digital platforms, software, and apps offering newer and faster programming daily, it's hard to know which one is right for your company. However, all these technological advances strive to go after the same thing for companies and clients worldwide: a more straightforward, faster, and more effective method that you receive for using their platforms. Now, this all sounds great for law firms as they need to satisfy their clients and keep pace within this fast-changing world of technology, which also means they need to work on protecting their data first and foremost.

Data has become one of the most important aspects of a business in this digital age. Law firms especially tend to face the greatest risks from data leaks, including significant reputational harm and financial loss. Data loss and prevention have become one of the businesses' most severe security challenges. When the volume of data grows for a company, data breaches occur more frequently, drawing in financially motivated actors and hackers.

sales@protectedharbor.com ✉
@protectedharbor f
@protectedharbor g+
@protectedharbor 🐦

AMERICAN BAR ASSOCIATION

2022 LEGAL SURVEY REPORT

27%
EXPERIENCED A SECURITY BREACH

46%
OF ATTORNEYS REPORTED THEY HAVE CYBER LIABILITY

42%
OF RESPONDENTS HAVE AN INCIDENT RESPONSE PLAN

TRENDING ATTACKS FOR 2023

EMAIL HACKING AND PHISHING SCAMS

Hackers follow patterns and will try to email you from an address similar to the one you may be familiar with. Take the ending of Protected Harbor's email address, for example, @protectedharbor.com. A hacker can easily change the ending of their address to @protected1harbor.com or @protectedharborr.com, tricking the receiver, who may not be paying close enough attention. Once one of these malicious links is downloaded onto your system, it can be challenging to get rid of as it can spread through the corporate network and compromise sensitive data.

RANSOMWARE

With ransomware, hackers can encrypt all your data, rendering it useless and demanding a ransom payment in return for the key to your files. Hackers find their way in through emails, making them dangerous to even view as a virus can be hidden through micro-coding and download itself automatically to your system.

MOBILE ATTACKS

Attacking cell phones by leveraging mobile access to data as an attack point. Stemming from 2022, spyware software like Pegasus has been known to access and compromise the phones of important government officials, causing this area of attack to grow exponentially.

WORKPLACE AND DESKTOP ATTACKS

Though these attacks are nothing new, cybercriminals are still trying to get in through your company's infrastructure regardless of the industry they're being practiced in. They are looking for that open window within your locked house, whether it's through a phishing email or ransomware email as stated above or through malware and micro coding, these hackers are looking for a way to compromise your company's infrastructure, and they're only getting stronger.

In-House Threats to Your LAW FIRM

LACK OF EMPLOYEE SECURITY TRAINING

Like most people, employees have probably encountered their own personal slew of phishing emails which should give them the upper hand in spotting them at the workplace, right? Unfortunately, not necessarily. Nowadays, these hackers are growing in sophistication with how they set up and deliver their emails.

Whether the email is set up as a ransomware attack or a bad actor hoping for you to fill in some personal information, if your employee needs to be properly trained on what to look out for, this can easily cause a data breach for your company.

LACK OF USER RESTRICTIONS

Let's face it; times have changed. Gone are the days when every employee is reporting to the office. Gone are the times when you could place all your files onto a shared network without second-guessing who may have eyes on it. Prying eyes are everywhere – sometimes they're from complete strangers looking to break into your files, but sometimes they're also from those closest to the company.

Allowing full user permissions to all employees puts your firm at significant risk. Not only is it a risk for files becoming corrupted by employees – whether by accident or on purpose, but a corrupted file with a virus can take down an entire infrastructure. Think of your shared server as a punch bowl; if somebody wants to spice things up, they spike the punch bowl, affecting everyone who takes a drink from it.

LACK OF 2-FACTOR AUTHENTICATION (2FA)

Though this feels like a tedious task, having a lack of 2FA can affect your safety and security. 2FA adds that extra layer of protection that is needed regardless of if you work in a legal firm or any other business sector. You need to make sure your most private and personal data is protected.

UNDERSTAFFED & UNDERFUNDED IT DEPARTMENTS

If you're a small firm just starting out or a top-tier firm within the industry, let's face it, IT safety and protection is usually the last thing on anyone's mind. Whether or not you have an IT department that you rely on or some guy named Jim that you use to fix random issues around the office, they're probably not enough to keep your company safe. Most IT staff, especially now, are typically understaffed and overburdened with the usual given day-to-day tasks. This leaves little time for them to improve their security infrastructure, as they always react rather than improve. It doesn't help that much of their time is spent on manual tasks like creating tickets, which could easily be automated.

HOW TO STOP THESE THREATS FROM HAPPENING

TRAIN EMPLOYEES

Working with expert engineers and setting up phishing simulations can help your employees to spot the difference between a legitimate email and a phishing email. They'll learn to look closely for the common and trending practices among these cyber criminals and will begin questioning every email they receive before clicking on any suspicious links.

LIMIT USER RESTRICTIONS

Limiting your employees' access can be a huge game changer when it comes to keeping your data safe. Let's be honest. A CEO of a company shouldn't have the safe permissions as an entry-level employee. This, in turn can save your files from potential prying eyes as well as file corruption. Remember, when you're on a shared network with shared files being open by everyone, all it takes is one infection within a computer to spread to a file and spread to every user's system after that. Keep your data safe by limiting what others have access to, only providing them with the necessary files and permissions.

MANDATORY 2-FACTOR AUTHENTICATION (2FA)

Instilling a mandatory 2FA for all employees, regardless of position, when it comes to any device, they use to log in to any of your firm's systems. This will add a guaranteed extra layer of protection, especially on the off chance that an employee's credentials become compromised, or they lose their usual work devices. This will make it extremely difficult for the hacker to break in as they will need to either pass a security question or receive a verification code through the employee's phone by text.

ZERO-TRUST POLICY

Our experienced engineers at Protected Harbor work on a zero-trust policy with our clients. This means, regardless of whether or not you are the CEO of the company or an admin, we do not allow for any worker to download any file to their system without our team first doing a thorough investigation of the files. That includes any updates, new software to download from the internet, or any files linked within an email. This helps to protect your and your company from comping into contact with any malicious links or micro code that can damage your company's infrastructure.

UNDERSTAFFED AND UNDERFUNDED IT TEAMS

Though there's no easy way to solve this problem, there are a few options. One would be to ensure that you have a dedicated IT team just for your staff, not somebody who works in multiple departments trying to fix the gap within your understaffed IT team. Another would be to truly evaluate the current IT team you have. We mentioned earlier how your current team may just be reacting rather than improving and we want to expand on this a bit further. What we mean by reacting is almost what it sounds like, they are waiting for the shoe to drop instead of finding ways to prevent the shoe from ever dropping. They aren't improving their current ways of getting ahead of tasks whether it's because they're overburdened by the amount of work that needs to be done or they're complicit in their ways.

A way that we personally recommend fixing this potential lack of security is by bringing in a managed IT service provider.

BRING IN A MANAGED IT SERVICE PROVIDER

Many law firms have installed firewalls, spam filters, and anti-virus software that are next-generation. Although these tools will help keep an eye on network activities, it is up to the IT team to respond to any 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, superior protection, better IT performance, and advanced technology to organizations. They will ensure that your organization is protected from outside threats with well-tested, proven, and integrated technology. Protected Harbor has helped support law firm security 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 a law firm. Protected Harbor concentrates on six elements throughout the stack, uplink, firewall, switches, hosts, VMs configuration, and storage to safeguard our customers' operations.

ABOUT PROTECTED HARBOR

Protected Harbor is a trusted IT partner responsible for the technology and applications that keep your business moving forward. We provide a wide range of cloud infrastructure, security, storage, networking, and monitoring managed services to companies looking to grow.

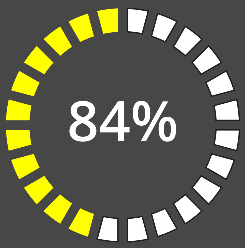
Regardless of the type of client, our focus is on ensuring that your applications and technology stay up at the lowest possible cost, regardless of location and cloud provider.

We can offer your firm Cybersecurity, Infrastructure Design, Network Configuration, Monitoring, Customized Protected Cloud, Change Management, and Data Protection & Recovery.

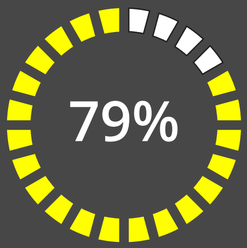
We listen, learn, think, and do not blindly deploy, unlike everyone else. Our team designs a custom solution for every client understanding there is no such thing as a one-size-fits-all when it comes to technology. We focus on durability and what is required to achieve unheard-of uptime. Once developed, we create a seamless migration process and enable our proprietary outage avoidance methodology to maintain uptime. We'll protect your technology while you grow your business.

Protected Harbor is the last IT company you are ever going to need to hire.

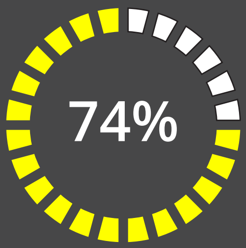
HOW WERE LAW FIRMS PROTECTING THEMSELVES IN 2022 ?



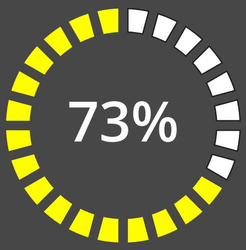
Spam Filter



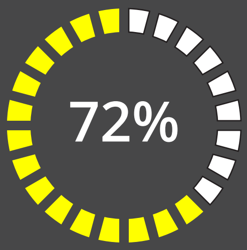
Software Firewalls



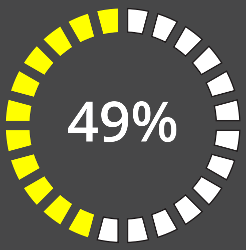
Mandatory Passwords



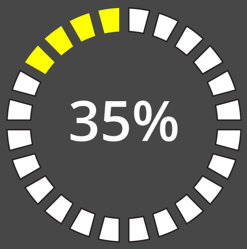
Anti-Spyware



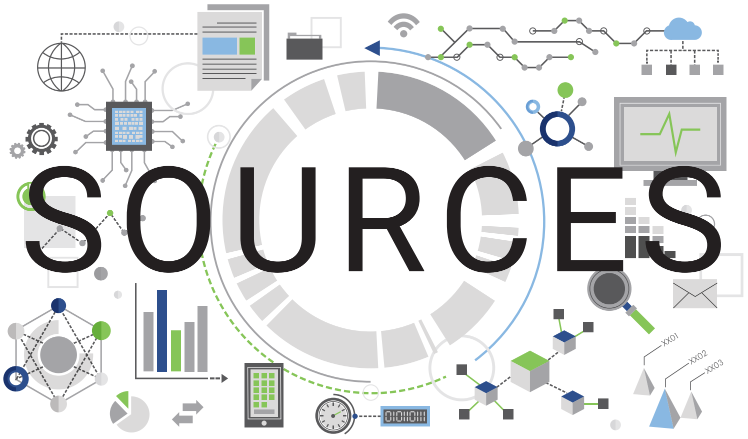
Email Virus Scanning



File Encryption



Security Assessments



SOURCES

Simek, W. John. Tech Report 2022. 2022 Cybersecurity. (2022, November 29). Retrieved February 3rd, 2023. https://www.americanbar.org/groups/law_practice/publications/techreport/2022/cybersecurity/

Tompkins, Amanda. turning Your IT Services From A Cost Center To A Cost Saver. (2023, January 18). Retrieved February 6th, 2023. https://rcbizjournal.com/2023/01/18/turning-your-it-services-from-a-cost-center-to-a-cost-saver/

The Mobile Malware Landscape in 2022 – Of Spyware, Zero-Click attacks, Smishing and Store Security. Retrieved February 3rd, 2023. https://blog.checkpoint.com/2022/09/15/the-mobile-malware-landscape-in-2022-of-spyware-zero-click-attacks-smishing-and-store-security/

A Sophos Whitepaper. The State of Ransomware 2022. (2022, April). Retrieved February 3rd, 2023. https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

Nelson, D Sharon. Simek, W. John. Maschke, C. Michael. Two Law Firm Data Breaches And New Breach Stats. 2022, May 3. Retrieved, February 6th, 2023. https://abovethelaw.com/2022/05/two-law-firm-data-breaches-and-new-breach-stats/

Kerner, Michael Sean. Ransomware Trends, Statistics, and Facts in 2023. 2023, January. Retrieved, February 3rd, 2023. https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

PROTECTED
HARBOR

Because IT Matters

THANK YOU

Looking For Some More Help? Protected Harbor is Offering A Free IT Audit To Any Legal Service Organization That Downloaded This Report.

Get A Free Legal IT Audit Now

Call Us- (201) 957-1616

VISIT US- 60 Dutch Hill Rd; Suite 16 Orangeburg, NY 10962

EMAIL US- support@protectedharbor.com