

2022 LAW FIRM DATA BREACH TREND REPORT

HOW ARE CYBERSECURITY TEAMS, LEGAL ORGANIZATIONS AND LAW ENFORCEMENT AGENCIES PREPARING FOR THE BIGGEST CYBER RISK TO HIT OUR LEGAL SYSTEM IN 2022?

Table of Contents

02

Introduction

13

Responses

05

Compliance
Obligations

15

Recent
Breaches

06

Risk of Attacks

16

Cybersecurity
Trends

09

9M'25 Financial
Statement

25

About Us

INTRODUCTION

The legal industry is likely to undergo significant changes due to technological advancements and ever-changing client demands.

Digital platforms, softwares, and apps will offer faster, more effective strategies while virtual programs will replace secure processes and labor-intensive tasks. Also, clients now are busier than ever and expect excellent digital experiences wherever they go. This includes mobile-first solutions, digital communication, control over their legal cases, speed, and efficiency. It is clear that in order for law firms to satisfy their audience they need to keep pace in the fast-changing world of technology, which means protecting their data.

AMERICAN BAR ASSOCIATION TECHREPORT: CYBERSECURITY OF RESPONDENT LAW FIRMS

26%

EXPERIENCED A SECURITY BREACH

36%

SYSTEMS HAVE BEEN INFECTED WITH VIRUSES,
SPYWARE, & MALWARE

33%

OF ATTORNEYS REPORTED THAT THEY HAVE CYBER LIABILITY

Data has become one of the most important aspects of a business in the digital age. Law firms face considerable risks from data leaking, including, significant reputational harm and financial losses. Data loss detection and prevention has become one of the most severe security challenges for businesses; as the volume of data grows exponentially the data breaches occur more frequently than ever before.

Financially motivated actors and ideologically motivated hacktivists increasingly target law firms. "They retain sensitive customer information, handle considerable funds, and are a crucial enabler in commercial and business transactions," according to the NCSC. Phishing, data breaches, ransomware, and supply chain compromises are among the most severe risks facing law firms, according to the NCSC. For example, a UK software firm exposed personal information belonging to more than 190 law firms in 2020

SIDE BAR: REMOTE WORK IN 2022

As remote and hybrid work continues to trend, there is no doubt law firms are growing acutely aware of their technological capabilities and deficiencies. Compared to other industries, law firms have historically struggled to keep up with the proliferation of technology and data due to security concerns, lack of technical resources, and a limited budget for necessary enhancements or proper software.

Here are the common challenges we encounter:

- Keeping client data on-premises versus the cloud provides a false sense of information security.
- Resisting budgeting for technology investments over time creates higher costs in the long run.
- Running outdated or legacy solutions increases your firm's exposure to data breaches and cyberattacks.

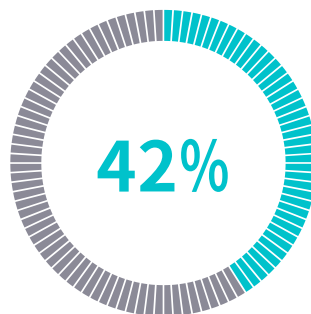
OBLIGATIONS AND RESPONSIBILITIES FOR LAW FIRMS

The American Bar Association (ABA) has held lawyers to the ethical and model rules of professional conduct since they were approved in 1983. These rules are the internal compass for lawyers to navigate various scenarios and interactions with clients.

Rule 1.6, regarding the confidentiality of client information, states that, “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”

This means lawyers must make efforts to protect their clients’ data.

In 2018, the ABA issued Formal Opinion 483, which discusses the importance of data protection and how to handle the inevitable security breach. The opinion states matter-of-factly that the risk of law firms experiencing a data breach is not a matter of if, but when.



OF LAW FIRMS WITH UP TO 100 EMPLOYEES HAVE EXPERIENCED A DATA BREACH.

RISK OF ATTACK

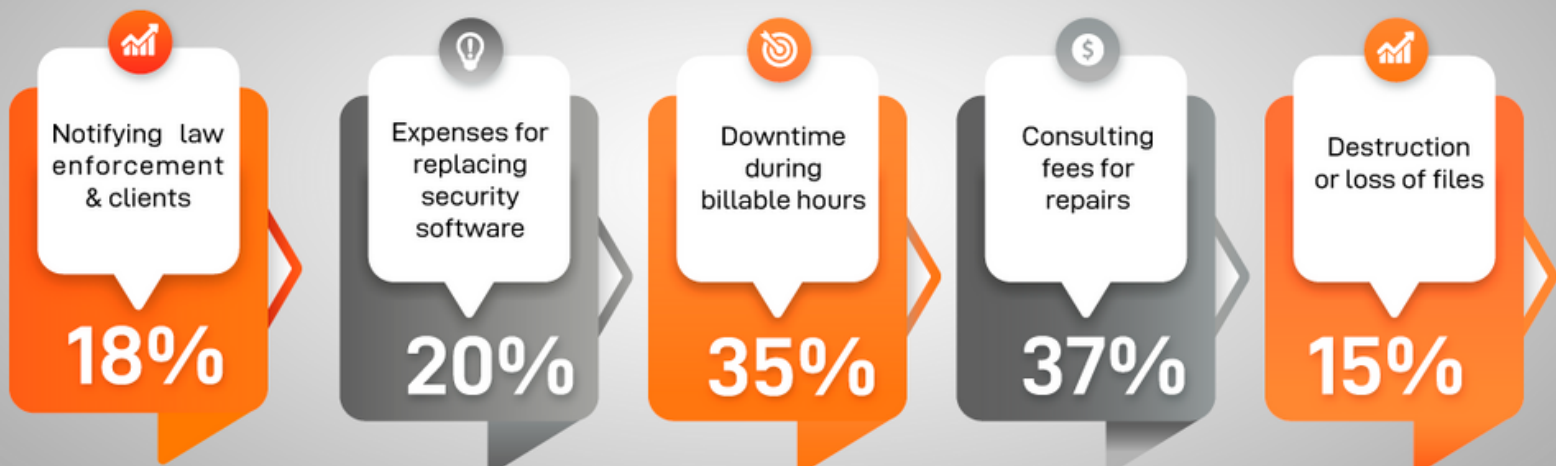
The threat landscape for law firms and businesses has increased as a result of our daily lives and work being conducted online.

Just consider one of your firm's top attorneys and how they allocate their time during work and life. Perhaps they start the day by checking email, updating their Facebook status, making a client call, and sending a follow-up email with the sensitive information attached. Not one, but every one of these actions exposes information that hackers can use to infiltrate your law firm.

They may have fallen victim to email spoofing, which forges the sender and can include malicious attachments or links. Hackers could use their Facebook status to tailor a hack based on location or personal information to identify potential passwords.

Cyber-attacks against law firms are not a new phenomenon, but the rate of incidence and year-over-year growth are staggering. In fact, according to the ABA, up to 42% of law firms with up to 100 employees have experienced a data breach.

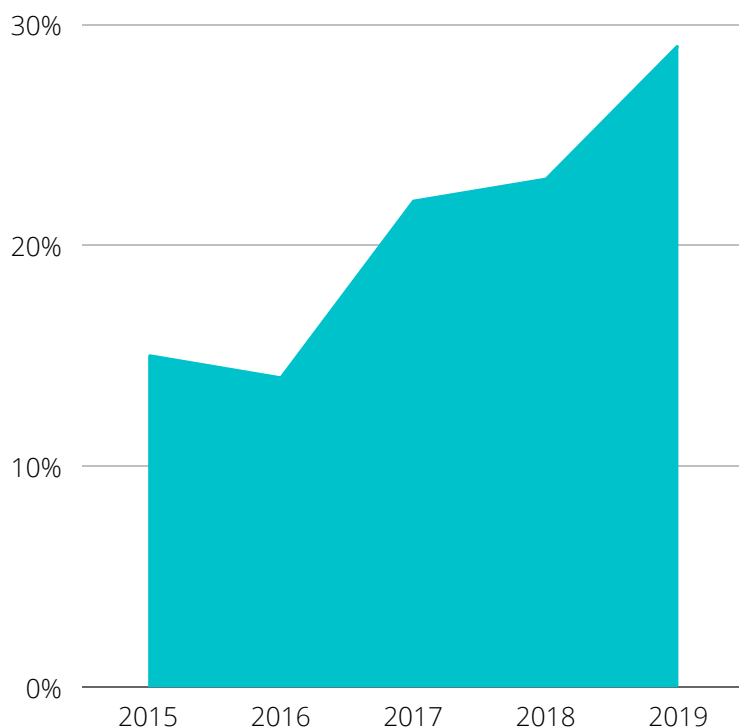
MOST COMMON CONSEQUENCES OF BREACHES



According to the American Bar Association's 2013-2019 Legal Technology reports

THE NATURE OF CYBERSECURITY RISK IN LEGAL SERVICES

GROWING NUMBER OF CYBERSECURITY BREACHES

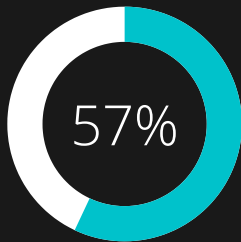


In her article titled, *The Risk of Data Breaches in the Law Firm*, Hanna from Texas Lawyers Insurance Exchange (TLIE) stated three primary categories of known data breaches involving lawyers and law firms. The two most important being the disposal of client documents, theft of mobile devices, and exploitation of internal security protocols. Of course, these are not all issues that could lead to data breaches or affect computer operations. Bloomberg reported that Chinese hackers once targeted specific Toronto law firms searching for information about a \$40 billion takeover deal. A Texas lawyer had crucial client information taken from his car in a case known to TLIE and supplied credit monitoring services to those customers.

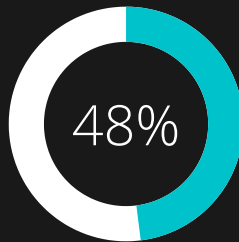
Some cyber dangers, such as the spread of viruses and Trojans, might result in liability by exposing data held by others. However, the three areas that have caused massive issues for lawyers thus far are listed below.

The most common data leak in legal firms is improper document disposal. There were three publicly recorded occurrences in Texas that highlight this issue. The first occurrence happened when attorneys allegedly dumped client data in San Antonio and Houston dumpsters, where they were recovered intact. Second, computers from a law firm were found in a pawn shop in another Texas case. Finally, a flash drive with personally identifiable information (PII) of about 627 clients was attached to **one** computer. This breach happened despite the legal firm's policy of thoroughly cleaning all donated computers of any client data.

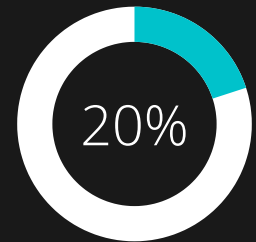
MALWARE INFECTIONS BASED ON FIRM SIZE



Firms with 10-49 attorneys



Firms with 2-9 attorneys



Firms with 500+ attorneys

The breaching of internal security systems is the next area described by Meade. These data breaches occur when security systems are mistakenly or purposely bypassed, despite the availability of excellent processes. Experian, for example, revealed to New Hampshire authorities that credentials supplied to a legal firm were misused to download a large number of credit reports containing sensitive information.



TOP THREATS

FROM BASIC BREACHES, LIKE THOSE RESULTING FROM A STOLEN LAPTOP, TO MORE ELABORATE HACKING SCHEMES, YOUR CLIENT DATA IS CONSTANTLY IN JEOPARDY. HERE ARE A FEW THINGS YOU'RE PROBABLY DOING RIGHT NOW THAT ARE PUTTING YOUR CLIENTS AT RISK.

SKIPPING ASSESMENTS

You can't protect something if you don't know it exists. To help prevent a data breach, an annual inventory should be taken to understand what devices and data you have, where they are located, and who has access to them. It's also essential to conduct a security and risk assessment. How vulnerable is your information? What would the ramifications be if it was stolen? According to the ABA, "Comment [18] to Model Rule 1.6 includes a risk-based approach to determine reasonable measures that attorneys should employ. The first two factors in the analysis are 'the sensitivity of the information and 'the likelihood of disclosure if additional safeguards are not employed.' This analysis should include a review of security incidents that an attorney or law firm has experienced and those experienced by others—generally and in the legal profession".

UNDERSTAFFED & UNDERFUNDED IT DEPARTMENTS

The growing burden on IT staff is a significant challenge that cybersecurity professionals in healthcare organizations have already identified. A majority of IT departments are still understaffed and overburdened with day-to-day work. This leaves little time for them to improve their security infrastructure, as they always react rather than improve. It doesn't help that a majority of their time is spent on manual tasks like creating tickets, which could easily be automated.

LACK OF EMPLOYEE SECURITY TRAINING

Employees usually know how to spot suspicious emails, lock-up devices with sensitive information, and so on.

Unfortunately, many legal service organizations have failed to adequately train employees on the basics of IT security. Analysts claim that non-malicious attacks are the most common security breaches that healthcare organizations face. A study by the Ponemon Institute showed that 47% of non-malicious attacks were caused by employee negligence, while 29% were due to system glitches, and 24% were because of third-party errors.

CLOUD MIGRATION & APPS

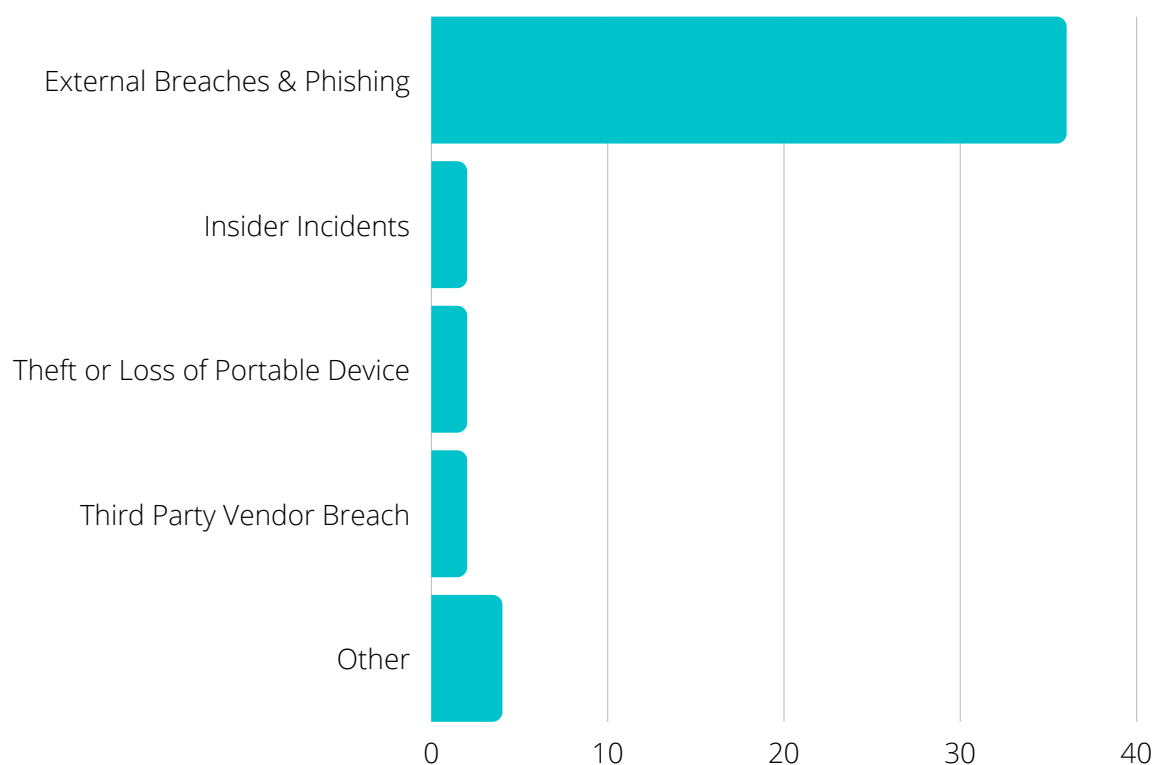
"Moving workloads to the cloud," is commonly heard among technology companies. However, when organizations plan to do so, they encounter a problem: security controls and practices in their on-premises environments are not what they need for the cloud. In this environment, everything is software-based and deeply integrated.

Your business needs to make sure it has a good strategy when it comes time to migrate, including; fundamentals like access control and governance, API integrations, and continuous monitoring.

Cloud providers are responsible for the physical security of their data center environments and disaster recovery plus making sure they comply with all regulations and best practices. Law firms still need to be responsible for disaster recovery and continuity processes. This is especially important if you move to an IaaS environment where you rely on shared resources only - without your hardware.

EXTERNAL BREACHES

HOW LAW FIRMS WERE BREACHED IN 2020

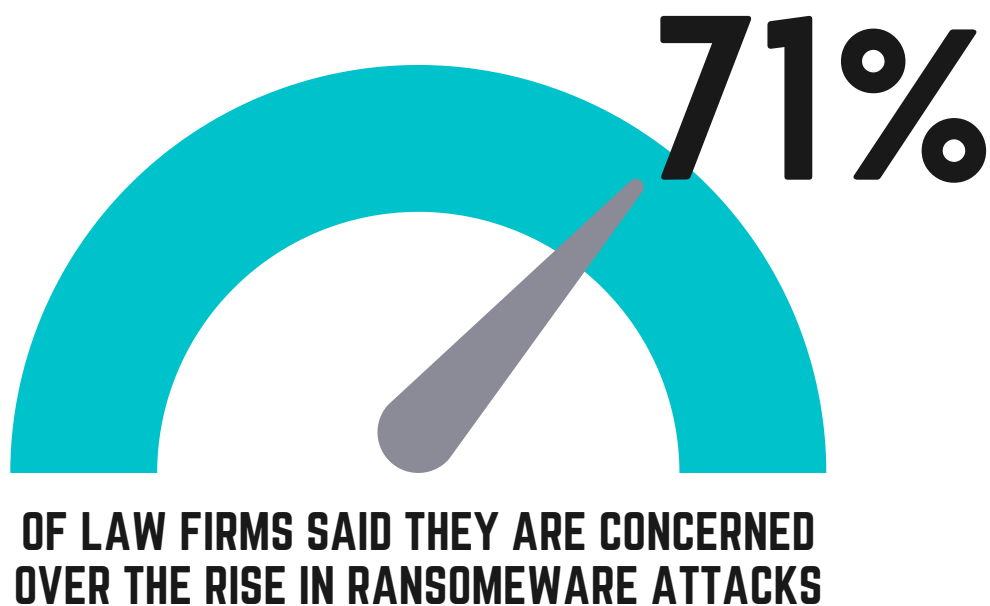


Of the firms that have notified state authorities, external breaches—including phishing, hacking, and malware attacks, were the most commonly identified source of data exposure events, according to Law360 Pulse's analysis. Several other firms reported data breaches through other factors, such as a third-party data breach, stolen or lost devices, or insider wrongdoing.

According to Lindsay Nickle, a Lewis Brisbois Bisgaard & Smith LLP partner and a vice-chair of the firm's data privacy and cybersecurity practice, the reason why we are seeing a significant number of firms filing notifications of external breaches is, "Mainly because these are the categories that end up in the compromise of information."

"External hacking or malware will cover any sort of unauthorized access to an environment or an email account, as well as covering ransomware attacks or other types of viruses or trojans that get into a system," Nickle said. "Those are the two biggest threats we have right now, ransomware and compromises of email accounts."

According to the records submitted to state authorities, many law firm investigations have identified that *unauthorized individuals* have accessed their email accounts, exposing individuals' personal information, such as names and Social Security numbers. In several cases, the breached information has also included government-issued ID numbers, financial information, medical records, and even employees' W-2 forms. However, the cybercriminals don't necessarily make money from the breached data. They mostly make money from either extorting payments or diverting funds and fraudulent transactions in compromised accounts. "The data, the breached information, is collateral damage," said Lindsay Nickle, a Lewis Brisbois Bisgaard & Smith LLP partner. "It's not what the bad guys are after, and it's not how they make their money," Claudia Rast, Butzel Long PC's cybersecurity group leader, added that doesn't mean that the breached information isn't for sale on the dark web. It's not like dollars; it's pennies, but if you have thousands of Social Security numbers or thousands of credit card numbers. It has some value," she said.





HOW LAW FIRMS ARE RESPONDING

53%

HAVE A POLICY
ON MANAGING
COMPANY DATA

56%

HAVE A POLICY
ON REMOTE
ACCESS

44%

HAVE A POLICY
ON EMPLOYEE
HANDLING OF
CLIENT
INFORMATION

A survey conducted by the Bar Association in 2021 asked respondents about various security responses adopted by law firms to tackle the increasing threats in the legal sector. Over 50% of respondents said they had official policy's on email, internet use, computer use, and remote access. In turn, 48% had social media policies, and only 32% had a policy on personal technology use/BYOD.

As firms anticipated growth, they planned to roll out more cyber and data protection policies.

CYBER INSURANCE

As data breaches continue to dominate the headlines, the necessity for cyber insurance is becoming increasingly apparent. Many general liabilities and malpractice plans do not cover data breaches or security issues. The percentage of attorneys who say they have cyber liability insurance has risen in recent years to 42% this year. There is coverage available for first-party losses to the law firm and cyber liability insurance, which covers liability to third parties like lost productivity, data restoration, and technical and legal expenses. For law firms of all sizes, an evaluation of the requirement for cyber insurance coverage should be part of the risk assessment process.

SECURITY STANDARDS AND FRAMEWORK

In a recent TechRepublic story Jennifer DeTrani, general counsel at Wickr, a secure communications company stated that, "lawyers, are becoming increasingly aware of their professional responsibility to encrypt and secure client communications." They are increasing their security protocol and incorporating various tools to safeguard themselves from data theft.

IMPLEMENTING NEW TECHNOLOGY

Manhattan Tech Support mentioned that most law firms now recognize that better technology is essential to this new, client-centered approach to legal services. According to the International Legal Technology Association's Legal Technology Future Horizons report, "The capacity for rapid, I.T.-enabled innovation will be a critical differentiator for law firms in the future. 73 percent of respondents — representing more than 440 firms worldwide — agree that, "the capacity for rapid, I.T.- enabled innovation will be a critical differentiator for law firms in the future."

RECENT BREACHES

New York City's Law Department:

The hackers infiltrated the law department by using a stolen ID from an employee. They had access to thousands of police records. The department disabled its network to prevent further access, resulting in many delays in court hearings.

Grubman Shire Meiselas & Sacks:

A hack on the business Grubman Shire Meiselas & Sacks in 2020 resulted in 756GB of stolen PII. Pro-athletes and Hollywood A-listers like Lady Gaga, whose legal documents were released in the attack, are among the firm's clientele. REvil ransomware was used in this attack on the law company. These attacks frequently employ phishing emails or stolen credentials to gain remote access to a network as the initial vector. When the corporation refused to cooperate, the hackers demanded a \$21 million ransom.

Vierra Magen Marcus: In 2020, the IP legal company Vierra Magen Marcus, whose clientele includes Fortune 500 corporations, had a data breach. Hackers were able to obtain 1.2 gigabytes of stolen data, including NDAs and patents, using the REvil ransomware, which they auctioned on the dark web.

Mossack Fonseca: Hackers allegedly exploited a weakness in a WordPress site and gained access to Mossack Fonseca's email system, dubbed, "the greatest data dump ever." The organization, which oversees offshore transactions for major clients such as heads of state and celebrities, had 11.5 million files stolen by the attackers. In addition, the press was given access to emails, documents, and photos, leading to a coordinated campaign by the media to expose the firm's clients for tax fraud and other crimes. Mossack Fonseca went out of business within two years of the attack due to the damage to the firm and clients' reputations.



TOP CYBERSECURITY TRENDS FOR 2022

The ABA's TechReport has reported some disturbing statistics this past year.

26% OF US FIRMS

HAVE SUFFERED A SECURITY BREACH IN THE PAST YEAR.

19% OF U.S. FIRMS

ARE UNSURE IF THEIR COMPANY HAS BEEN AFFECTED IN THE PAST

35% (DOWN FROM 28%)

HAVE ENACTED THE ABA'S CYBERSECURITY PRECAUTION RECOMMENDATIONS

28% (DOWN FROM 28%)

HAVE REVIEWED VENDOR PRIVACY POLICIES

THE PROTECTED METHODOLOGY

The cyber threats and security vulnerabilities to healthcare facility data can jeopardize patient-protected health information (PHI), distract healthcare professionals, and potentially harm its reputation within your community.

Protected Harbor presents a 10-step checklist that Healthcare IT professionals can implement to overcome the cyber security challenges.

PASSWORD AUTHENTICATOR

Password authentication is a method in which a user enters a unique ID and key compared to previously stored credentials. It is one of the quickest forms of security; you can set up your device to require some identification before letting someone access your phone. It can be in a passcode, PIN, password, fingerprint, or 2-factor authentication (2FA) can be adopted as well.

2FA is an additional layer of protection which verifies that anyone attempting to access an online account are whom they claim to be. The user must first provide their username and password. They will then be requested to submit another piece of information before receiving access.

USE EFFECTIVE EDR

The Endpoint Detection and Response (EDR) tools is the technology that alerts the security teams regarding any malicious activity or security threat. They enable fast investigation and containment of attacks at endpoints like an employee's workstation, a cloud system, a server, mobile or IoT device.

Using effective EDR tools can help you improve the security of your network by aggregating data on endpoints, including process execution, endpoint communication, and user logins. It is vital to use practical EDR tools to detect and respond to any suspicious activities as soon as they are performed.

Some of the best EDR tools for law firms include FireEye, Symantec, RSA, Cybereason, and CrowdStrike.

MOVE TO A VIRTUAL SERVER

A server that shares the hardware and software resources with other operating systems is called a virtual server. You can re-create the functionality of a physical server through a virtual server. Multiple virtual servers can be set on a single physical server. They help to better resource allocation and utilization plus allow for hardware independence, mobility/failover, and advanced disaster recovery. By moving to a virtual server, legal services can control who accesses their data, information, networks, systems, while improving resiliency and uptime.

Moving to a virtual server is essential as it has so many benefits that address the security concerns that law firms face. These benefits include getting the ability to prioritize the critical traffic and improving the network agility while reducing the burden from the IT department.

A legal organization can move to a virtual server using an industry-standard hypervisor (virtualization software), such as VMWare, Microsoft Hyper-V, Solarwinds Virtualization Manager, or Oracle VM Virtual Box.

ISOLATE BACKUPS

A remote or isolated backup is stored separately from other backups and is inaccessible from the end-user layer. Creating a remote backup helps to reduce security breaches, especially ransomware attacks. Ransomware is an attack that quickly encrypts all files on a hard drive and starts attacking other devices connected to a network. Creating local backups is not enough to prevent the system and network from this attack, so isolated backups are the best choice. An organization can quickly recover all of its data if it has a remote backup.



KNOW YOUR NETWORK MAP

Understanding the network map is critical to complying with data privacy regulations as it provides an overview of devices and data on your network. This overview is crucial in identifying and minimizing the attack surface of a system. It will also uncover devices that IT staff may not know are there. For instance, an old, decommissioned server.

To monitor your network map, you can use tools that help you understand the interconnectivity of devices and data flow through the network. Understanding the data flow can help pinpoint what information is vulnerable to attack and how.

TOOLS TO ANALYSE YOUR NETWORK

- SOLARWINDS NTM
- EDRAW MAX
- PAESSLER PRTG NETWORK MONITOR
- NAGIOS
- MANAGEENGINE OP MANAGER
- LUCID CHART

UPDATE ALL SOFTWARE

It sounds simple, but vulnerabilities caused by outdated software are a significant problem. Keeping all the software up to date is essential for better performance.

It also helps discourage potential cybercriminals who like to take advantage of previously-found weaknesses in software.

Whenever a new version of the software is released, the software developers inform all users regarding the updates. The IT admins should update all the software and operating systems throughout the organization from time to time to keep their IT system and network security strong.

DATA ENCRYPTION MATTERS

Large law firms handle both bulks of and varieties of data. The heterogeneous pool of data makes them vulnerable to cyber-attacks. In 2022, law firms must use encryption methods for systems, data in the cloud, data at rest, and data in transit to protect their files. Hard drives, USB devices, and phones should use encryption if holding sensitive data.

DATA ENCRYPTION TIPS:

- Look at data in all cases, both in transit and at rest. Encryption is used to protect data in all scenarios.
- Back up all files and create an image backup before encryption. Create a boot disk or removable media and ensure that you have installed media for the operating system.
- Your organization can benefit from distributed encryption, including more robust performance, better availability, low network bandwidth, and high-quality data transmission.
- Use the hub-spoke model to encrypt data. While combining the distributed execution with the central key management, the encryption and decryption mode will be anywhere within your network. The critical management can integrate with encryption software and deploy on more than a single node. You can encrypt and decrypt at the node level with all the spokes in place. By structuring this way, data does not need to travel much.



TRY NEW SECURITY MODELS

DATA MASKING

Data Masking is a method to develop a fake yet realistic version of your company data by altering the data values while using the same format. The aim is to create a version that can not be reverse-engineered or deciphered. There are various ways to change data, including encryption, word or character substitution, and character shuffling.

TOKENIZATION

Tokenization replaces sensitive data with non-sensitive, randomly generated substitute characters as placeholder data. These characters, known as tokens, have no intrinsic value. They allow authorized users to get sensitive data when needed. It isn't exactly easy to maintain performance and scale as securely as databases increase in size.

ZERO-TRUST

The fundamental principle of the Zero-Trust model is to give the least-privileged access assuming that no application or user should be inherently trusted. Trust is established based on the user identity and context, such as the security posture of the endpoint device, the user's location, and the app or services being requested.

PROTECT THE CLOUD

Cloud computing has become an integral aspect of digitalization, but, it also increases security vulnerabilities. Security concerns have spurred intense disputes in information security circles and CIOs as data migrates to the cloud. Legal services organizations do not have control over cloud security, but Cloud Service Providers do. This makes Legal IT departments concerned; therefore, they use cloud security technologies to encrypt data before uploading it to the cloud, rank data by risk level, protect and monitor end-points, and give enterprises more control over cloud data security.

THE BEST CLOUD SECURITY TOOLS:

- **CloudStrike Falcon:** It's a next-gen cloud-based endpoint protection solution that takes care of any connected device, ranging from light with a tiny digital footprint to powerful enough to handle attacks like shell injections and zero-day exploits.
- **Cloudflare Web Application Firewall:** It's a powerful online protection service that can keep millions of web applications safe and connected effectively.
- **Barracuda CloudGen Firewall:** A next-gen SaaS security system to protect complex distributed network architectures. This tool identifies and protects against phishing emails and also offers backup.
- **TOPIA:** A cloud security tool that gathers data on assets and analyzes them to detect threats and rank them based on their severity. It applies in-memory protection and Patchless Protection to defend a network. Zero spam protects corporate email servers by fighting against cyber threats like spear-phishing and ransomware. It's an easy-to-use, highly effective tool with performance enhancement capabilities.

STOP USING VPN'S

A VPN (Virtual Private Network) helps you establish a private network while using the public networks. While beneficial to provide access to employees and third parties, this access is open-ended and unsecure. All security capabilities are lost when granting third parties remote access via VPN. VPNs lack access controls and session monitoring, both effective means of security for network access. VPNs don't manage, vault, or verify credentials, so password protection is dependent on your third parties keeping them safe.

Additionally, VPN will allow any virus on the PC to come right into the network. At Protected Harbor, we install Remote Desktop Protocols for all legal services clients. With RDP, if an employee connects to the network from an infected device, it will not infect the network.

Remote desktop solutions are becoming more and more familiar with the increased prevalence of distributed workforces and more employees regularly working from home. It's perfect for people who are frequently on the go, work out of a home office, or are often out in the field and need access to their local desktop computer. RDP is encrypted by default with a higher level of encryption than VPN and requires no additional connection time.

IF YOU MUST USE A VPN, THEN ENCRYPTION, ENCRYPTION, ENCRYPTION!

Due to sensitive client data and privileged information, law offices handle, if you **MUST** use a VPN for sending and receiving critical data over your network, you can stop attackers from getting any information with the right tools.

You can use and improve your VPN Encryption by:


- Using IPsec Protocols
- Using the most robust encryption and hashing algorithms and key groups (AES256, SHA256, DH14)
- Stopping DNS Leaks
- Using a Kill Switch
- Using a Network Lock
- Stopping IPV6 Leaks
- Limiting VPN Access



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 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, 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.

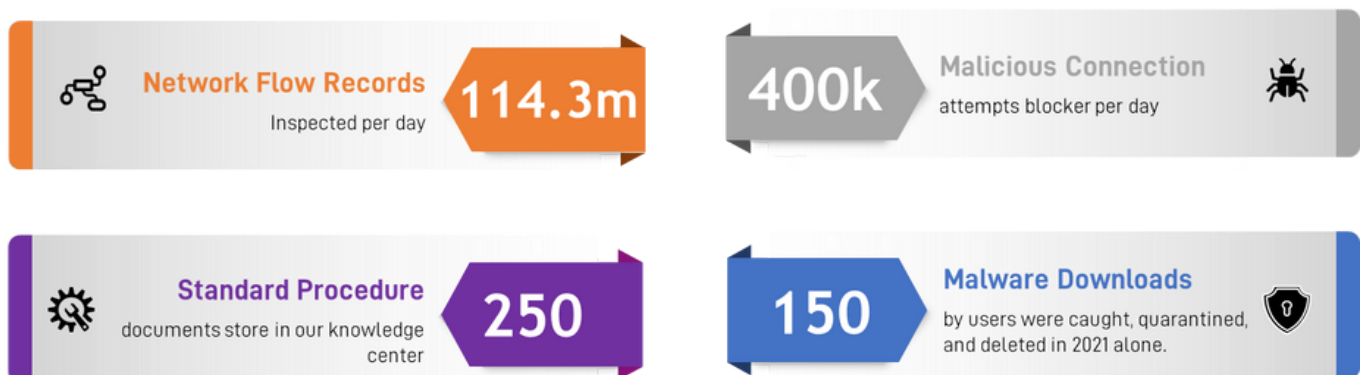
ABOUT PROTECTED HARBOR

WHEN YOU NEED RIDICULOUSLY RELIABLE, DURABLE & SECURE TECHNOLOGY SOLUTIONS

Protected Harbor is a trusted IT partner responsible for the technology and applications that keep your business moving forward. We provide a range of cloud infrastructure, security, storage, networking, and monitoring managed services to companies looking to grow. Regardless of client type, our focus is on ensuring that your applications and technology stay up at the lowest possible cost, regardless of location and cloud provider.

Like everyone else, we offer 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. We design a custom solution for every client, focusing 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 – you grow your business.



SOURCES

**THANK YOU TO ALL THE GREAT
RESEARCH THAT CONTRIBUTED
TO THIS REPORT**

- 2022 law firm Data Security Guide: Secure Your Practice. Clio. (2021, December 23). Retrieved April 29, 2022, from <https://www.clio.com/blog/data-security-law-firms/>
- 4 data breaches at law firms and what you can learn from them. Dashlane Blog. (2022, April 21). Retrieved April 29, 2022, from <https://blog.dashlane.com/data-breaches-in-law-firms/>
- Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: Causes, challenges, prevention, and Future Directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5). <https://doi.org/10.1002/widm.1211>
- 'The cyber threat to UK Legal Sector' 2018 report. NCSC. (n.d.). Retrieved April 29, 2022, from <https://www.ncsc.gov.uk/report/-the-cyber-threat-to-uk-legal-sector--2018-report>
- Cybersecurity biggest threats legal sector. The Law Society. (n.d.). Retrieved April 29, 2022, from <https://www.lawsociety.org.uk/topics/the-city/cybersecurity-biggest-threats-legal-sector>
- Cybersecurity standards and risk assessments for law offices. Crowell. (n.d.). Retrieved April 29, 2022, from <https://www.crowell.com/files/Cybersecurity-Standards-and-Risk-Assessments-for-Law-Offices.pdf>
- Hope, A. (2020, May 20). Over 190 law firms affected by advanced data leak that exposed over 10,000 legal documents. CPO Magazine. Retrieved April 29, 2022, from <https://www.cpomagazine.com/cyber-security/over-190-law-firms-affected-by-advanced-data-leak-that-exposed-over-10000-legal-documents/>
- Lauria, J. (2019, July 1). Four ways law firms can safeguard sensitive client data. Law Technology Today. Retrieved April 29, 2022, from <https://www.lawtechnologytoday.org/2019/07/four-ways-law-firms-can-safeguard-sensitive-client-data/>
- Meade, M. H. (n.d.). Eckert Seamans. Retrieved April 29, 2022, from <https://www.eckertseamans.com/our-people/>
- PR Newswire. (2020, May 27). Over 15% of a global sample of law firms show signs of compromise. Over 15% of a Global Sample of Law Firms Show Signs of Compromise. Retrieved April 29, 2022, from <https://www.prnewswire.com/news-releases/over-15-of-a-global-sample-of-law-firms-show-signs-of-compromise-according-to-bluevoyant-sector-17-report-301065918.html>
- Strategic imperatives for the law firm of the future. (n.d.). Retrieved April 29, 2022, from <https://fastfuture.com/wp-content/uploads/The-Future-of-Law-Firms-ILTA-Legal-Technology-Future-Horizons-Final-Report.pdf>
- Top Technology Cybersecurity Best Practices for law firms. Albatross Cloud Home. (n.d.). Retrieved April 29, 2022, from <https://albatross.cloud/top-technology-cybersecurity-best-practices-for-law-firms>



PROTECTED HARBOR

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 Audit Now](#)

www.protectedharbor.com