Cyber Risks and Exposures in Professional Services Firms

Help your professional services clients identify and understand their exposure to cyberattacks
HOW VULNERABLE ARE BUSINESS PROFESSIONALS TO A CYBERATTACK?

Professional service firms, which store sensitive data and have commitments to client confidentiality, are especially at risk from cyber-related exposures. From lawsuits to tax information, intellectual property to strategic plans, today’s cyber criminals who target professional service firms know exactly what they are looking for.

“The exposure of confidential information can completely derail a professional firm’s obligation to safeguard its clients’ information,” says Michele Epstein, VP Professional & Management Liability, Worldwide Facilities, LLC. “This can cause more than just a temporary disruption of services, including considerable harm to the business’s reputation as well as more substantial, long-term losses associated with recovery and remediation efforts.”

The fact is, the success of a professional service firm requires establishing trust and maintaining solid relationships with clients. When a cyberattack occurs, it doesn’t take long for client confidence, along with the firm’s good reputation, to disappear. But loss of business continuity and reputation may be the least of the company’s worries. If sensitive client data is leveraged for nefarious purposes, clients that were harmed could launch costly liability lawsuits, alleging that the business didn’t properly protect client confidential data and allowed itself to become vulnerable.

Today’s professional firms have a legal responsibility to protect all information that they collect and store for the purposes of doing business. In some cases, businesses may be governed by the Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), Biometric Information Privacy Act (BIPA) and several others, making it the firm’s responsibility to comply. And while certain risk management strategies can help eliminate many common types of cyber risks, emerging technologies, changes in regulations and the increased sophistication of hackers are creating even more new exposures.

In 2019, the number of cybercrime complaints from both individuals and business organizations reached a staggering 467,361 with a total cost of over $3.5 billion.

- 2019 Internet Crime Report1
PROFESSIONAL INDUSTRIES WITH GROWING CYBERSECURITY RISKS

No organization is immune to hackers looking to access private information. And while breaches at large enterprises tend to make the headlines, the data held by the following professional service firms typically has a much higher value and has become a key focus for hackers.

Law Firms

Hackers recognize that law firms are goldmines for highly sensitive corporate, financial and personal data. However, gaining access to private client data is only part of the havoc caused by cybercriminals. According to the ABA Legal Technology Survey Report, of the law firms that reported breaches in 2018:

» 41% said that cyberattacks had cost their firms downtime and substantial losses in billable hours.
» 11% reported a destruction or loss of files.
» 27% reported having to replace hardware and/or software.
» 40% reported significant costs associated with consulting fees for repairing systems.

In addition, as more lawyers and their legal staff work remotely in order to comply with COVID-19 mandates and reopening requirements, hackers know they will have even more opportunities to infiltrate vulnerable systems. According to Forbes, numerous COVID-19-related scams included fake coronavirus map apps that when downloaded were malware-ridden and gave cybercriminals access to individuals’ smartphone cameras, microphones and even text messages.

Currently, the top five cyberattacks on law firms are:

☞ Phishing Emails. Phishing is the most common cyberattack in the legal industry, affecting law firms of all sizes. At the end of 2018, 80% of law firms reported having experienced at least one phishing attempt.4

☞ Ransomware. According to a recent survey of 1,200 ransomware attacks, 42 occurred within the legal profession. Of those 42, law firms topped the list at 61.36%, followed by courts at 22.73%, legal aid associations at 6.82%, and legal services and prosecutors’ offices at 4.55%. Even when the ransom is paid, hackers can still refuse to decrypt the data, or extort more payments with threats to expose sensitive data or sell it on the dark web.

Cybersecurity and COVID-19

Using intelligent IT systems, updating software, encrypting data and setting up two-factor authentication are just a few of the ways professional firms can protect their data while working remotely during the COVID-19 pandemic.
Whether a firm is large or small does not insulate it from a ransomware attack. According to a recent survey, small firms (1-19 lawyers) accounted for 52.27% of attacks, midsized firms (20-499 lawyers) 27.27% and large firms (500+ lawyers) 20.45%.

Source: Law.com

Data Breaches. In 2019, 26% of law firms reported experiencing some form of a data breach, exposing sensitive client and attorney information and resulting in the loss of or unauthorized access to confidential data. The loss of this data can lead to a number of devastating consequences for a firm, including being sued if a client believes that his or her privacy has been violated in the breach. If criminals penetrate a firm’s security, the consequences can be extensive – ranging from minor embarrassments to serious legal issues.

Malware and Spyware. Consequences of a malware infection include loss of data and loss of data confidentiality. Spyware, another malicious program, is also used to spy on and obtain confidential information by way of the computer system – including webcams. Both attacks are used by hackers to steal sensitive data and to exploit vulnerabilities in the firm’s endpoint security – including mobile devices. Today, hackers are deploying some of the most sophisticated malware attacks ever seen and making law firms their primary targets.

Lawyers are especially vulnerable to cyber data breaches. Unfortunately, for too many firms, cybersecurity is a secondary concern.

Source: American Bar Association

Mortgage Lenders

One of the most critical topics for mortgage lenders has been cybersecurity and the related regulatory pressure. Unfortunately, many firms continue to struggle with where they should invest to best reduce their overall cybersecurity risk and how to avoid additional regulatory scrutiny and fines due to a cybersecurity incident.

Risk exposures that make mortgage lenders particularly vulnerable to a cyberattack include:

- Personally Indefinable Information. The fact that lenders have access to a wide variety of sensitive client personal and business information – including personal information on borrowers, tax returns, financial statements, banking information, credit card numbers and credit applications – makes them a prime target for hackers.

- Third-Party Vendors. Mortgage companies do business with a variety of third-party service providers such as title companies and appraisers. Vendors that have not adopted standardized technology or cybersecurity controls can leave lenders they partner with open to an attack.

- Digital Lending. As the mortgage industry embraces technology to provide more on-demand services to better serve its clients, these digital systems are making lenders incredibly vulnerable to cybercrimes.

- Outdated Processing Software. Lenders that continue to operate on older legacy mortgage processing software applications are putting themselves and their clients at risk, as these systems were not designed with security in mind.

Compared with previous years, more lenders are now offering electronic options to aid in the mortgage process, as borrower demand for online options has increased 18% in the past two years. Of borrowers surveyed:

» 46.5% said they were “somewhat concerned” about entering their personal information online.

» 22.6% said they were “very concerned” about entering their personal information online.
The financial industry was the target of the third-highest number of cyberattacks in 2019, behind government and health care.

Source: Cybersecurity Threatscape 2019¹¹

Financial Services

Thieves of data, rather than theft of money, more than doubled last year compared with 2018, accounting for 66% of the financial services cyberattacks. Among all attacks on financial services firms, the use of malicious software as an attack method jumped from 58% in 2018 to 85% in 2019. Attacks such as convincing the victim to click on an infected web link increased from 49% in 2018 to 80% in 2019.¹²

Today, financial services firms fall victim to cybersecurity attacks 300 times¹³ more frequently than businesses in other industries do. Currently, firms are being hit the hardest by:

Ransomware. By far the biggest cyberthreat to financial companies is ransomware. In fact, in 2019, ransomware accounted for 31% of all system infections, and ransoms that were paid went up to the hundreds of thousands of dollars.

Web Application Attacks. In addition to ransomware, financial firms are rapidly experiencing an uptick in cybersecurity attacks due to web applications that make it easy for employees to share files and collaborate. These services are vulnerable to attack because of their ease of accessibility and reliance on user input, which result in unvalidated redirects or links that trick users into clicking.

Malicious Chat Bots. As much as everyone likes chat bots, the automated programs that are designed to help improve customer service, a bot can be programmed to be malicious and attack a firm both directly and indirectly.

More recently, the COVID-19 pandemic has caused a sharp increase in phishing attacks at financial service firms as criminals exploit consumer fears of the virus, convincing people to click on web links or open attachments that then install malware on computers and allow criminals to steal information or money.

Windows Domain Name System Vulnerabilities: The Next Generation of Cyberattacks

Becoming more prevalent in professional service firms are domain name system cyberattacks. These incidents occur when a hacker finds weaknesses in the DNS for the purpose of gaining widespread access to a company’s systems.

Currently, the Microsoft Windows DNS Server that uses versions from 2003 to 2019 are particularly vulnerable, allowing the spread throughout networks without any human interaction. If exploited successfully, a hacker is granted domain administrator rights that could compromise the company’s entire infrastructure.

For firms at risk, Microsoft recommends a patch be implemented as soon as possible.

CPA and Accounting Firms

According to last year’s Symantec Internet Security Threat Report¹⁴, cybercriminals are in a continuous quest to develop innovative malware to access the bank accounts and financial transactions of accounting clients. As a result, CPA and accounting firms are more susceptible to cybersecurity threats than are businesses from other industries. And while accounting firms face many of the same risks that financial services firms do, the three cybersecurity vulnerabilities related specifically to CPA and accounting firms are:

» Wire Transfer Fraud By Way Of Social Engineering

According to Deloitte¹⁵, there has been a significant risk in wire transfer scams against accounting and treasury functions. Using social engineering tactics, hackers obtain
information about their prospective victims and then trick people within the firm to help facilitate a wire transfer. In addition to social engineering, other potential methods of compromise can include spear phishing, masquerading, email impersonation/spoofing, whaling (phishing directed at CEOs), fake caller IDs, and pretexting.

» Data in Transit. More accounting firms are communicating both internally and externally through multiple channels, transmitting a large percentage of information online, including as attachments via email. As a result, cybercriminals are using malware attacks such as ransomware to steal sensitive financial data of business in transit.

» Remote Data Access. Accounting firms are using cloud-based computing to enable employees to access accounting software and client data remotely over the internet. However, remote data access also makes it easier for hackers to steal sensitive financial data.

» Cryptojacking. Cryptojacking mines cryptocurrencies on behalf of hackers through the unauthorized use of computing devices. In phishing-like attacks, cybercriminals distribute cryptomining malware through a website and browser extensions.

Insurance Services
Collectively, over 100 million Americans have had their personally identifiable information compromised in insurance sector data breaches.16

Over the past two years, the insurance industry has experienced a dramatic increase in the amount of successful cyberattacks. Much like financial services, cybercriminals recognize that insurance companies use and store large amounts of personal information on their policyholders and, as a result, are aggressively targeting that information.

The primary cyber risks to insurance companies today include:

» Infrastructure vulnerabilities
» Identity theft
» Automated threats such as denial of service, credential cracking and vulnerability scanning
» Ransomware
» Outdated computers, servers and software that are not compliant with today’s cybersecurity needs

Only 20% of insurance CEOs believe that their firm is prepared for a cybersecurity event.
Source: KPMG17

Prevent, Detect and Correct: Security Measures to Help Your Clients Manage Cybersecurity Risks
Today, a cybersecurity event isn’t a matter of if - but when. And how a professional firm can mitigate the risk will determine how soon it can bounce back without long-term financial and reputational consequences. In addition to the right cyber liability policy, instituting the proper security measures and tools in the following three areas can help your professional business clients ensure the greatest security. And while some firms elect to perform at least one of the three, the controls offer the best protection when combined.

Preventive Measures. This means identifying and addressing the firm’s most vulnerable areas with the proper prevention systems. These can include intrusion prevention systems, antivirus protection, two-factor authentication, etc.

Detective Measures. These include controls for detecting potential breaches so that corrective controls can quickly respond, e.g., an intrusion detection system, network alerts and the monitoring of database activity and compliance.

Corrective Measures. When a cybersecurity event occurs, the proper corrective controls can help minimize the impact and begin the recovery process. These can include forensics, system isolation, disaster recovery and business continuity plans, and next-step administrative or legal actions.

MITIGATING YOUR PROFESSIONAL SERVICES CLIENTS’ FINANCIAL EXPOSURE WITH CYBER INSURANCE
In many cases, larger professional management firms have the internal technical support and finances to self-insure against a cyberattack. However, small and midsize businesses may find it more cost-effective to buy coverage under a cyber insurance policy to mitigate the risk.
Today, most cyber insurance policies can be purchased as a stand-alone policy or as part of an insurance package. And while terms and coverage will vary among insurers, most offer policy endorsements that can be added to enhance coverage based on the business’s needs and budget.

“In assessing coverage for clients, begin by considering the fact that a professional firm’s central concern is the loss of client data — not just because of the risk to which the clients are exposed, but also because of the loss of client trust and the general reputation of the firm itself,” Epstein says.

Most cyber liability policies offer:

**First-Party Coverage** responds to loss suffered by the insured as a result of a data breach or cyber attack and will generally include:

- Forensics expenses
- Business interruption as a result of a breach of the insured’s network
- Business interruption as a result of a breach of a dependent business network
- Ransom payments
- Data restoration expenses
- Notification to clients and other victims
- Public relations expenses
- Cyber Crime and Social Engineering loss

**Third-Party Coverage** responds to lawsuits and demands by third parties if they allege they have suffered financial loss as a result of a breach of the insured’s network.

- Responds to civil lawsuits
- Responds to government investigations
- Payment of any related governmental fines and penalties
- Payment of Payment Card Industry (PCI) fines and penalties

**CONCLUSION**

No professional firm is too small or too large to fall victim to a cybersecurity crime. By implementing preventive measures now, your professional lines clients can best protect against cyberthreats and liability claims.

**ABOUT WORLDWIDE FACILITIES, LLC**

For 50 years, the ultimate goal of Worldwide Facilities has been to help our retail brokers find innovative insurance solutions that meet the needs of their clients. Contact one of our commercial lines experts to learn about our comprehensive cyber liability insurance policies and recommendations for how you can help your professional lines clients reduce their exposure to a cyberattack.

**JOE ROBUCK**

SVP, Executive Liability  
(213) 236-4519  
jrobuck@wwfi.com

**MICHELE EPSTEIN, MLIS, AAI, AIS, CPIW, DAE**

VP, Professional & Management Liability  
(818) 578-4042  
mepstein@wwfi.com
NOTES

6. Ibid.
12. Ibid.
ABOUT WORLDWIDE FACILITIES

Established in 1970, Worldwide Facilities is a national wholesale insurance broker, managing general agent, and program underwriter. Our team of insurance specialists has access to virtually every specialty domestic and international insurance market.

DISCLAIMER

This whitepaper is Copyright © 2020 by Worldwide Facilities, LLC. It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. This whitepaper is provided “as is” without any express or implied warranty. This whitepaper is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by Worldwide Facilities. The listing of an organization or website does not imply any sort of endorsement and Worldwide Facilities takes no responsibility for the products, tools, and Internet sites listed.

HEADQUARTERS

Worldwide Facilities, LLC

725 S. Figuroa Street, 19th Floor
Los Angeles, CA 90017
(213) 236-4500

Visit wwwfi.com for a full list of offices around the country