Cyber Incidents Take Aim At Law Firms

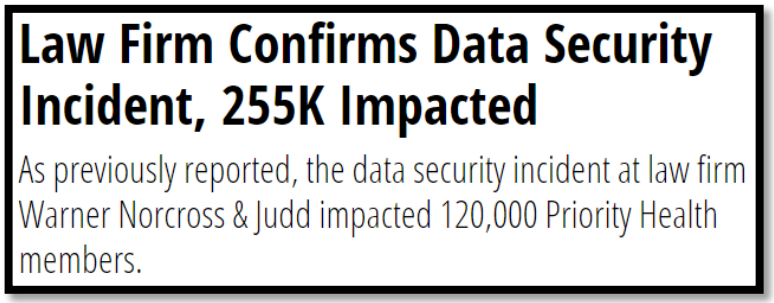
One of the first prominent ransomware attacks on a law firm was **DLA Piper** in 2017. Since then, there have been a number of high-profile attacks on firms, including the MAZE ransomware attack that threatened to leak data if the ransom wasn't paid and the October 2020 attack on Chicago law firm **Seyfarth Shaw**. In 2020, threat actors stole nearly a terabyte of data from the New York law firm **Grubman Shire Meiselas & Sacks**. They initially demanded $21 million and later doubled it to $42 million.


NEWS

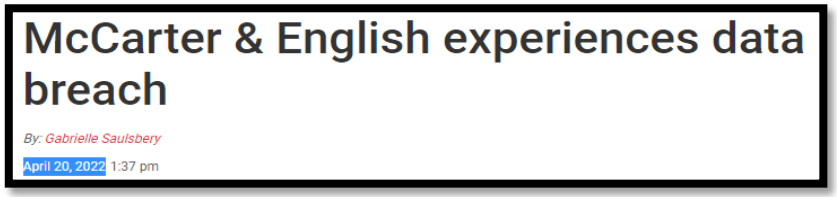
Rawle & Henderson Suffers Cybersecurity Incident

Although the letter did not say when the breach occurred, it said there was reason to believe personal data may have been accessed in July. The letter added that the information included people's names and Social Security numbers.

September 02, 2022 at 10:50 AM


Law Firm Confirms Data Security Incident, 255K Impacted

As previously reported, the data security incident at law firm Warner Norcross & Judd impacted 120,000 Priority Health members.


McCarter & English experiences data breach

By: Gabrielle Saulsbery

April 20, 2022 1:37 pm


Alex Murdaugh sued by his former law firm for allegedly stealing client funds

By Pamela Kirkland, CNN

Updated 10:20 PM EDT, Wed October 6, 2021


High-powered Campbell law firm discloses ransomware attack

By Derek Kortepeter / August 4, 2021


HOME > DIGITAL > NEWS May 13, 2020 4:40pm PT

Hackers Reportedly Demand $21 Million From Entertainment Law Firm in Data Extortion Scheme


Gateley suffers data breach following 'cyber security incident'

JUNE 17, 2021 DISSENT

Ben Edwards reports:

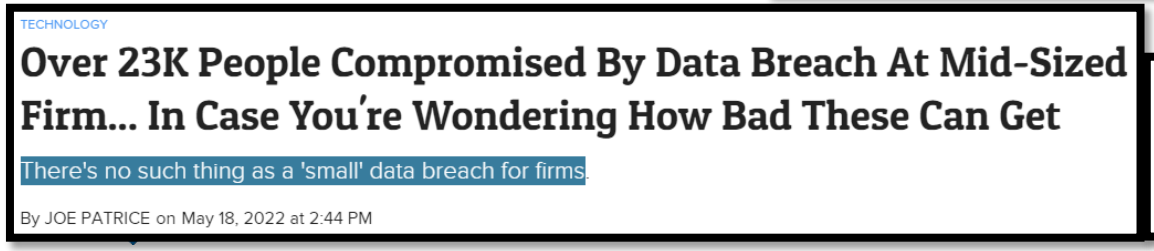

Google employees personal info exposed in law firm data breach

By Lawrence Abrams


MARKETS

Hackers Breach Law Firms, Including Cravath and Weil Gotshal

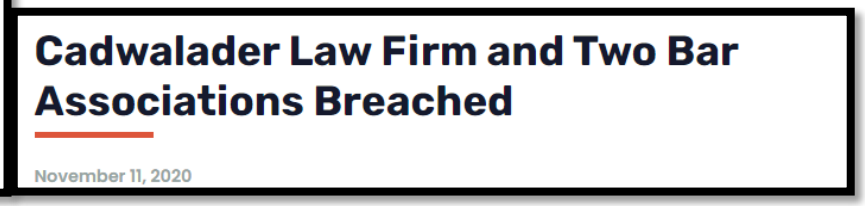
Investigators explore whether cybercriminals wanted information for insider trading


TECHNOLOGY

Over 23K People Compromised By Data Breach At Mid-Sized Firm... In Case You're Wondering How Bad These Can Get

There's no such thing as a 'small' data breach for firms.

By JOE PATRICE on May 18, 2022 at 2:44 PM


Cadwalader Law Firm and Two Bar Associations Breached

November 11, 2020

Executive Risk Advisors| Cyber Insurance
Computer and Technology Section

Are You and Your Clients Protected?

McGriff

Natalia Santiago, JD

Senior Vice President and Claims Manager
Head of Cyber Claims
Houston, Texas | Email: nsantiago@mcgriff.com
Direct: 713.402.1410
Mobile: 281-450-4206

Natalia serves as Senior Vice President and Claims Manager for McGriff's Executive Risk Advisors (ERA) Division.

With over 20 years of legal and insurance experience, in addition to handling complex claims she is also responsible for overseeing all aspects of the claims division.

Prior to joining McGriff, Natalia was the Financial Lines Claims Director for Latin America and the Caribbean for AIG. Prior to AIG, Natalia worked for Chubb as the Financial and Professional Lines Claim Supervisor for Puerto Rico and the Caribbean. Natalia joined Chubb after having served as Claims Counsel for AIG in the Puerto Rico office. Previous to Natalia's career with the insurers she spent a few years as coverage counsel in a private law firm.

Natalia was a university professor for over 10 years. She taught criminal investigation, forensic psychology, employment law, labor relations, interpreting labor contracts, torts, collective bargaining agreements, arbitration and mediation.

Natalia developed (and continues to develop) claims handling, policy interpretation, and coverage trainings in topics such as Cyber 101, EPL Exposures, D&O 101, among others. Natalia has vast experience in coverage litigation, negotiation and claims handling strategies to maximize financial reimbursements. Natalia has managed, and manages, a portfolio of highly technical, highly service oriented, complex claims.

Natalia has assisted, and assists, clients handle challenging cyber claims from the time a ransomware is detected, strategizing over ransomware negotiations and payment/not payment strategies, assisting in the incident response, class action suits, recovery of expenses including documentation of Business Interruption, all the way through claims resolution. In addition, to helping clients update their incident response plan from an insurance stand point.

Natalia specializes in lines of business such as Cyber, D&O, Political Risk, Medical Mal Practice, EPL, Fiduciary Liability, E&O, R&W, Commercial Crime, Special Crime.

Natalia holds a B.A. in Labor Relations and Psychology from University of Puerto Rico and a J.D. from Interamerican University of Puerto Rico.

Cybersecurity threats for law firms is a growing concern. Working with sensitive and confidential information is at the core of most legal services. In today's age information is power. The volume and type of sensitive information law firms are entrusted with makes them an attractive target for threat actors. Additionally, law firms are increasingly turning to working remotely with many law firms already operating on a fully or partially remote basis.

Now not only would a data breach or a security incident lead to loss of reputation for law firms, but it also brings with it monetary losses in cases of negligence and failure to comply with regulations.

According to an American Bar Association survey, the number of law firms that experienced a cybersecurity breach in 2020 marked an uptick from the 12 months prior. In fact, **29%** of survey respondents suffered the fate compared to **26%** in 2019. In ABA's 2021 Legal Technology Survey Report states that **25%** of the survey's respondents reported their law firm had been breached at some time.

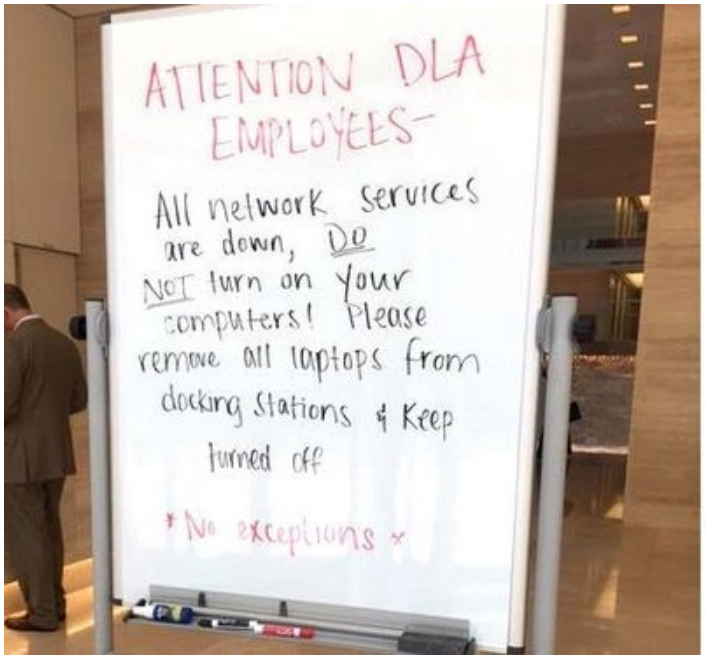
A report by Law360 Pulse revealed a spike in breaches of firms under 50 lawyers in 2021. From 33 breaches in 2020 to 68 breaches in 2021, an increase of more than **100%**, and 106 out of 116 breaches occurred due to hacking, phishing, or malware.

A report by Coveware indicates that Q1 of 2021 brought a **70%** increase in ransomware attacks on small and medium-sized law firms.

McGriff

Do law firms need cyber insurance?

YES. Any business that stores data online can use the protection that's offered through cyber security insurance.



Why add McGriff as your Broker and part of your Incident Response Team?

McGriff's market leverage is clear. We are the country's sixth largest broker backed by one of the country's biggest banks, Truist. While our market clout is strong, so is that of our largest competitors. What makes us different is not how much we broker, but how we broker, a concept we detail in our thoughtful, tailored approach to our responses contained herein. At our heart, McGriff is a boutique specialty firm uniquely structured and tailored to the specific risks presented by each of our clients.

What is your risk?

Failing to keep data secure is more than just a huge risk for any law firm—it can also have incredibly negative consequences for their clients. To threat actors, law firms are remarkably interesting. Valuable information—that may include trade secrets, intellectual property, merger and acquisition details, personally identifiable information (PII), and confidential attorney-client-privileged data—will attract the ill-intentioned to a firm.

Despite these risks, law firms are obligated to protect their clients' information. If criminals penetrate your firm's security, the consequences can be extensive—ranging from minor embarrassments to serious legal issues, including:

- Compromised communications due to phished or compromised email accounts
- Inability to access firm information due to ransomware (i.e., where hackers encrypt files and demand money to restore access)
- Public leaks of personal or business information (e.g., on social media)
- Loss of public and client trust in your firm
- Malpractice allegations and lawsuits

Common Cyber Attacks Law Firms Face

The 3 most common cybersecurity threats:

1. **Ransomware Threats:** Being denied access to systems and personal files and having them held under ransom by a threat actor is not a scenario in which you want a law firm and/or clients to be in.

2. **Weak Email Security Policies**: Phishing emails as a common method used by threat actors to gain access to law firms' networks. A common scenario of a phishing attack entails the use of a false email address that resembles closely a trusted and legitimate service, organization, or even a client to target employees of a law firm. There is often an attachment in those emails that is cleverly introduced as an e-contract, invoice, or anything that would further incite the receiver to click on it.

3. **Internal Threats To Law Firm Cybersecurity:** Outsiders and cybercriminals that lurk outside of a law firm's network are one thing, but having insiders with malicious intent is a whole different level of danger. And insider threats don't only count in resentful former employees, competitors, strategically placed insiders or just someone from the inside with malicious intent — one moment of carelessness from a staff member can lead to an unintentional data leak.

Quick Checklist

ABA Model Rules	Several of the ABA Model Rules are particularly related to safeguarding client data, including competence (Model Rule 1.1), communication (Model Rule 1.4), confidentiality of information (Model Rule 1.6) and supervision (Model Rules 5.1, 5.2 and 5.3).
Who is in charge in your firm?	Solo practitioners have the primary responsibility for the security of their firms. The larger the firm, the more likely it is to have expert consultants, IT staff or a chief information officer.
Security Programs and Policies	The firm has the responsibility of having a policy to manage the retention of data held by the firm including policy on email use, internet use, computer acceptable use, remote access, social media, for personal technology use/BYOD (Bring Your Own Device), employee privacy and others. • Lawyers must take “reasonable steps” to monitor for data breaches. • When a breach is detected, lawyers must act “reasonably and promptly” to fix the breach and mitigate resulting damages.
Incident Response Plan	Every law firm should establish a plan to follow in the event of a cyber breach. Further, like fire drills, law firms should practice cyber drills. Are documents routinely backed up? Are copies of the most important documents at an off-site, secure location? In the event of a hack or a ransom, does everyone know who to call? Do you have cyber liability coverage?
Cybersecurity Awareness Training	All attorneys, staff, and vendors must exercise the utmost level of cybersecurity care, awareness and diligence. Employing and/or training your team is the best prevention to a cyber incident
Clients Driving Cybersecurity Requirements	Lawyers have a duty to notify clients of breaches that have significant likelihood of involving client information. In addition, clients are now requesting to be notified of a cyber incident within a short period of time.

Securing Data

- **You're Responsible for Local Security**

Even when you use Cloud or hosted services, you are still responsible for the security of your local devices and your portion of the network you use to connect to your Internet Service Provider.

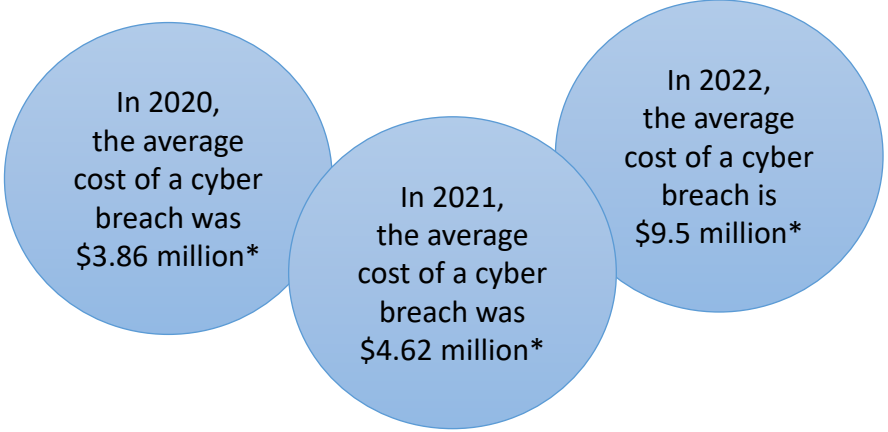
- **Restrict Remote Access**

Because cloud services make it easier for you to access data from anywhere, it also becomes easier for a third party to access your data from their own device. Review, among other things, the below:

- ❑ **Virtual Private Networks (VPNs)** work by creating an encrypted tunnel so that the information traveling over the Internet is protected from view by other people on that public WiFi network.
- ❑ **Remote Wipe** for any mobile device (smart phones, laptops, etc.) that has access to firm data or client information. Remote wipe allows you to delete files and information from a device even if you have lost physical access to it.
- ❑ **MFA**: protect the login process with two-factor authentication. MFA means you have to (1) enter your password, and (2) verify your identify by doing something like answering a secret question, or entering a code that is texted to your phone. You can also use an authenticator app on your phone.
- ❑ **Have a best practices for passwords:** Password length is the primary factor of password strength. If your password is too short, it is vulnerable to brute force attacks. "Password" is a Terrible Password.

Why Cyber Insurance?

Increased reliance on computer systems, technologies and access to information will significantly increase a company's exposure to cyber security threats. Purchasing cyber insurance is the first step to help protect you organization from significant losses experienced when cyber incidents occur.



Affirmative Protection	You don't have to be the target to be affected	Insurance covers response and recovery expenses	Adapting to emerging cyber risks	Complement to your Incident Response Team
• Traditional insurance policies may be inadequate or insufficient to respond to cyber exposures. • A cyber Policy is specifically designed to address these gaps and provide affirmative protection against exposure that can be difficult to grasp.	• Cyber attacks can spread through your suppliers or your outsourced technology providers, leading to significant impact even when you aren't the target. • We have seen significant collateral damage from cyber incidents originating at separate companies, arising from a vendor's cyber incident.	• Liability arising from the loss or misuse of sensitive data is only one potential outcome of a cyber incident. • Business interruption, incident response, and digital data recovery costs make up a significant portion of claims payments, even without liability claims.	• McGriff provides regular updates on trends and risks, keeping you aware of what is happening.	• Cyber insurance does not undermine the effectiveness of your teams – it supplements their skills and protects a business from the unknown.

*Data breaches are diverse; they can be targeted, self-spreading or come from an insider; affect individuals or businesses; steal data or demand ransoms. Data for 2020 gathered from "The Cost of a Data Breach" by IBM. The data for 2021, provided by Statista on their report "Average total cost per data breach worldwide 2021". Data for 2022 from ForgeRock in report titled "2022 ForgeRock Consumer Identity Breach Report".

McGriff

Understanding Cyber Insurance for Law Firms

It is a commonly held belief that cybersecurity and liability risk is insured by lawyers professional liability (LPL) coverage. Certainly, there is some truth, but there is more to digital privacy, cyber incidents, and cyber insurance than LPL is able to cover.

LPL coverage is intended to protect lawyers, and firms, against malpractice, human error, acts or omission, deemed wrongful, and breaches of fiduciary duty or contract. Nonetheless, if an attorney's or firm's networks, servers, or systems are attacked and breached, though, there is a chance that LPL will not be able to pick up all the tab. Some policies have a sublimated endorsement with very limited coverage. To be indemnified from such attacks lawyers and firms need to have a cyber policy.

To understand why cyber insurance, it is helpful to get a firm grip on what exactly these policies are and what they cover. The level of coverage your law firm needs is based on your individual operations and can vary depending on your range of exposure. It is important to work with McGriff who can identify your areas of risk and tailor your Cyber Insurance to meet your specific needs.

What Should Cyber Insurance For Law Firms Cover

When working with your broker on your cyber liability coverage, make sure your policy includes these coverage options, if applicable to your firm:

First-party coverage	Third-party coverage
Helps you respond to a cyber incident and the financial impact arising out of such. This can range from fees associated with restoring data, income loss due to downtime, crisis management, or forensic investigations—to name a few examples.	Helps pay for Claims made against you caused by a cyber incident. Coverage can span from payments to clients whose data is affected to regulatory fines for noncompliance.

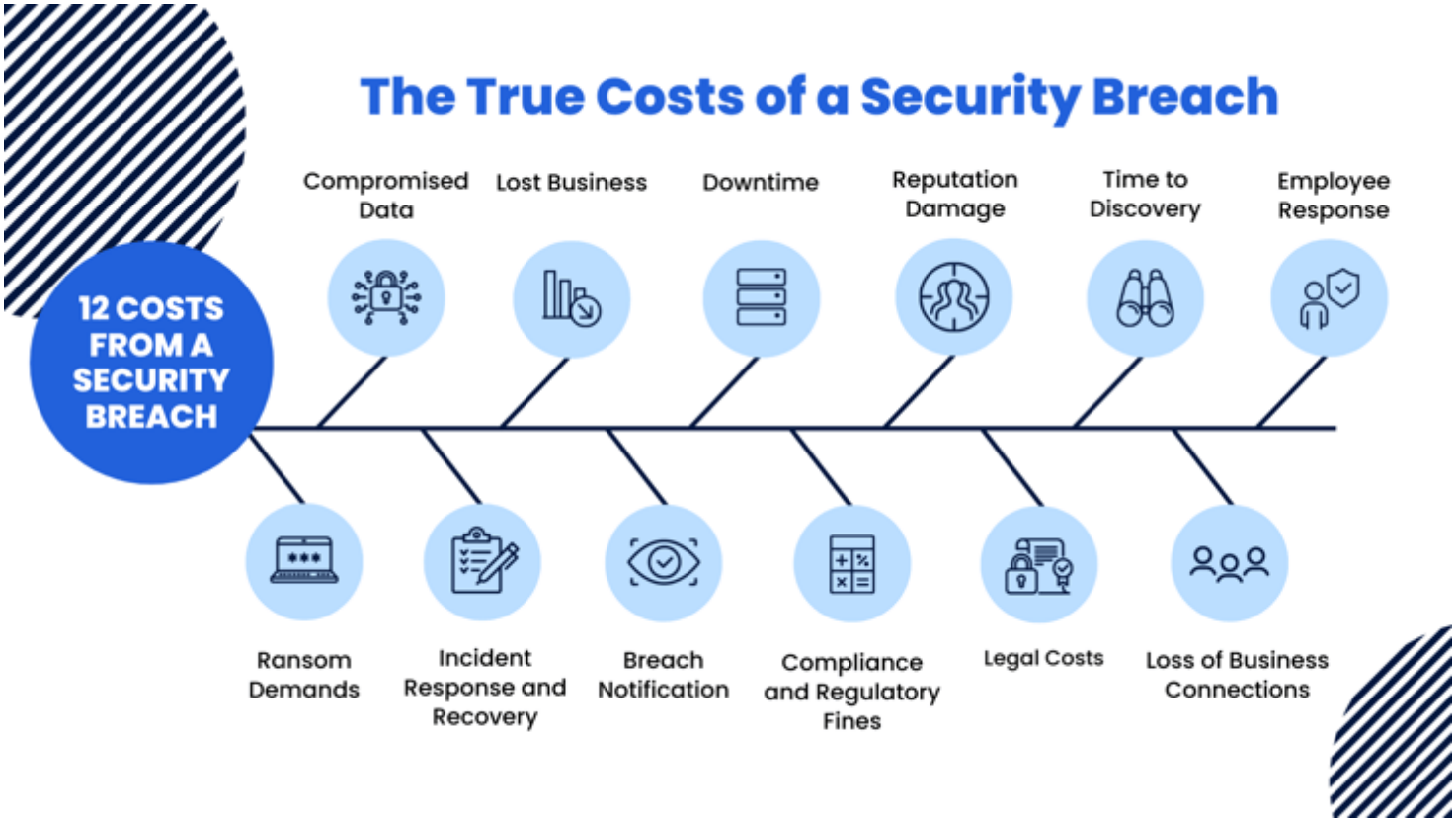
Understanding Cyber Insurance Coverage

Coverage	Description
Business Income / Extra Expense	Reimbursement for loss of income and/or extra expense resulting from an interruption or suspension of computer systems due to a network security breach; Coverage may be triggered by malicious attack, administrative mistake / human error, accidental damage or destruction. May Include event at outsourced technology service provider. Subject to hourly waiting period deductible.
Data Asset Protection	Reasonable and necessary expenses and costs incurred in restoring, updating, recreating, or replacing damaged digital assets (including data and software); Coverage triggered by same acts above for BI / EE
Cyber Extortion	Coverage for costs of consultants and extortion monies (including cryptocurrency) for threats related to interrupting access to systems and releasing or compromising private information
Data Breach & Crisis Management Response	Coverage for costs of complying with various breach notification laws and regulations, legal expenses, call centers, credit monitoring, forensic services, identity / fraud monitoring and public relations
Privacy and Security Liability	Defense and liability for the failure to prevent unauthorized access, disclosure or collection of confidential information, including failure of others to whom you have entrusted such information; failure to properly notify a privacy breach; defense and liability for the failure of system security to prevent or mitigate a computer attack or use of your systems to leapfrog into third party systems
PCI Related Liability	Liability to Card Brands and Acquiring Banks under Merchant Services Agreements; may include the fine or penalty levied for not being PCI compliant, and may include operating expenses of the Card Brands to research the compromised cards, an assessment for fraud incurred (or a percentage), and allocation for costs of Issuing Banks to reissue replacement cards
Regulatory Defense	Defense and liability arising out of a regulatory proceeding or investigation following an actual or alleged privacy or security breach; may include requests for information; may include fines, penalties and compensatory damages
Media Liability	Defense and liability for online libel, slander, misappropriation of name or likeness, plagiarism, copyright infringement, disparagement, negligence in publication of content; often covers social media

The Cost of a Security Breach

The effects of a security breach last far beyond the time it takes to contain and remediate the attack. Data breaches are expensive, in 2021 the average cost was around $5 million.

While this is a good indication of the severity of data breaches, it is still difficult for many organizations to recognize the true impact and related cost of a security breach. When a data breach occurs, an organization will face certain upfront costs like ransom demands, investigation into the attack, and remediation to repair and secure the network. After all of this is taken care of the attack is over. Yet, the aftermath of the breach is just beginning. The effects and related costs of a data breach can affect an organization for several years after the incident is contained. Often, the ongoing costs are far more than a ransom or the upfront costs of responding to an attack.



Responding to a Ransomware Attack

Ransomware is a type of malware that prevents users from accessing their system by encrypting files and demanding a ransom payment for the system to be unlocked. The ransom payment is usually requested in Bitcoin or in other cryptocurrencies that are difficult to trace. Cybercriminals will typically assign a deadline for the ransom to be paid, and if the deadline passes, the ransom payment will be doubled or the files permanently locked and sold in the dark web.

How to get cyber insurance for your law firm?

Determine what you need coverage for.
The first step is to conduct a comprehensive audit of the cyber security threat landscape within your firm. This will allow you to better understand your current risk, along with specific areas that you need to protect. You'll want to be clear on your most critical data—in other words, your "crown jewels"—so you're investing the most resources in safeguarding them.

Once you've gained a clearer picture of your security risk, you'll be one step closer to understanding the coverage needed. There isn't a clear formula for determining that. Rather, spend time reviewing your audit, assessing your budget, and choosing a coverage that best suits the needs of your firm. For instance, a larger firm that handles a significant amount of highly confidential information like medical records will want to invest in extra protection.

A final word on cyber insurance.
For all the efficiencies that technology delivers, one downside is that it also brings an increased risk of cyber threats. Sometimes, the damage can be so severe law firms simply can't recover from it. In fact, one study found that 60% of small businesses close after a cyber attack.

Although law firms can never be entirely secure, they can take steps to dramatically reduce their risk. That's why cyber insurance is key. It mitigates the financial costs to a law firm when attacks strike—helping lawyers get back to doing the work that truly matters.

Top-100 firm Ward Hadaway was blackmailed for up to $6m (£4.75m) in bitcoin after confidential documents were obtained in a cyber attack, the High Court heard today.

Ince Group granted injunction after ransomware attack

5 April 2022

CYBERSECURITY: LAWYERS NEED A BACK UP PLAN FOR THEIR BACKUP PLAN

Jul 15, 2022 By Jim Ash Senior Editor Top Stories

Bornstein & Bornstein, P.S.C.
28 April ·

Cyber thieves ransom Louisville law firm, vowing to publish stolen files if not paid
https://www.courier-journal.com/…/ransomware-at…/9538798002/

QUESTIONS

YOU'VE BEEN HACKED, AND NOW YOU'RE BEING SUED: THE DEVELOPING WORLD OF CYBERSECURITY LITIGATION

McGriff