CYBER SECURITY THREATS AND THE PRACTICE OF LAW:

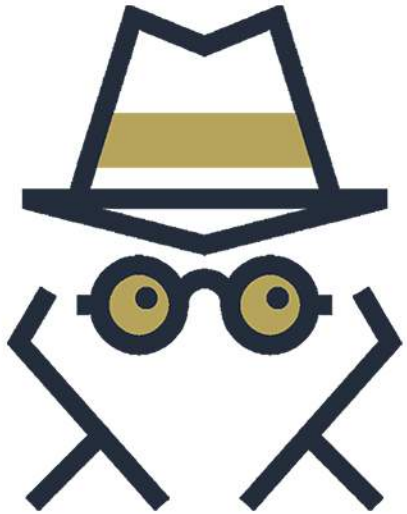
UNDERSTAND THREATS, PREVENT LOSSES, AND LEARN REQUIREMENTS

A PUBLICATION OF

LiabilityPro
INSURANCE ADVISORS

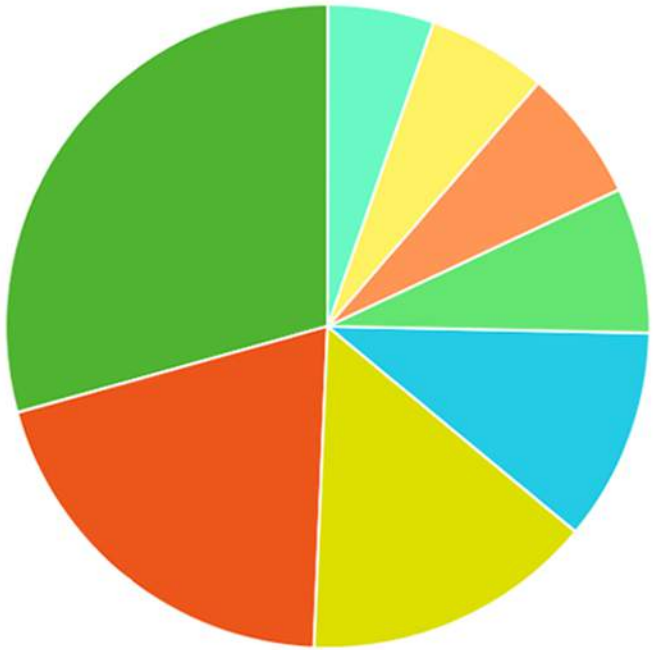
Each year brings newer technology and with that newer threats to sensitive information. It is important to stay on top of your security measures because there can be hefty financial repercussions if you don't. In this book we will cover what cyber threats you should be aware of, legal requirements for law firms, risk management strategies you can implement, how a stand-alone cyber insurance policy can protect your business and what to look for to optimize your purchase of a cyber insurance policy.

Where the threat comes from



Nationwide Insurance Company sponsored an online Harris Poll of some 500 U.S. small business owners with fewer than 300 employees between June 8 and June 19, 2015. 63% of small business owners surveyed admitted that they have been victims of at least one of the following:

- Computer Virus - 44%
- Phishing - 30%
- Trojan Horse - 22%
- Hacking - 16%
- Data Breach - 11%
- Unpatched Software - 10%
- Unauthorized Access to Customer Info - 9%
- Unauthorized Access to Company Info - 8%



An ABA Journal article reports that common sources of breaches of law firm confidential information include:

- Loss of an unencrypted laptop or other mobile device
- Insider misuse or mishandling
- Visiting questionable websites
- Downloading unapproved software onto the firm's network or mobile device
- Communication over unsecured or public networks
- Using a thumb drive on an unsecured network

The 2014 Verizon Data Breach Investigations Report found that 19% of the breaches reported were the result of insider misuse defined as intentional, non-intentional, legal, or illegal activity by an insider (attorneys, staff and third party partners) that resulted in the loss or exposure of confidential data.

Safelaw Solutions, a cyber liability insurance provider that markets a policy specifically designed for law firms, has published a collection of real life breaches that occurred at real law firms. The amounts listed are the company's estimate of the potential cost to the law firm. Here are a few of the more interesting examples provided:

Attorney working on documents for an investment deal leaves his laptop in his car overnight. In the morning, his back window is smashed and the laptop is stolen. Although the computer was password protected the hard drive was not encrypted. The laptop had investment documents and spreadsheets with names, addresses and other information for thousands of clients and investors.

Estimated cost: a breach at a small firm that lost data for 1,000 – 5,000 people is estimated at $600,000. The breach could also bring a lawsuit for professional negligence for hundreds of thousands of dollars alleging damage to the client's reputation.

During the peak of tax season, a tax law firm's network is infected with ransomware, a common malicious program (malware) that encrypts a firm's data and won't allow the company access until a ransom is paid. An employee opened an email disguised to look like a notice from their voicemail service. The email contained the ransomware. The firm's IT department has a backup of the data but in the process of wiping the firm's servers, the IT folks mishandle the data and the backup was lost as well.

Using a cost calculator, the resulting damage to a medium sized law firm with 20 lawyers who bill on the average $240 an hour, resulted in a two day outage costing $72,000 purely in lost productivity. The loss data could easily cost between $100,000 and $500,000 in potential lawsuits and the restoration costs.

An employee is responsible for destroying old desktop computers at a law firm. Rather than properly disposing of the computers with a company who will wipe the contents of the hard drives, the employee decides to take the computers to a pawn shop for a couple hundred dollars. The computers contained bank account information, social security numbers and other PII for 2,000 individuals.

In this example, no one is sued, but the company spends $10,000 to contact clients; $50,000 in reputational damage and $10,000 in loss of productivity.

The law firm does not make sure that it's cloud storage platform (e.g. Dropbox) encrypts data when it passes between servers. The storage site unencrypted their data while it was being stored and moved on its servers. The unencrypted data breaks HITECH and HIPAA standards and is considered a data breach.

The estimated cost for a data breach involving $10,000 protected health information records: the law firm can expect to pay $140,000 in notification, credit monitoring, and crisis management costs; $1,250,000 in HIPAA regulatory fines and sanctions; $100,000 from a client lawsuit; and $100,000 in damage to repair the firm's reputation for a whopping total of $1,590,000.

TAKEAWAY

There are many ways a law firm's confidential information may be breached from sophisticated malware attacks by hackers to unintentional internal mistakes like a stolen unencrypted laptop. Law firms are targets every day for breaches of confidential information which can result in lawsuits, regulatory fines, loss of reputation, loss of productivity and a loss of business.

Cyber threats are an ever increasing risk of financial and reputational loss

The Cyber Security Insurance industry reports that Law firms in general have been slow to recognize the threats that privacy and security breaches represent to their practices or have not taken these risks seriously. There has been recent publicity on businesses falling prey to cyber terrorism attacks. Sites have been corrupted, had lost or stolen data. Denial of service attacks or ransomed data are now common occurrences and law firms are learning, sometimes the hard way, that their businesses are not exempt from these attacks and, in fact, they make excellent targets.

Marsh's 2014 Global Law Firm Cyber Survey reports that "almost 80% of respondents consider cyber/privacy security to be one of their firm's top 10 risks and 40% place it as one of their top five risks".

Technology advancements are changing how businesses are run. A law firm's ability to protect sensitive client information, internal employee information and other personal identifiable information (PII) including personal health information are top privacy concerns for law firms; however, security challenges for law firms continue. Untrained lawyers and support staff are the number one weaknesses according to IT Execs in an ABA Journal article. Having security policies, people in place with authority to enforce such policies, and the reluctance to spend money for needed training, data security, and vulnerability assessments are also too common. Insurance coverage is readily available and affordable with more than 60 insurers offering cyber or privacy security policies, yet law firms are slow to take advantage of the insurance.

TAKEAWAY

Cyber security is a real concern for law firms. Experts advise that cyber liability best practices list cyber liability insurance as the number one consideration.

Ethical and legal requirements concerning confidential information

The ABA Model Rules stipulate under rule 1.6 (c) 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."

Comment 8 to Model Rule 1.1 provides additional guidance by explaining that:

> "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology....."

Lawyers are subject to ethical and legal requirements to protect the release and/or misuse of confidential information. “Confidential information” should not be available to the general public and can include various information that is routinely stored in a law firm’s computer system, or on external electronic devices like laptops, tablets, or phones. Confidential Information may include:

- Client Legal Information
- Evidence
- Background Research and Development
- Legal Strategies
- Expert Materials
- Legal Filings and Settlement Documents
- Business Information
- Commercial Financial Information
- Competitive Information
- Marketing Information
- Strategies and Planning Data
- Product Data
- Vendor Data
- Contractor Data
- Information Subject to a Confidentiality Agreement or Attorney Client Privilege
- Trade Secrets
- Patent Applications
- Data
- Designs
- Forecasts Formulas
- Methods
- Practices
- Processes
- Records
- Reports

The ABA's 2013 Cyber Security Handbook states that technology over the last 20 years has tested the application of the model rules: When a lawyer decides to use new technologies, the lawyer should have an understanding of the technology employed and he or she must take reasonable, prudent steps to preserve client confidentiality and balance the degree of sensitivity of the information with the need to take additional precautions.

TAKEAWAY

Law firms store all kinds of client confidential information on internal computer systems and external devices. The list of confidential information is expansive. The ABA has commented that its Model Rule 1.1 extends to changes in the practice of law including the benefits and risks associated with relevant technology.

Overall Risk Management Strategies

Law firms of all sizes have legal, ethical, and business obligations to secure client and firm confidential information. The ABA published recommended Best Practices in its news article entitled, “Experts Warn Law Firms to Protect Themselves Against Cyberattacks,” and in its 2013 Cyber Security Handbook.

Best Practices

- Maintain cyber liability insurance
- Conduct proper background screenings for new hires and vendors
- Choose a cyber liability insurer that provides a breach service provider, outside cyber counsel and crisis management provider to address reputational risk
- Provide e-learning certification courses to employees on safeguarding data
- Develop an incident response plan

- Conduct annual risk assessment exercises
- Know where your confidential information is stored and identify vulnerabilities
- Pre-arrange for cyber counsel or have available through your insurance carrier current state and federal disclosure laws
- Ensure encryption of confidential data on all computers, laptops, other portable devices and cloud storage providers
- Erase data from computers including printers prior to disposal
- Have systems to delete data remotely if a device is lost or stolen
- Have procedures in place to be sure current software protection is in place against viruses, malware and spyware
- Eliminate metadata from electronic documents before sending
- Disclose and have clients accept the risks associated with the use of technology
- Educate lawyers and staff on the confidentiality issues involved in discussing or making reference to a case via social media

TAKEAWAY

Cyber liability insurance is top on the list in risk management approaches to defeat the threat of cyber terrorism, but insurance isn't the only response for law firms that need to take cyber concerns seriously. Risk assessment, education and preparedness with a formal cyber liability response plan in place are all critical to contain financial disaster from a data breach, data loss or computer system disruption.

Why law firms (of any size) should consider a stand-alone cyber insurance policy

Ace Insurance Company in its brochure, The evolution of Cyber Risk, reports that only 11% of all cyber claims actually involve a professional liability lawsuit. Some, but not all, professional liability insurers include some basic cyber exposures in their malpractice policies. The coverage includes the traditional third party exposures centered around damage to a client's computer system or breach of a client's confidential information. Such coverage may also include some first party coverage for the law firm including notification and credit report monitoring expense and may even respond to regulatory fines and sanctions (usually subject to a lower sublimit). The coverage afforded, however, under a professional liability policy rarely comes close to covering all of the potential first party expenses associated with a breach of a law firm's computer system.

A stand-alone Cyber Liability Policy provides a separate limit of liability so that the firm's professional liability limit is not depleted. A cyber liability policy covers both third party and first party costs associated with most if not all claims arising from:

Privacy and Data Breach Liability

- Failure to protect sensitive personal or corporate information including employee data in any format
- Provides coverage for regulatory proceedings brought by a governmental agency alleging violation of any identity theft or privacy protection law.
- Covers fines and penalties associated with data breach laws
- Covers expense for a forensics expert to verify and determine the scope of a breach
- Pays for Cyber Counsel to advise on the latest regulatory, ethical and legal malpractice requirements in a data breach.
- Pays for notification and credit monitoring expenses to affected individuals.
- Covers public relations or reputation reparation expense for the insured organization.
- Crisis management expense

Network Security Liability

- Liability of the insured organization arising out of the failure of network security including internal or external unauthorized access or unauthorized use of corporate systems, a denial of service attack or transmission of malicious code
- May cover extortion or ransom money and expenses out of criminal threat to release sensitive information or crash a network.

Internet Media Liability

- Covers copyright infringement, invasion of privacy, libel or slander arising out of the organization's internet site.

Business Interruption

- Covers loss of income or loss of billable hours resulting from viruses, malware or DDOS attacks.

Data Recovery

- Covers the insured organization's costs to recover or restore lost data due to a computer hacker, virus, a denial of service attack or administrative errors.

Breach Response Resources (An effective cyber insurance plan will provide the policyholder with access to cyber security breach experts):

- Security auditors at forensic companies to identify the source and scope of the data breach, aid in the recovery, restoration or replacement of data and software as well as removal of a hacker's tools. These security partners should have the expertise to determine if the law firm is in compliance with current ethical and legal cyber security requirements.
- Public relation companies experienced in working with law firms and can effectively design and execute a tailored public response to the breach.
- Notification Services that will assist in the drafting and delivery of notificaions to clients, opposing counsel, courts, State Attorney Generals, law enforcement and credit bureaus.

- Provide credit and internet monitoring services that will alert the exposed individual if nonpublic personal information has been made public.
- There is a lag between when legal services are performed, billed and paid for. Most cyber liability insurance policies include standard business income coverage which does not take this lag time into consideration. Forensic accounting and loss valuation firms will help you determine the value of the economic loss including the inability to bill for current services that are not represented in historical cash flow models.

TAKEAWAY

Professional liability policies may cover some third party and first party losses and expenses from a cyber liability incident, but usually fall short on coverage for all first party losses and expenses. A stand-alone cyber liability policy can provide coverage up to its full limit of liability for most first party and third party cyber liability exposures without the risk of reducing your professional liability policy limits. A carrier's breach response team with 24/7 technical advice in the event of an actual or suspected security breach is equally important with today's ever expanding cyber threats.

What to look for in a stand-alone cyber insurance policy

Cyber liability insurance, just like professional liability insurance, is all uniquely designed and marketed and can vary substantially in coverage terms and premiums. That is why an independent professional liability insurance broker is a good idea to help you analyze your risk and choose the best cyber liability insurance to meet your exposure needs and premium budget.

Look for innocent partner coverage to provide protection to any member of the firm that did not participate in or had knowledge of or consented to a fraudulent claim, data breach, data loss or computer disruption. Cyber insurance policies often include a “control group” definition to define coverage for the acts of an inside rogue employee. If a member of control group is that rogue employee, the policy can become void and coverage for any claims forfeited.

In order to keep insurance premiums competitive, some cyber liability insurers require certain minimum anti-virus and malware prevention solutions on the policyholder's computer system and require regular updates and firewall maintenance including a formal patch management system and procedures. All confidential information must be encrypted on all remote devices. Generally, these minimum requirements must be met in order for coverage to apply.

Additionally, some carriers offer coverage that specifically dovetails with any coverage afforded under a professional liability policy. This helps to eliminate the coverage gaps and conflicts when two policies and usually two different insurers respond to the same claim. If the professional liability policy provides full coverage, then the cyber carrier provides excess coverage usually with no deductible obligation. If the professional liability insurer provides only partial coverage for the claim, then the cyber insurance carrier drops down and covers the uncovered portion of the claim. If no coverage exists under the PL policy, then the cyber carrier is the primary insurer.

Beware: Some cyber security insurance policies exclude terrorist acts or exclude breaches by a third party service provider such as a cloud provider.

TAKEAWAY

Cyber liability insurance policies are all crafted differently and may or may not dovetail with coverage provided by your professional liability insurance. Use an independent professional liability insurance broker skilled with the knowledge of different cyber liability insurance policies to help you analyze your risk and choose the best cyber liability insurance to address your critical exposure needs.

Review

Lawyers are subject to ethical and legal requirements to protect the release or misuse of confidential information. Surveys have shown that a law firm's ability to protect sensitive client information, internal employee information and other personal identifiable information are top privacy concerns for law firms today, but not without security challenges. Internal training is the number one weakness contributing to the unintentional introduction of malware on networks followed by lost or stolen external devices unprotected with encryption. Strategies to defend against this cyber terrorism threat recommend that cyber liability insurance including coverage for the law firm's breach expenses be included in the first line of defense, but also that risk assessment, education and preparedness with a formal cyber liability response plan be put in place and endorsed by law firm leadership. All of these solutions are critical to contain financial disaster from a data breach, data loss or computer system disruption.

Protect Your Law Firm

Look into Cyber Liability Insurance coverage now, premiums are very affordable but won't stay that way as claims continue to occur. A stand-alone Cyber Liability Insurance product offered by a specialized Cyber Liability Insurer will give you access to resources so you will be prepared to fight back against the ever changing Cyber Security threat and stand with you should a breach occur.

Receive more educational info from LiabilityPro

Subscribe

For more help understanding Cyber Liability Insurance

Contact Us

Get your Cyber Liability quote today

Get Started

*Coverage terms subject to underwriting acceptability and actual policy terms and conditions'

LiabilityPro INSURANCE ADVISORS

Sources

ABA Journal April 2015 Net Risk: Cyber liability insurance is an increasingly popular, almost necessary choice for law firms

AMERICAN BAR ASSOCIATION COMMISSION ON ETHICS 20/20 in regards to ABA Model Rules of Professional Conduct dated August 2012, providing guidance regarding lawyers' use of technology and confidentiality

Attorneys must keep pace with technological advancements to meet their "duty of competence" to clients BY MATT NELSON MARCH 28, 2013

ABA News Archives 10/2014 Experts warn law firms to Protect against cyberattacks

Des Moines Register- The 2015 Small Business Owner Study commissioned by Nationwide and conducted by Harris Poll Online

SafeLaw Cyber Liability Insurance website: www.safelawsolutions.com