STATE BAR OF WISCONSIN
PINNACLE
Your Practice. Our Purpose.

WSSFC 2025

Practice Management Track – Session 1

Lock it Down: Cybersecurity Essentials for Small Law Practice

Presenters:
Katharine H. Campbell, Neal Gerber & Eisenberg LLP, Chicago, IL
Thomas J. Watson, Wisconsin Lawyers Mutual Insurance Company, Madison

About the Presenters...

Kate Campbell is a Partner at Neal Gerber & Eisenberg, a Chicago law firm, and a member of the firm's Cybersecurity & Data Privacy team. She has several certifications from the International Association of Privacy Professionals and regularly counsels clients on cybersecurity related incidents and issues.

Thomas J. Watson is President and CEO at Wisconsin Lawyers Mutual Insurance Company (WILMIC). He has been with WILMIC since 2005. Prior to becoming President and CEO, Tom was Senior Vice President, overseeing Underwriting and Claims, and developing and coordinating the company's risk management programs and law firm and lawyer outreach. He is a 1981 Marquette University graduate with a degree in Journalism and Broadcast Communications and a 2002 graduate of Marquette University Law School. Watson was the Public Relations Coordinator for the State Bar of Wisconsin for more than seven years, and was then in private practice in Madison, focusing primarily on Family Law, before joining WILMIC. He serves on the Editorial Board of the State Bar of Wisconsin's *Wisconsin Lawyer* magazine.

Lock it Down: Cybersecurity Essentials for Small Law Practices

State Bar of Wisconsin Solo and Small Firm Conference
Thursday, October 16th

Thomas J. Watson
WILMIC, President & CEO

I. Why Should Attorneys Care About Artificial Intelligence (AI) and Cyber Risk Exposure?

A. It is Your Ethical Duty to Be Concerned about AI

1. The ABA Standing Committee on Ethics and Professional Responsibility has issued its first formal opinion, focusing on the use of generative AI by lawyers. American Bar Assoc. Standing Committee on Ethics and Professional Responsibility, Op. 512 (7/29/ 2024). The following excerpts recently appeared in "The AI Revolution in Law: There's No Turning Back," *Wisconsin Lawyer,* 97 Wis. Law. 41-44 (November 2024)

    a. **Model Rule 1.1 – Competence -** "To competently use a GAI [generative artificial intelligence] tool in a client representation, lawyers need not become GAI experts. Rather, lawyers must have a reasonable understanding of the capabilities and limitations… Because GAI tools are subject to mistakes, lawyers' uncritical reliance on content created by a GAI tool can result in inaccurate legal advice to clients or misleading representations to courts and third parties. Therefore, a lawyer's reliance on, or submission of, a GAI tool's output—without an appropriate degree of independent verification or review of its output—could violate the duty to provide competent representation as required by Model Rule 1.1."

    b. **Model Rules 1.6, 1.9(c), and 1.18(b) – Confidentiality** – "Before lawyers input information relating to the representation of a client into a GAI tool, they must evaluate the risks that the information will be disclosed to or accessed by others outside the firm. Lawyers must also evaluate the risk that the information will be disclosed to or accessed by others inside the firm who will not adequately protect the information from improper disclosure or use… Because GAI tools now available differ in their ability to ensure that information relating to the representation is protected from impermissible disclosure and access, this risk analysis will be fact-driven and depend on the client, the matter, the task, and the GAI tool used to perform it."

    c. **Model Rule 1.4 – Communication** – "Of course, lawyers must disclose their GAI practices if asked by a client how they conducted their work, or whether GAI technologies were employed in doing so, or if the client expressly requires disclosure under the terms of the engagement agreement or the client's outside counsel guidelines. There are also situations where Model Rule 1.4 requires lawyers to discuss their use of GAI tools unprompted by the client.40 For

example, as discussed in the previous section, clients would need to be informed in advance, and to give informed consent, if the lawyer proposes to input information relating to the representation into the GAI tool. Lawyers must also consult clients when the use of a GAI tool is relevant to the basis or reasonableness of a lawyer's fee."

d. **Model Rules 3.1, 3.3, and 8.4(c) – Meritorious Claims and Candor** – "In judicial proceedings, duties to the tribunal likewise require lawyers, before submitting materials to a court, to review these outputs, including analysis and citations to authority, and to correct errors, including misstatements of law and fact, a failure to include controlling legal authority, and misleading arguments."

e. **Model Rules 5.1 and 5.3 – Supervisory Responsibilities** - "Managerial lawyers must establish clear policies regarding the law firm's permissible use of GAI, and supervisory lawyers must make reasonable efforts to ensure that the firm's lawyers and nonlawyers comply with their professional obligations when using GAI tools. Supervisory obligations also include ensuring that subordinate lawyers and nonlawyers are trained, including in the ethical and practical use of the GAI tools relevant to their work as well as on risks associated with relevant GAI use." The opinion also discusses a lawyer's obligations to vet third party providers, as discussed in prior ABA opinions.

f. **Model Rule 1.5 – Fees** – "…before charging the client for the use of the GAI tools or services, the lawyer must explain the basis for the charge, preferably in writing… If a lawyer uses a GAI tool to draft a pleading and expends 15 minutes to input the relevant information into the GAI program, the lawyer may charge for the 15 minutes as well as for the time the lawyer expends to review the resulting draft for accuracy and completeness." The lawyer should also consider whether a cost is overhead or an out-of-pocket expense, "For example, when a lawyer uses a GAI tool embedded in or added to the lawyer's word processing software to check grammar in documents the lawyer drafts, the cost of the tool should be considered to be overhead. In contrast, when a lawyer uses a third-party provider's GAI service to review thousands of voluminous contracts for a particular client and the provider charges the lawyer for using the tool on a per-use basis, it would ordinarily be reasonable for the lawyer to bill the client as an expense for the actual out-of-pocket expense incurred for using that tool."

B. Lawyers are not the only ones using AI in the legal world. Technology hackers are more active than ever before, capitalizing on the pandemic chaos and the emergence of generative artificial intelligence to ramp up their attacks.

1. AI cyber-attacks have risen tremendously since the mainstream use of the technology. In the absence of a moral compass, AI systems can be taught to carry out cyber-attacks.

2. AI allows cyber criminals to automate and simplify hacking processes – making it an easy route for novices and newcomers in the field. Defining AI Hacking: The Rise of AI Cyber Attacks.

    a. Generative AI can be used to automatically create convincing emails or documents to lure people into phishing campaigns.

    b. Generative AI can also create malware that can evolve to fix itself as needed to infiltrate a network or exploit a vulnerability. Moreover, AI can be used to create deep fake videos to manipulate people. AI is an innovative tool that can be weaponized to create cyber threats that are self-learning, increasingly persuasive, and worryingly invulnerable.

B. Lawyers handle a significant amount of client data, which they have a legal and ethical duty to protect electronically stored information under SCR 20:1.6..

1. Law firms are highly attractive to cyber criminals.

    a. April 2024 - Orrick, Herrington & Sutcliffe paid $8 million to settle class action claims stemming from a March 2023 data breach. Hackers accessed the names, addresses, dates of birth, and Social Security numbers of more than 600,000 individuals from files stored by the law firm. Among other claims, plaintiffs alleged the law firm did not inform the victims of the data breach for over one year.

    b. March 2024 - Commercial and business litigation firm Houser LLP failed to protect the personal information of more than 325,000 people that was exposed in a May 2023 ransomware attack and data breach, two proposed federal class actions said.

    c. Checkpoint Research reported in April 2023 all sorts of organizations, in the first quarter, experienced 1,248 attacks. One out of every 40 attacks targeted a law firm or an insurance provider.

2. Most significant exposure – theft or loss of personal or corporate information in the firm's care, custody or control.

This includes:

a. Confidential information regarding clients' corporate finances.

b. Documents regarding corporate transactions.

c. Personal information such as financial records, health records, Social Security numbers, intellectual property, depositions and criminal records.

3. Ethical obligations:

SCR 20:1.1 Competence A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

ABA Comment

Maintaining Competence [8] 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, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Atty. Dean Dietrich, past chair of the State Bar of Wisconsin Professional Ethics Committee, in *Wisconsin Lawyer* magazine, July 2017:

> "The essence of this comment is that lawyers need to understand how they use different types of technology and different types of electronic devices to provide services to their clients and also understand the benefits and the risks of using these new technology advancements.
>
> As has been often stated, this comment does not mean that all lawyers must go back to school to obtain an electrical engineering or computer science degree, but it does mean that lawyers need to understand the different types of technology that they use to practice law."

ETHICS OPINION

A lawyer may use cloud computing as long as the lawyer uses reasonable efforts to adequately address the risks associated with it. The Rules of Professional Conduct require that lawyers act competently both to protect client information and confidentiality, and to protect the lawyer's ability to reliably access and provide relevant client information when needed.

To be reasonable, the lawyer's efforts must be commensurate with the risks presented. Among the factors to be considered in assessing that risk are the information's sensitivity; the client's instructions and circumstances; the possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party; the attorney's ability to assess the technology's level of security; the likelihood of disclosure if additional safeguards are not employed; the cost of employing additional safeguards; the difficulty of implementing the safeguards; the extent to which the safeguards adversely affect the lawyer's ability to represent clients; the need for increased accessibility and the urgency of the situation; the experience and reputation of the service provider; the terms of the agreement with the service provider; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.

To determine what efforts are reasonable, lawyers should understand the importance of computer security, such as the use of firewalls, virus and spyware programs, operating systems updates, strong passwords and multifactor authentication, and encryption for information stored both in the cloud and on the ground. Lawyers should also understand the dangers of using public Wi-Fi and file sharing sites. Lawyers who outsource cloud computing services should understand the importance of selecting a provider that uses appropriate security protocols. Lawyers should also understand the importance of regularly backing up data and storing data in more than one place. A lawyer may consult with someone who has the necessary knowledge to help determine what efforts are reasonable.

EF-15-01 Amended, September 8, 2017.

ABA Commission on Ethics 20/20:

"Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [8] specifies that, to remain competent, lawyers need to 'keep abreast of changes in the law and its practice.' The Commission concluded that, in order to keep

abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document."

Other Relevant Ethical Obligations: SCR 20:1.6 Confidentiality, SCR 20:1.4 Communication, SCR 20:5.1 Responsibilities of a Partners, Managers, Supervisory Lawyers, SCR 20:5.3 Responsibilities Regarding Non-Lawyer Assistance

ABA Formal Opinion 477R (related to securing communication of protected client information)

Lawyers have a duty to do the following related to email communications based on Model Rule 1.6(c) [which has not been adopted by Wisconsin]

- Understand the nature of the threat.
- Understand how client confidential information is transmitted and where it is stored.
- Understand and use reasonable electronic security measures
- Determine how electronic communications about client matters should be protected.
- Train lawyers and non-lawyer assistants in technology and information security.
- Conduct due diligence on vendors.
- Model Rule 1.4(c) may require a lawyer to discuss security safeguards with clients.

ABA Formal Opinion 483

- "The opinion underscores the importance for lawyers to both plan beforehand for an electronic breach or cyberattack and to understand how model rules come into play when an incident is either detected or suspected." *See* ABA Issues New Guidance on Layer Obligations After a Cyber Breach or Attack, ABA (Oct. 17, 2018).
- References Model Rule 1.15 (Safekeeping Property), which requires lawyers to protect trust accounts, documents and property the lawyer is holding for clients or third parties, as a fiduciary.

- Lawyers have a duty to notify clients of a data breach under Model Rule 1.4 "in sufficient detail to keep clients 'reasonably informed' and with an explanation 'to the extent necessary to permit the client to make informed decisions regarding the representation**."**

C. Many lawyers work with real estate clients and/or wire funds as part of their business practice. In recent years, an increasing percentage of these firms have become victims of eCrime. In particular, wire transfer schemes based on business email compromises, or social engineering.

D. Other exposures for law firms:

1. Ransomware

   Ransomware expenses or the cost to repair/recreate data damages by a ransomware may be significant. Ransomware has been the most common type of cyber security incident in the past couple years.

2. System outage

   Law firms rely on computer systems. An extended outage of a computer system may result in significant extra business expenses or a loss of business income.

3. Vendors

   A law firm's information can be access when a vendor experiences a data breach, highlighting the importance of conducting due diligence on vendors and reviewing vendor contracts to see how a firm's liabilities resulting from the same would be covered or indemnified by the vendor.

Examples: Vendor Advanced exposed information from 193 law firms.

E. Law firm websites and usage of the internet have become the 21st century law firm "buildings" – especially since the pandemic hit in March 2020.

II. Key Statistics

In the last three years:

- 30 percent of fraudulent wire transfer loss events were associated with professional services firms.

- 21 percent of ransomware claims were associated with professional services firms.

- The average fraudulent wire transfer loss payout nationally was $51,000.

Source: netDiligence Cyber Claims Study

- Average cost of breach for a small to medium enterprise is $178,000 (median of $48,000).

Source: NetDiligence Cyber Claims Study 2019 Report

III. Where does "PII" come from? Where is it stored?

A. Comes from:

- Clients
- Employees
- Credit card companies
- Financial institutions – banks
- Vendors
- Other businesses

B. Stored in:

- Law firm network computers/laptops
- Employees' home computers
- Disks/tapes
- Databases
- Flash drives
- Smart phones/tablets
- Printers
- Copy machines
- Vendor's systems/software

IV. Law firm dependency on technology

A. This dependency creates a business risk not covered in standard Business Owners Policies and only partially covered in professional liability policies.

B. Law firms gather and transmit Personally Identifiable Information (PII) from their clients such as names, addresses, birth dates, social security numbers, credit card information, and medical information.

V. Security Breach/Notification Requirements

A. Inadvertent disclosure of PII creates the possibility of identity theft. Wisconsin, along with 48 other states, has a law requiring PII to be protected and notification to affected persons if PII security has been breached.

B. The average cost for each PII record that is lost is $50-$214. This cost includes notification to victims, investigative expenses to determine loss, and credit monitoring for managing identity theft.

C. PII can be lost by something as simple as leaving a laptop or cell phone in an airplane or coffee shop, or by something as complex as a hacker attack or Botnet on a law firm's information system.

D. A loss of PII is a significant event for a law firm, requiring a prompt, effective and legally sufficient response. Unfortunately, most lawyers and law firms are not equipped to make this response.

E. Wis. Stat. § 134.98 outlines notification requirements, including language, timeline and notice to regulators.

VI. Are law firms attractive to cyber criminals? If so, why? And in what ways do cyber criminals often try to take advantage of law firms and their systems?

A. Cyber criminals find certain law firms very attractive to target.

B. It's likely that every law firm that is engaged in real estate transactions has been targeted for attack. Attacks against law firms are both widespread phishing attacks and individually and specifically targeted spear phishing attacks. Simply follow the funds. The criminals target firms involved in real estate transactions, whereby they can hack into computers, impersonate the firm, falsify payment details and abscond with funds sent by wire to the wrong accoun

VII. What are the most common methods cyber criminals use to compromise law firms' technology systems? Do they also use law firm employees? How so?

A. Phishing

Phishing attacks are simple and effective. Click on a link in an email about COVID or perhaps an email from a fellow employee, family member or vendor. That link will often have malware that the criminal uses to then record your keystrokes. They uncover your username and passcode and voila, they are in your system using your email and looking at your files. Support staff all the way to partners are exposed and targeted. Would you click on a link that looks 100% legitimate and that came from the CEO, CFO or managing partner?

B. Remote Desktop Protocol (RDP)

Separately, technology today can scan the entire internet and find computers that have vulnerabilities. More specifically, if firms allow remote access to workstations, called RDP for remote desktop protocol, criminals will search for it, find it, attack it and gain access by using a phishing scam or mere brute force. Once again, they are in your system and masquerade as you or encrypt all the files and hold you ransom.

C. What is the most significant and common exposures for law firms?

For law firms, email systems are most commonly under attack. Again, when a criminal can masquerade as a member of the firm, seriously bad things occur. Most of our law firm clients use Microsoft 365, like we do. At a minimum, M365 needs to have 2-Factor authentication enabled to restrict access, have logging enabled and restrict email forwarding.

VIII. Law Firm Cyber Claims Real Life Examples

A. Wire Fraud

The Law Firm was engaged for a real estate transaction. The Firm's client, the Seller, had an email account that was breached. The Seller received false information from an imposter and from an email address similar to that of the Law firm. The Law Firm received and then forwarded these fraudulent instructions to the buyer who then sent $552k astray. Just prior to this transaction, the Law Firm also had an employee that had their Microsoft 365 email hacked. Investigation expenses, legal fees and damages were incurred.

B. Breach

The Law Firm's email was hacked and login credentials were obtained through Microsoft 365. The bad actor had access to the Firm's email records and communicated fraudulent wire instructions for a real estate transaction to a Client. $145,000 in funds were wired to an unknown account and unrecoverable.

C. Data Breach

The Law Firm received telephone calls from their clients relating to suspicious emails the clients had received. A prompt investigation indicated that emails were being sent from an employee's online Microsoft Office 365 account. It was confirmed that unauthorized access to Microsoft 365 was made and many emails were sent fraudulently. Also, years of data in Microsoft 365 were exposed.

D. Ransomware

The Law Firm suffered a malware and ransomware incident. While no ransom demand was paid, efforts were made by the Firm's I.T. Vendor to help get the Firm operational again with an exception of the Firm's QuickBooks records that were damaged completely and unrecoverable as a result of the malware.

E. Data Breach

The Law Firm's Office was burglarized. A company laptop was stolen that contained sensitive details on clients in multiple states, including their SSNs.

F. Phishing

This Law Firm has an employee that received an email purportedly from the CEO. She followed the instructions and wired roughly $10,000 to an imposter who ran away with the funds.

G. Phishing

The Firm received notice from their encryption email vendor that a number of emails were being forwarded to an unknown Gmail account. It was confirmed that unauthorized access to Microsoft 365 was made and that a rule was created to forward emails to a rogue Gmail account.

H. eMail Breach

The Law Firm's Microsoft 365 Outlook email was hacked and any emails that were sent to a specific employee from other employees were redirected out to a third-party source/hacker. Researching activity over several weeks, numerous emails were identified as having sensitive PII.

I. Unauthorized Disclosure of Personally Identifiable Information

The Law Firm sent an email with sensitive information regarding a real estate transaction astray when the email was sent with a typo in the recipient address.

J. eMail Spoof

The Law Firm's client received an email from what appeared to be from the Firm; however, it was an imposter email and not from the Firm. The Firm's client sent $19,400 astray to a Wells Fargo account not belonging to the Firm or the Client.

IX. Cyber Insurance & Risk Management

A. Prevention – Essential Risk Management – Be Prepared

Wisconsin Formal Ethics Opinion EF-21-02: "Working Remotely," 1/29/21:

> "Because working remotely relies on technology, competence in technology and cybersecurity practices are essential. The following cybersecurity practices have been recommended by a number of ethics opinions and other resources. None of these practices are new: they are reasonable precautions that have helped lawyers fulfill their ethical obligations, especially the duty of confidentiality, when working in the office and when working remotely, whether at home during evenings and weekends, or during travel for work or vacation."

1. Know who has access to personal information

2. Develop and Implement a Written Information Security plan

   Outline security controls and business practices for handling PII that addresses the security and confidentiality of PII and protecting against any anticipated threats or hazards to the security and integrity of such information

3. Protect against unauthorized access to or use of such information that creates substantial risk

4. Conduct background checks on employees who have access to PII (many acts of theft occur within a company or law firm

5. Develop and Practice an Incident Response Plan

6. Engage data security and privacy counsel prior to a breach that:

   a. can assist with reviewing and practicing Incident Response Plan

b. can be identified in your cyber liability policy, so you are not required to use data breach counsel without institutional knowledge of your operations

c. can assist in the review of your cyber liability policy to ensure there are no surprise sublimits or exclusions, and that coverage is commensurate with the risk

7. Be Alert and Stay Alert.

a. Train employees

b. Law firm wide privacy risk and awareness training on an annual/semi-annual basis.

c. Conduct an audit on your computers, printers, scanners, copiers, wireless devices and any other electronic devices that can store personal or sensitive information to determine if PII is unnecessarily stored in an unintended place.

d. Monitor and watch for common fraud schemes

- Social engineering involved wire fraud
- Confirm money transfers through non-email means (Out of Band Communications)
- Phishing, including spear phishing and whaling

  - If you weren't expecting it, or don't know the sender, don't open it – TEST YOUR PEOPLE.

  - Deal with important messages on non-mobile devices, where URL verification is easier.

  - Carefully read the email address for intentional misspellings – *e.g.,* www.northemtrust.com instead of www.northerntrust.com.

8. Use technological measures to reduce the attack surface and mitigate common risks:

a. Maintain firewalls on any computer device connected to the internet.

b. Use anti-virus software and update it no less than every 30 days.

9. Use strong passwords or have password managers

10. Store client data records in a locked file cabinet or room

11. Securely destroy information that is no longer necessary to retain, through a retention/destruction policy, including, for exampling, shredding any paper-based PII documents when recycling or disposing

12. Encryption
13. Two-factor authentication

14. Testing—penetration testing, social engineering, etc.

B. Protection - Cyber Insurance Coverage

1. The Basics

a. Cyber liability insurance covers financial loss due to data breaches and other cyber events, including theft, loss or unauthorized disclosure of protected information in the care, custody or control of the insured.

b. Many policies cover first-party and third-party claims.

i. First party claim – out-of-pocket expenses that a firm directly incurs as a result of a data breach or cyber event (e.g., costs incurred to notify subjects of the data breach, cost of restoring data, ransoms paid, costs incurred to manage a crisis)

ii. Third-party claim – damages or settlements a firm is obligated to pay as a result of injuries resulting from the firm's negligence (e.g., a client sues his lawyer for negligence after a hacker breaches the firm's IT system, steals the client's confidential information and publishes it on the web).

c. Typical Exclusions

i. Bodily injury and property damage.
ii. Intentional acts committed by the insured.
iii. War and terrorism.
iv. Contractual liability.
v. Utility failure.
vi. Costs of upgrades after restoration.

2. Cyber Extortion / Ransomware

Ransomware, one of the fastest growing areas of cybercrime, refers to malicious software that is specifically designed to take control of a computer system or its data and hold it hostage so the attackers can demand payment from their victims.

3. Dependent eNetwork Interruption

In the interconnected global economy, a company's business may rely on the operations and products/services of another company (think of an Auto Manufacturer relying on the supply of steel for the production of vehicles, or an online retailer relying on the functionality and dependability of a 3rd parties hosting platform).

4. Dependent Business Interruption loss, also known as Contingent Business

Interruption loss occurs as the insured is unable to access the necessary materials or services which support the insured's operations (raw materials, website functionality, cloud service provider, etc.), thus impacting revenues.

5. Business Interruption & Data Reconstruction

A network interruption loss happens when a cyber-event causes a disruption in the operations of a company, which results in lost business revenue. Some of the more common cyber-attacks against businesses which may lead to a NI Loss include denial-of-service, insertion of malware or malicious code, and ransomware.

6. Social Engineering & eCrime

Also known as Fraudulent Wire Transfer Loss, a social engineering scheme is accomplished by tricking an employee of a company into transferring funds to a fraudster. The fraudster sends

an email impersonating a vendor, client, or supervisor of the company and advises that banking information for the vendor/client has changed or company funds immediately need to be wired at the "supervisor's" direction. The email looks authentic because it has the right logos and company information and only careful study of the email will reveal that the funds are being sent to the fraudster's account. Unsuspecting and trusting employees unwittingly have cost their companies millions of dollars in connection with social engineering claims.

C. Response

1. Having access to an Incident Response Team is critical when faced with a cyber incident. Review access to the Incident Response team afterhours—when most ransomware attacks hit.

2. Cyber insurance policies typically include a Cyber Response Unit, who are knowledgeable about cyber related attacks. The Cyber Response Unit can provide access to or coverage for a breach coach that can help guide you through an incident. The Cyber Response Unit can also make recommendations for trusted third party service providers-likes forensics investigators and ransomware negotiators.

3. Helps assess and contain the loss, preserve evidence, and support continuity of the business. You will need help with data forensics and an investigation into exactly what happened.

X. State of the Cyber Security Insurance Market

For years, WILMIC has been telling its policyholders how vulnerable IT systems can be and all the ways you need to protect yourself, including with cyber security insurance protection.

As cyber claims have risen, especially among large law firms, cyber security insurance carriers have pulled back from the market to some degree and have instituted rate increases and tighter underwriting guidelines in an effort to recoup some of the losses endured through rising and more expensive cyber claims.

However, there are affordable options out there. WILMIC recommends cyber coverage of at least $100,000. Anything less than that, depending on the attack, may get eaten up quickly.

What is difficult about insuring against cyber risk?

According to many reports in the industry, the challenges the cyber insurance market are facing include:

- Rapid growth in exposure without adequate underwriting controls;

- The growing sophistication of cyber criminals that have exploited malware and cyber vulnerabilities faster than companies and law firms that may have been late in protecting themselves; and

- The far-reaching implications of the cascading effects of cyber risks and the lack of geographic or commercial boundaries.

Solution

WILMIC has partnered with HSB to offer policyholders comprehensive coverage and risk management services in a powerful product specifically designed for small to medium-sized businesses. HSB Cyber Suite offers:

- in-house cyber experts are available to assist with 24/7 claims support, risk management tools, and industry insights;
- comprehensive coverages that can be layered together to create a safety net tailored to the specific risks and operational needs of the insured;
    - data compromise response
    - computer attack
    - cyber extortion
    - misdirected payment fraud
    - computer fraud
    - identity recovery
- coverage limits that range from $50,000 to $1 million
- access to eRisk Hub:
    - training modules
    - eRisk resources
    - risk management tools
    - learning center
    - news center

XI. Tips for Obtaining and Maintaining Coverage

A. There are certain cybersecurity controls that are critical to obtaining coverage. Without these controls you will likely not obtain coverage, or the premium will be obscenely high.

- Multi-factor authentication
- Segmented, frequent, and encrypted backups
- Prompt implementation of security patches/updates
- Endpoint Detection and Response Tools

B. Overall, you need to have a strong cybersecurity program in place; for example, with the Written Information Security Plan and Incident Response Plan we discussed earlier, in addition to the other security measures that constitute good cyber-hygiene. The programs need to be in place and need to be operational. You also need to be knowledgeable about the program and security and IT in place when filling out the application.

C. You need to be thorough and truthful on your insurance application. A trend we are seeing lately is cyber insurance claims being denied based on a misrepresentation in the application—stating you had certain protections or policies in place when they were not or were not followed. In the past, you may have handed the questionnaire off to your IT department, maybe they were afraid to state that the company doesn't do X, Y, and Z, so fudges things a bit. Based on high ransoms, insurance companies are looking for ways out.

XII. Conclusion

The basic responsibilities that a lawyer owes the client – competence, diligence, communication, and confidentiality - lie at the core of lawyer's professional obligations and remain unchanged –even when working remotely. Keeping abreast of ethical obligations is imperative for lawyers discharging these responsibilities effectively in a world increasingly dominated by technology and, more recently, in an environment where lawyers are working in a virtual environment. Fortunately, the insurance industry is responding and providing protection with cyber liability policies like HSB/Bultman's Total Cyber package.

Lock It Down:
Cybersecurity Essentials for Small Law Practices

Kate H. Campbell
Tom Watson

October 16, 2025

1

Today's Agenda

- The Current Threat Landscape
- Legal Obligations Post-Breach
- Ethical Obligations for Lawyers
- Best Practices and Practical Pointers
- Cyberinsurance

2

The Current Threat Landscape

3

Why Should Lawyers Care?

- Law firms are attractive targets
- Significant exposure and exponential losses
- Volumes of sensitive information
- Ethical and legal obligations

4

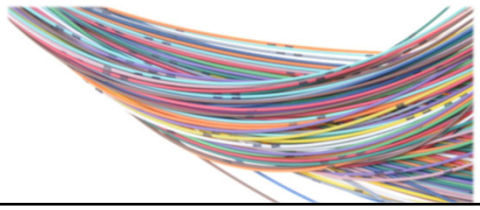
Law Firms are Vulnerable

Attack Vectors

- Physical Security
- Phishing
- Social Engineering
- Vendor Compromise

Attack Types

- Ransomware
- Email Compromise
- Wire Fraud
- Rogue employees



5

Ransomware

- Malicious software
- Locks down a system and files making them inaccessible unless a ransom payment is made
- Can be accomplished through security vulnerabilities or phishing schemes

6

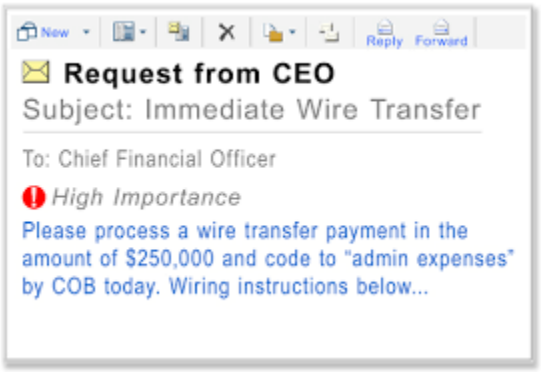
Business Email Compromise

- Threat actor breaks into your email account
- Has access to entire inbox, can create rules to direct emails to folders so you have no idea
- Can send emails through your account without your knowledge
- Can be accomplished through security vulnerabilities or phishing schemes

7

Wire Fraud

- Fraudulent wire instructions are communicated to parties through a business email compromise or phishing scheme
- A party unknowingly sends money to a threat actor



8

Evolving Threat Landscape

- Law firms are especially susceptible to double and triple extortion models
- Emerging trends show law firms as top targets

9

Key Statistics (2016-2020)

- Average Incident Cost for Professional Services Companies: $211,000
- Most Frequent Claims (SMEs)
  1. Ransomware (~1500, $179,000 avg)
  2. Hacker (~450, $430,000 avg)
  3. BEC (~400, $123,000 avg)
  4. Phishing (~275, $13,000 avg)
  5. Human Error (~250, $72,000 avg)

- Source: 2021 NetDiligence Cyber Claims Report

10

Legal Obligations for Lawyers

11

Breach Notification Laws

- Each state has its own data breach notification laws
- The definition of personal information may vary across states
- Each state will have its own standard for when notification is required
  - Unauthorized access to personal information
  - Unauthorized access to personal information PLUS risk of harm
- Timing and the necessity to also notify the state's Attorney General varies across state laws

12

Wisconsin's Data Breach Notification Law—Wis. Stat. § 134.98

- Personal Information means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:
  - The individual's social security number.
  - The individual's driver's license number or state identification number.
  - The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.
  - The individual's DNA profile.
  - The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

13

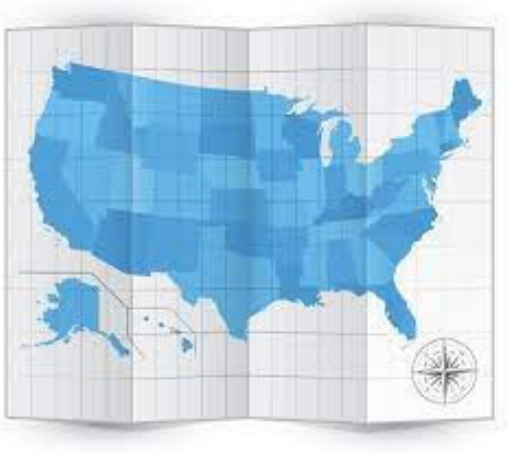
Wisconsin's Data Breach Notification Law—Wis. Stat. § 134.98

- Notice is not required if "the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information."
- Notice to be provided within a reasonable time, not to exceed 45 days after learning of the incident.
- The Wisconsin Attorney General is not required to be notified.

14

Breach Notification Laws

- You will need to do an analysis of every state's law in which an affected individual resides



15

Other Required Notifications Common for Lawyers

HIPAA IF YOUR FIRM ACTS AS A BUSINESS ASSOCIATE

OUTSIDE COUNSEL GUIDELINES

16

Ethical Obligations for Lawyers

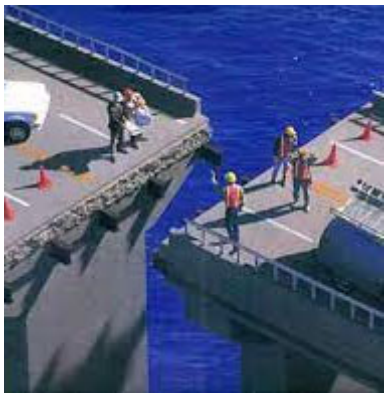
17

Ethical Rules

- SCR 20:1.1 Competence
  - Edits to Model Rules in 2012 – Rule 1.1 – Obligation to "keep abreast of knowledge of the benefits and risks associated with relevant technology"
- SCR 20:1.6 Confidentiality
  - Edits to Model Rules in 2012 – Rule 1.6 – "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."
- SCR 20:5.1 Responsibilities of Partners, Manager, and Supervisory Lawyers

18

SCR 20:1.1 Competence



19

ABA Guidance

- ABA Formal Opinion 477R (Securing Communications)
- ABA Formal Opinion 483 (Lawyer Obligations After a Cyber Breach or Attack)
- Wisconsin Formal Ethics Opinion EF-21-02 (Working Remotely)

20

ABA Formal Opinion 477R

- Lawyers have a duty to do the following related to email communications based on Model Rule 1.6(c) [which has not been adopted by Wisconsin]
  - Understand the Nature of the Threat
  - Understand How Client Confidential Information is Transmitted and Where It is Stored
  - Understand and Use Reasonable Electronic Security Measures
  - Determine How Electronic Communications About Client Matters Should be Protected
  - Train Lawyers and Non-lawyer Assistants in Technology and Information Security
  - Conduct Due Diligence on Vendors

21

ABA Formal Opinion 483

- Lawyers have a duty to notify current clients of a data breach under Model Rule 1.4 "in sufficient detail to keep clients 'reasonably informed' and with an explanation 'to the extent necessary to permit the client to make informed decisions regarding the representation.'"
- While notice is not required under the opinion to former clients, "lawyers should recognize… data privacy laws, common law duties of care, or contractual arrangements with the former client relating to records retention, may mandate notice to former clients[.]"

22

ABA Formal Opinion 483

- "The opinion underscores the importance for lawyers to both plan beforehand for an electronic breach or cyberattack and to understand how model rules come into play when an incident is either detected or suspected."

  —ABA Issues New Guidance on Lawyer Obligations After a Cyber Breach or Attack, ABA (Oct. 17, 2018), *available at* https://www.americanbar.org/news/abanews/aba-news-archives/2018/10/aba-issues-new-guidance-on-lawyer-obligations-after-a-cyber-brea/.

23

Wisconsin Formal Ethics Opinion EF-21-02

- "Basic technological competence includes, at a minimum, knowledge of the types of devices available for communication, software options for communication, preparation, transmission and storage of documents and other information, and the means to keep the devices and the information they transmit and store secure and private."

- Lacking the knowledge to manage the technological aspects of the practice is not an excuse for failing to maintain technological competence.

24

Best Practices and Practical Pointers

25

Best Practices Pre-Breach

- Be Prepared!
  - Written Information Security Plan (WISP)
  - Incident Response Plan
    - Tabletop Exercises
  - Engage data security and privacy counsel

26

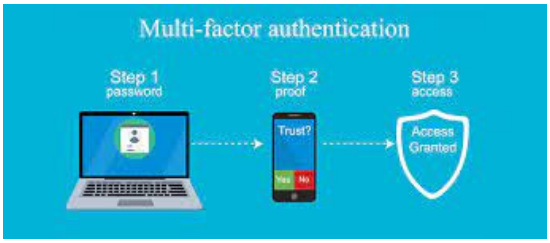
Best Practices Pre-Breach

- Data Minimization
  - If you don't need it, don't collect it
- Limit Access
  - Only those with a need to know should have access
- Emphasize Awareness
  - Employee Training

27

Best Practices Pre-Breach

- Use technological measures to reduce the attack surface and mitigate common risks
  - Multi-factor authentication
  - Encryption
  - Password managers like LastPass or strong passwords that vary across accounts
  - Email security
  - Endpoint Detection and Response



28

Best Practices Pre-Breach

- Conduct vendor due diligence and use strong data security contractual provisions
  - Understand the measures a vendor uses to secure and keep private sensitive information
  - It is not sufficient to conduct due diligence at the outset, and never thereafter
  - Contractual provisions relating to reasonable security measures, data breach notification, reimbursement for notification expenses, and audit rights

29

Best Practices Post-Breach

Follow	Follow Incident Response Plan
Take	Take Action to Mitigate Harm if Possible
Contact	Contact Insurer
Contact	Contact Counsel
Consider	Consider Attorney Client Protections when Working with Forensic Provider

30

Cyberinsurance

31

Cyberinsurance Tips

- Certain cybersecurity controls are critical to obtaining coverage:
  - Multi-factor authentication
  - Segmented, frequent, and encrypted backups
  - Prompt implementation of security patches/updates
  - Endpoint Detection and Response Tools
- Have a strong cybersecurity program in place and be knowledgeable about the security in place.
- Be thorough and truthful on your insurance application.

32