STATE BAR OF WISCONSIN
PINNACLE
Your Practice. Our Purpose.

WSSFC 2026

Technology Track – Session 6

Cybersecurity: 10 Practical Steps Every Law Firm Can Take Today

Presented By:

Brent J. Hoeft
State Bar of Wisconsin, Madison

About the Presenter...

Brent J. Hoeft is the Practice Management Advisor for the State Bar of Wisconsin's Practice411™ Practice Management Program. He guides State Bar members on increasing law practice productivity and efficiency and advises on all things law practice management, including legal technology, information security practices, technology competence, employee management, policy and systems implementation, business development and marketing, and improving client relationship management. Prior to his time at the State Bar of Wisconsin, Brent was in private practice since 2006. In 2010, he founded Hoeft Law LLC, Wisconsin's first completely web-based virtual law firm providing legal services in business law, cybersecurity, and estate planning. Brent was also the founder of FirmLock Consulting, LLC, a cybersecurity behavior awareness consulting firm focusing on assisting solo and small law firms with cybersecurity training, education, and implementation of policies and procedures to better protect law firm data. Brent is a frequent presenter on legal technology, practice management, and cybersecurity. Since 2018, he has served as co-chair of the Technology Track for the Wisconsin Solo and Small Firm Conference (WSSFC) Planning Committee and had the honor of serving as the Conference Chair in 2022. Brent received his B.A. in Psychology from the University of Wisconsin-Eau Claire and his law degree from Cleveland State University College of Law. He lives in the Madison area with his family, where he enjoys mountain biking, camping, photography, and all things Wisconsin sports.

CYBERSECURITY

10 Practical Steps Every Law Firm Can Take Today

Presented by:

Brent J. Hoeft
Practice Management Advisor
State Bar of Wisconsin

The Guiding Standard

Goal: Not perfect security, but reasonable and repeatable safeguards that make a firm more difficult to attack and better able to recover. Creating a culture of security within the firm.

Why Law Firms Are Targets

Law firms retain financial records, personal information, litigation strategy, business records, and credentials for court, banking, and government systems. They may be viewed as "soft targets" because they hold valuable information but are not primarily in the business of securing information.

Attackers may seek data that can be sold, exploited, or used to access other systems.

In a ransomware attack, information need only be valuable to the firm that depends upon it. In this scenario the hackers know that the information has value to the firm and they will want it back.

A cybersecurity incident can interrupt operations, create substantial recovery expense, trigger legal obligations, impair client trust, and ultimately threaten the viability of the firm.

Wisconsin Ethical and Legal Framework

SCR 20:1.1 and Comment 8: Competence includes maintaining the knowledge and skill necessary for representation, including awareness of **the benefits and risks associated with relevant technology.**

SCR 20:1.6: Lawyers must make reasonable efforts to prevent unauthorized access to or disclosure of information relating to a representation and take reasonable precautions when transmitting that information.

SCR 20:5.1 and SCR 20:5.3: Partners, managers, and supervisory lawyers must provide reasonable assurance that lawyers and nonlawyers act consistently with professional obligations.

SCR 20:1.4: Appropriate client communication may include the technology and communication methods the firm will use.

Wisconsin Formal Ethics Opinion EF-15-01: Reasonable efforts must be commensurate with the risks and evaluated in light of the firm, client, information, technology, cost, and circumstances.

Wisconsin Formal Ethics Opinion EF-21-02: Written cybersecurity practices, training, supervision, and suitable remote-work procedures support the protection of client information.

Wisconsin's Data Breach Statute - Wis. Stat. § 134.98: Notice of unauthorized acquisition of personal information.

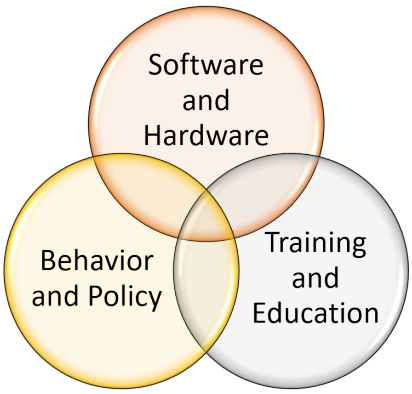
If an entity knows an unauthorized 3rd party has accessed Personal Information in its possession, the entity must take reasonable steps to notify those affected.

Personal Information = Last name, first name, middle name or initial in any combination and order + any other sensitive information. (SS#, Driver's license, Bank Account #, Biometric information, medical information)

Safe Harbor = If the information is already publicly available or if the data is in an unreadable format (encrypted, redacted etc.), then no notice required.

Why are people so important to the security of the law firm?

Cybersecurity Triad



You need all three parts of the cybersecurity triad to have the best chance against the hackers. "Software and Hardware" are the hard defense methods, and the "Behavior and Policy" along with the "Training and Education" are the soft defense methods. If you spend all your time, money and focus on the hard defenses the lack of focus on the soft defenses will make that investment meaningless. Think of purchasing and installing a state-of-the-art home security system but every day when you leave the house you leave all of the doors unlocked and never arm the system.

Remember, the bad actors only need to be right once; we have to be right every single time.

What steps can be taken to improve law firm security?

STEP 1 | Build a Security-First Culture

Cybersecurity begins with people. Every person in the firm should understand that security protects client confidentiality, preserves trust, supports ethical compliance, and helps keep the firm operating.

Core practices

- Discuss security routinely at staff and firm meetings.
- Explain why security matters to clients, the firm, and each person's work.
- Identify the person to whom suspicious activity and mistakes must be reported.
- Encourage prompt reporting without punishment for an honest mistake.
- Give lawyers and staff permission to pause and independently verify unusual requests.

- Apply a simple decision rule: slow down, scrutinize, and decide before acting.

Immediate action: Add a five-minute security item to the next staff meeting and name the firm's reporting contact.

STEP 2 | Turn On Multifactor Authentication

Multifactor authentication, sometimes called two-factor authentication, requires more than a password. It generally combines something the user knows with something the user has, such as an authenticator code or physical security key.

Priority accounts

- Firm email and Microsoft 365 or Google Workspace
- Practice-management and document-management systems
- Cloud storage
- Banking, trust accounting, and payroll
- Remote-access tools
- Password manager
- Court and government accounts
- Website and social-media administration

Authentication options

- Text or email code
- Authenticator application (popular examples)
  - Microsoft Authenticator
  - Google Authenticator
  - Authy
- Physical hardware key
  - Yubikey

Immediate action: Enable MFA first on firm email and the password manager, then work through other high-value accounts.

STEP 3 | Use a Password Manager and Stop Reusing Passwords

A password manager helps generate and securely store long, unique passwords. Password reuse is dangerous because credentials exposed in one breach may be tested against many unrelated services, a practice commonly called credential stuffing.

Implementation checklist

- Select a reputable password manager suitable for the firm.
- Create a strong and unique master password.

- Enable MFA on the password-manager account.
- Replace reused passwords, beginning with email, financial, cloud-storage, and practice-management accounts.
- Do not share passwords through email, spreadsheets, sticky notes, or unsecured documents.
- Establish a recovery procedure that preserves appropriate security controls.

A password manager can also provide a useful warning about a spoofed login page. If the website address does not match the legitimate page saved with the credentials, the manager may not offer to autofill the username and password.

Password Managers (popular examples)

- Bitwarden
- 1Password
- NordPass

Red flag: If the password manager unexpectedly refuses to autofill a familiar account, stop and verify the website address. This acts as an added security step against spoofed or fake websites. If the password manager is not recognizing it as a known website to fill the login credentials it could be because the website is fake and is trying to obtain your credentials.

STEP 4 | Keep Software and Connected Devices Updated

Security updates frequently correct known vulnerabilities. Automatic updates should be enabled when appropriate, and devices should be restarted when necessary to complete installation.

Include the entire technology environment

- Operating systems and web browsers
- Office, PDF, and practice applications
- Antivirus and antimalware software
- Mobile phones and tablets
- Router and network-device firmware
- Printers, scanners, and multifunction devices
- Other internet-connected office equipment

Network basics

- Change default router usernames and passwords.
- Close unnecessary router ports.
- Avoid placing inadequately secured internet-connected devices on the primary firm network.
- Assign responsibility for confirming that updates are installed.

Immediate action: Turn on automatic updates and identify one person who is responsible for monitoring exceptions and failed installations.

STEP 5 | Train Everyone to Recognize Phishing and Social Engineering

Short, recurring reminders can be more effective than relying only on a single annual lecture. Training must include email, text messages, telephone calls, social media, file-sharing notices, and in-person interactions.

Common methods

- **Phishing:** Broad fraudulent email campaigns.
- **Spear phishing:** Messages targeted to a particular person.
- **Whaling:** Attacks aimed at executives or other high-value individuals.
- **Smishing:** Phishing through text messages.
- **Vishing:** Phishing by telephone.
- **Pretexting:** Using public information to create a believable story.
- **Partner or executive impersonation:** A supposed leader requests payment, credentials, or gift cards.
- **Baiting:** A gift, survey, prize, attachment, or USB drive prompts interaction.
- **Tailgating:** An unauthorized person follows an authorized person into a restricted location.

Warning signs

- Urgency, pressure, or secrecy
- Unexpected requests or login prompts
- Changed payment instructions
- Requests to bypass ordinary procedures
- Unfamiliar links or attachments
- Requests for passwords or authentication codes
- Messages inconsistent with the sender's usual practices

Generative AI can produce polished scam messages. Misspellings and poor grammar are no longer dependable warning signs. The better habit is to evaluate the context, follow established procedures, and independently verify unusual requests.

Firm rule: Do not sign in through a link in an unexpected email or text. Navigate independently to the known website or application.

STEP 6 | Create a Verification Rule for Money and Sensitive Information

Requests involving money, credentials, or confidential information should be verified through a separate, trusted channel. Do not reply to the questionable message or use contact information supplied in that message.

Require independent verification before

- Changing wiring or payment instructions
- Sending or redirecting funds
- Purchasing gift cards

- Disclosing passwords or authentication codes
- Releasing sensitive client information
- Changing a client's contact information
- Granting remote access
- Adding a new vendor or payment recipient

Voice cloning and video deepfakes

Very convincing audio deepfakes can be created with inexpensive software using only a minute worth of audio of the target's voice. Anyone who has there voice publicly available on social media, podcast, recorded videos uploaded to YouTube should be aware of this risk and proactively plan for the potential that a bad actor will use available voice audio for nefarious purposes. Some things to look for with audio deepfakes are:

- Unusual pacing
- Odd pauses
- Flat emotional tone
- Inconsistent pronunciation
- Missing background noise
- Robotic transitions between words

Currently, video deepfakes are a bit more easily detected especially with inexpensive and readily available AI tools. Some of the things to look for with video deepfakes are:

- Lip movements slightly out of sync
- Unnatural blinking
- Distorted teeth or ears
- Facial edges that shimmer
- Lighting inconsistencies
- Strange head movements
- Strange or inappropriate hand gestures

Voice cloning and deepfake precautions

- Limit unnecessary public information about key firm personnel.
- Require a multistep approval process for financial transactions.
- Use previously verified contact methods.
- Consider an internal passphrase for highly sensitive transactions.
- Treat video or audio as one point of evidence, not as automatic proof of identity.

Sample policy: No payment instruction, account change, credential request, or release of sensitive information may be completed solely on the basis of an email, text, phone call, or video meeting. Verify through a previously established method.

STEP 7 | Back Up Data and Test Restoration

Backups help protect against ransomware, hardware failure, accidental deletion, and physical disasters. A practical framework is the 3-2-1 method.

Element	Meaning
3	Maintain three copies of important information.
2	Store copies on two different forms of media or systems.
1	Keep at least one copy offsite, which may include appropriate cloud storage.

Four qualities of a useful backup

- Automatic: The process should not depend on someone remembering.
- Easy: Another authorized person should be able to understand and maintain it.
- Secure: Copies should be protected against unauthorized access and physical loss.
- Reliable**:** The firm must be able to restore information when needed.

Restoration checklist

- Identify what is backed up and where each copy is stored.
- Determine whether ransomware could reach every copy.
- Name the person responsible for monitoring backups.
- Schedule and document a test restoration at least once or twice each year.
- Confirm that the restored information is complete and usable.

Backup Software (popular examples):

- BackBlaze
- Acronis Cyber Protect
- Crashplan

Key principle: A backup that cannot be restored is not a functioning backup. Testing is a crucial step to assure that a backup is reliable.

STEP 8 | Encrypt Devices and Require Screen Locks

Portable devices can be lost or stolen. Encryption helps make stored information unreadable without the proper credentials or recovery key. Firms should confirm that encryption is active rather than assuming it is enabled.

Devices to address

- Desktop computers and laptops
- Smartphones and tablets
- Portable drives and backup devices
- Scanners, copiers, and multifunction devices that retain data

Baseline controls

- Full-device encryption, including BitLocker for Windows or FileVault for macOS where appropriate
- Password, PIN, or biometric access
- Automatic screen locking after a defined period of inactivity
- Remote-wipe capability where available
- Secure storage of encryption recovery keys
- A prohibition on storing client information on unauthorized devices

Immediate action: Verify encryption, automatic locking, and remote-wipe capability on every device used for firm work.

STEP 9 | Limit Access to What People Actually Need

Restricting access reduces the potential damage from a compromised account, accidental disclosure, or misuse. Apply the principle of least privilege: each person receives only the access needed for that person's work.

Review access to

- Client and matter files
- Accounting, trust accounting, and payroll
- Email administration
- Practice-management and document-management systems
- Website and social-media administration
- Cloud-storage sharing
- Remote-access tools
- Backup-system administration

Review access when

- A lawyer or employee joins the firm.
- A person changes roles or responsibilities.
- A lawyer, employee, contractor, or vendor leaves.
- A vendor no longer requires access.
- The firm conducts its scheduled quarterly access review.

Immediate action: Create a list of everyone with administrator privileges and remove unnecessary access.

STEP 10 | Write Down the Basics Before There Is a Crisis

A short written information security policy is better than an unwritten understanding. The policy should tell everyone what the firm expects, who is responsible, and what to do when something goes wrong.

Minimum contents of an information security policy

- **Security responsibility:** Policy owner, reporting contact, decision-making authority, and authority to approve exceptions.
- **Account security:** Password manager, MFA, account-sharing prohibition, and administrator-account rules.
- **Device security:** Encryption, screen locks, updates, remote work, personal devices, and portable media.
- **Client information:** Approved storage and sharing, secure portals, email attachments, retention, and destruction.
- **Access management:** Permissions, onboarding, role changes, contractors, vendors, and offboarding.
- **Training and reporting:** Frequency of training, reporting process, and expectation of immediate reporting.
- **Backups and recovery:** Systems and data covered, responsible person, monitoring, and restoration testing.
- **Incident response:** Immediate actions, preservation of evidence, decision-making, notifications, and outside contacts.

Additional policy subjects

- Confidentiality, integrity, and availability of information
- Data classification
- Disaster recovery and business continuity
- Electronic communication and secure document sharing
- Physical security
- File retention and destruction
- Remote workspaces and supervision
- Approved vendors and service-provider oversight

Incident-response contact list

- IT support
- Cyberinsurance carrier or broker
- Malpractice carrier
- Banking contacts
- Firm leadership
- Outside breach or privacy counsel, if designated
- Critical cloud and technology vendors

Key principle: A firm experiencing a breach or ransomware event will not have time to invent a process from scratch.

Start Small, but Start Now

Cybersecurity is not a set-it-and-forget-it project. It is an ongoing collection of habits supported by a culture in which people have permission to pause before clicking, sending, paying, or sharing.

Cybersecurity checklist of starting tasks

- ☐ Turn on MFA for the firm's accounts.
- ☐ Select and implement a password manager.
- ☐ Verify that automatic updates are enabled.
- ☐ Confirm that device encryption is active.
- ☐ Review who has administrator access.
- ☐ Schedule a backup restoration test.
- ☐ Create a payment-verification rule.
- ☐ Name the firm's security-reporting contact.
- ☐ Add cybersecurity to the next staff meeting.
- ☐ Begin a one-page information security policy.

Remember: Secure the accounts. Train the people. Protect the data. Prepare for the incident.

Reasonable-Efforts Risk Assessment

Wisconsin Formal Ethics Opinion EF-15-01 explains that reasonable efforts must be commensurate with the risks. Relevant considerations include:

- The sensitivity of the information.
- The client's instructions and circumstances.
- The potential effect of inadvertent disclosure or unauthorized interception.
- The lawyer's ability to assess the technology's level of security.
- The likelihood of disclosure without additional safeguards.
- The cost and difficulty of additional safeguards.
- The effect of safeguards on the lawyer's ability to represent the client.
- Accessibility needs and urgency.
- The provider's experience and reputation.
- The terms of the agreement with the provider.
- The legal and ethical environments where services will be performed.

Selected Authorities and Resources

- **Wisconsin Supreme Court Rules, Chapter 20**
  https://www.wicourts.gov/sc/rules/chap20a.pdf
- **Wisconsin Supreme Court Rules, Chapter 20, Part B**
  https://www.wicourts.gov/sc/rules/chap20b.pdf
- **Wisconsin Formal Ethics Opinion EF-15-01, Cloud Computing**
  https://www.wisbar.org/formembers/ethics/Ethics%20Opinions/EF-15-01%20Cloud%20Computing%20Amended.pdf
- **Wisconsin Formal Ethics Opinion EF-21-02, Working Remotely**
  https://www.wisbar.org/formembers/ethics/Ethics%20Opinions/EF-21-02%20Working%20Remotely.pdf
- **Wisconsin Statute § 134.98, Notice of Unauthorized Acquisition of Personal Information**
  https://docs.legis.wisconsin.gov/statutes/statutes/134/98
- **CISA Cybersecurity Resources and Tools**
  https://www.cisa.gov/resources-tools/all-resources-tools
- **CISA Cyber Incident Reporting**
  https://www.cisa.gov/report
- **NIST Small Business Cybersecurity Corner**
  https://www.nist.gov/itl/smallbusinesscyber
- **Federal Trade Commission, Protecting Personal Information**
  https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business
- **National Cybersecurity Alliance Resources**
  https://staysafeonline.org/resources/