`

STATE BAR OF WISCONSIN
PINNACLE
Your Practice. Our Purpose.

WSSFC 2024

Technology Track – Session 3

Cybersecurity for Solo and Small Firms: Updates and Best Practices

Presenter:
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 and privacy 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, 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 & privacy, and estate planning. Brent also founded FirmLock Consulting, LLC, a cybersecurity behavior 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 graduated from Cleveland State University College of Law (J.D., 2006) and University of Wisconsin-Eau Claire (B.A., Psychology, 2002). He lives in the Madison area with his family, where he enjoys mountain biking, camping, photography, and all things Wisconsin sports.

CYBERSECURITY FOR SOLO AND SMALL LAW FIRMS: UPDATES AND BEST PRACTICES

WISCONSIN SOLO AND SMALL FIRM CONFERENCE 2024

WISCONSIN DELLS, WI

PRESENTED BY:

Brent J. Hoeft, Practice Management Advisor
Practice411™ Practice Management Program
State Bar of Wisconsin

I. **Why Do Lawyers Need to Worry About Information Security?**

A. Rules of Professional Responsibility, Ethical Guidance, and Data Breach Statute

1. SCR 20:1.1; and Comment 8: Competency regarding technology used and available
    a) in "legal knowledge, skill, thoroughness and preparation *reasonably necessary* for the representation" (emphasis added)
    b) Comment 8 – including the *"benefits and risks associated with relevant technology"*
    c) 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. Larger firms will often employ expert staff to address these concerns. Smaller firms or sole practitioners may need to retain the services of an expert if they lack the knowledge to personally manage the technological aspects of practice. Wisconsin Formal Ethics Opinion EF-15-01
2. SCR 20:1.6: Confidentiality - Must make *reasonable efforts* to prevent disclosure of client information to 3rd parties without client's consent.
    a) Wisconsin Formal Ethics Opinion EF-15-01 provides guidance on "reasonable efforts" regarding technology:
        (1) "To be reasonable, those efforts must be commensurate with the risks presented. Because technologies differ and change rapidly, the risks associated with those technologies will vary. Moreover, because the circumstances of each law practice vary considerably, the risks associated with those law practices will also vary. Consequently, what may be reasonable efforts commensurate with the risks for one practice may not be for another. And even within a practice, what may be reasonable efforts for most clients may not be for a particular client."
        (2) Factors to consider:
            (a) the information's sensitivity;
            (b) the client's instructions and circumstances;
            (c) the possible effect that inadvertent disclosure or unauthorized interception could pose to a client or third party;
            (d) the attorney's ability to assess the technology's level of security;

(e) the likelihood of disclosure if additional safeguards are not employed;
(f) the cost of employing additional safeguards;
(g) the difficulty of implementing the safeguards;
(h) the extent to which the safeguards adversely affect the lawyer's ability to represent clients;
(i) the need for increased accessibility and the urgency of the situation;
(j) the experience and reputation of the service provider;
(k) the terms of the agreement with the service provider; and
(l) the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.

(3) Note: While this list is not exclusive, it provides a good basis for assessing risk.

b) See ABA Comment [18] and [19] to SCR 20:1.6

(1) 20:1.6(d) When the lawyer is transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.

(2) The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. This duty of reasonable precautions, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy.

(3) Special circumstances, however, may warrant special precautions. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this rule.

3. SCR 20:5.1 and 5.3 Supervision

a) Addresses the duties that law firm partners, managers and supervisory lawyers have to provide reasonable assurance that all

lawyers in the firm conform to the Rules. Similarly, SCR 20:5.3 addresses the duties that partners, managers and supervisory lawyers have to provide reasonable assurance that the conduct of each nonlawyer, including consultants and vendors, is compatible with the Rules.

b) Wisconsin Formal Ethics Opinion EF-21-02 provides guidance on training and supervision
    (1) Establish and implement policies and procedures for cybersecurity practices.
        (a) These policies and procedures should be in writing and provided to all lawyers and nonlawyer assistants. Compliance should be stressed.
            (i) Everyone in the firm needs to understand the "why."
    (2) Establish and implement policies and procedures for the training and supervision of lawyers and nonlawyer assistants in the firm's cybersecurity practices.
        (a) Training is the most basic step in avoiding a cyberattack at a law firm. In other words, it is extremely important to develop a culture of awareness. The most serious vulnerabilities of a cybersecurity system are not the hardware or software, but rather the people who use it. Currently, it is estimated that 75% of cybersecurity breaches are due to human error. (Verizon 2023 Data Breach Investigations Report)
        (b) Make sure everyone in the law firm understands the risks involved with phishing and ransomware.
            (i) Includes training on best practices when interacting with email and other communications.
    (3) Establish and implement policies and procedures regarding remote workspaces to mitigate the risk of inadvertent or unauthorized disclosures of information relating to the representation of clients.
        (a) Remote workspaces should be private to ensure that others do not have access to phone conversations, video conferences, or case-related materials.
    (4) Hold sufficiently frequent meetings (including remote meetings) between supervising attorneys and supervised attorneys, and between supervising attorneys and

supervised nonlawyer assistants to achieve effective supervision.

4. SCR 20:1.4 Communication – The duty of communication to a client may extend to informing the client about the technology used by the law firm and the extent the client agrees to communicate via certain methods.
5. WI Stat §134.98 Wisconsin "Data Breach Notification" and Safe Harbor Rules
    a) If sensitive information was taken, then business may have to comply with this statute.
    b) This statute applies to breaches of businesses (law firms are a business that must comply with the statute).
    c) Says if unauthorized 3rd party access to Personal Information (defined below) occurs the business must take reasonable steps to notify those affected.
        (1) Personal Information = Last name, first name, middle name or initial in any combination and order along with any other sensitive information.
            (a) SS#, Driver's license, Bank Account #, Biometric information, medical information
        (2) 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.

B. Potential effects of a breach on law firm
    1. Extremely high financial cost of a breach
        a) The average cost of a data breach was $4.45 million in 2023, the highest average on record. In US, average was much higher at $9.48 million (IBM)
    2. Law firm will experience significant downtime as the result of a breach, even in the best case scenario.
    3. Malpractice and law violations: Not only is there loss of business and expense due to the breach itself, but also malpractice with potential for discipline, and notice requirements under data breach statute. Security breaches and unauthorized 3rd parties obtaining confidential client files is extremely bad for law firms. These occurrences could potentially put an end to the law firm if client and community trust in the law firm cannot be restored.

C. Law Firms are Targets.
    1. Soft Targets – Law firms have lots of sensitive information that is important to the firm and not enough attention paid to the security of that information.

a) Whether the information is valuable to anyone else doesn't matter. In the case of ransomware, all that matters to the hacker is that the information is valuable to the target so that they are willing to pay the ransom to the hacker to get the information back.

2. Humans are the "low hanging fruit"
    a) 75% of security incidents investigated had human error as a contributing factor. – Verizon Report 2023
    b) Technological security safeguards have improved, requiring a greater technological sophistication for a hacker to breach that security. Therefore, it is easier to manipulate the humans than it is to breach the network. Humans are the low hanging fruit in the security tree.
    c) The end-user's behavior affects security.
    d) Hackers don't just hack computer systems they hack people.
    e) Hackers who use social engineering are really just con artists.
    f) In order to compromise security, the hackers prey on the employee's trust, desire to help, and desire not to avoid making waves in the office or with clients.

D. Creating a Security-First Culture in the law firm.
    1. Start with *Why*: Making sure your employees understand why this matters beyond "we have to," is an important foundation to build upon a culture of security in your law firm.
        a) Convey the "why": "A lot of time, money, and effort has been put into creating a good name for the firm in the community. The reputation of the firm is one of the most valuable assets a law firm can have. The people in the firm are a crucial part of the security plan. A data breach that reveals sensitive information of firm clients is going to have a huge impact on the level of trust clients and the community have in the law firm. Without trust, the law firm will not be able to keep clients or obtain new clients. Without clients, there is no law firm. Without the law firm, we are now out of a job."

E. To summarize, cybersecurity and technology competence matters because:
    1. It is required by the rules of professional conduct;
    2. Cyber threats are a real concern to law firms and companies of all sizes;
    3. Law firms are soft targets and one of the most targeted industries;
    4. Hackers see humans as the weak link in security and therefore go after them first; and
    5. It is important for employees to understand and be trained that human behavior affects security and that a data breach can have dire

consequences for a law firm. Understanding these things will help to promote a culture of security within a law firm.

II. **Threats to Information Security**

A. Social Engineering

1. Security threats by phone, email, text, and in-person, where hackers attempt to get the target to perform some action that the hacker wants.
2. Threats
    a) "Straight Cons"
        (1) These are often the kinds of cons that existed even before computers and the internet. Premise is the same, but the tolls have evolved with new technologies. Hackers in these situations act more like con-artists than what is thought of as a stereotypical hacker breaching a system.
        (2) Pretexting – using publicly available information to build a sense of trust.
            (a) Researching a company than posing as IT or other 3rd party offering help
            (b) CEO Fraud – Impersonating a high-level executive and requesting another employee carry out an act of some kind. For example, the Amazon gift card or Apple Gift Card scam where the fake CEO, by email or phone call, requests the employee to buy gift cards with the company credit card and then email the fake CEO with the gift card identification codes.
            (c) Out-of-office reply exploits
                (i) Providing too much information in an out-of-office message allowing hackers to use the information in a social engineering attack.
        (3) Baiting – An offer of some tangible gift, prize or windfall in exchange for information.
            (a) Fake Surveys – answer questions and win a free gift
        (4) USB drive drops
            (a) Dropping USB drives in parking lots or common areas with malicious code installed. Goal is that someone will find and insert the drive into a network computer in an attempt to find who the

drive belongs to. Doing so will initialize malware to install on the computer and infiltrate the network.

(5) Quid Pro Quo – Similar to baiting but offer services instead of tangible item
    (a) Cold-calling offering to fix a slow running PC to get the target to give the hacker remote access.
(6) Tailgating – in-person attack, unauthorized person follows authorized person into a secure location.
    (a) Fake delivery person waiting for employee with access to hold door on the way into the building.

b) Phishing - Security threats through email, text, phone, and social networks
    (1) Phishing was the leading infection vector, identified in 41% of incidents, making it the most common initial attack vector. (IBM)
    (2) Types of phishing
        (a) Phishing - general, mass email campaign without being directed at a specific target end-user
        (b) Spear phishing and whaling
            (i) Spear phishing is a targeted phishing campaign directed at a specific person. Whaling starts with social engineering to determine who is the top person to go after and who their contacts are Goal is to determine from whom to send a targeted phishing email so the target will fall for the attack.
        (c) Vishing
            (i) Phishing by phone.
            (ii) People tend to trust a phone call more than an email.
            (iii) Often a spoofed call from a bank or credit card company informing them of suspicious activity and provides a number to call which is a fake number.
            (iv) Request account information or PIN.
            (v) Beware - Some banks will not honor request to refund the money as you voluntarily gave your information. The bank's position is that

the fault lies with you for not protecting your information.

(d) Smishing
    (i) Phishing by text messaging, otherwise known as SMS (SMS + phishing)
    (ii) Often the same kind of notice from a bank or credit card stating that there is some unusual activity and to call a number if this activity seems unusual.

(3) Threats from Phishing
    (a) User login information compromise in order to obtain access to and takeover of user accounts.
        (i) Obtaining target's username and password through use of a faked website login.
        (ii) Login page looks familiar, so target enters login credentials which then are sent directly to the hacker.
        (iii) Hacker then uses the information to login and change the password on the account thereby locking the target out of their own account.
    (b) Malware - Clicking on a link or attachment in an email, text, or social media post downloads and runs malicious software in the background, unknown to the target.
    (c) Keyloggers – Software that is downloaded in the background after a bad link or attachment is clicked. Software sits in the background recording keystrokes and sending the information out to the hacker's database where it is analyzed for sensitive information that would be valuable to the hackers.
    (d) Botnets – software that adds your computer to a collection of compromised computers that are then collectively used to unleash a Distributed Denial of Service (DDOS) attack, credential stuffing, or used to send very large quantities of spam.
    (e) Ransomware
        (i) Usually delivered via phishing.
        (ii) Clicking on a link or attachment launches software that encrypts the system files and

requests payment (usually in Bitcoin) in exchange for the key to unlock the files.

(iii) This is the major threat to law firms right now and will therefore be explored in greater detail below.

c) Ransomware

(1) This is a type of malware delivered almost always through email in which clicking a link in the email deploys a program that then encrypts your entire system or network so that all files are inaccessible without the decryption key.

(2) The average ransom payout has increased dramatically from $812,380 in 2022 to $1,542,333 in 2023. (SC Magazine)

(3) Ransomware is cheap and low risk for hackers.

(a) Rise of affordable ransomware software-as-a-service on the dark web.

(b) Allows non-technical hackers access to more sophisticated software without requiring any actual knowledge.

(c) Low risk with a potentially big reward

(i) Easy to stay anonymous and with Bitcoin used as payment of the ransom the money is very difficult to track down.

(ii) Focusing on many small ransoms makes finding them ever more difficult.

(d) Volume based - send out many phishing emails so that even if only a small percentage of emails actually deploy the ransomware a lot of money can still be made.

(i) Many firms often say “They won’t target us. We are too small and don’t have any major clients with information anyone would want.”

(ii) The hackers do not choose their targets in that manner. Anyone can be a target because hackers execute mass email campaigns so even if there is a low success rate and a low ransom ask the campaign is still lucrative.

(iii) The value of information that is being sought by the hacker is the value to the

target. Since this is a ransom scheme the information must be valuable to the target so the target will be willing to pay to get it back.

(4) Encrypt-and-extort

(a) More recently hackers have been utilizing a new approach to exfiltrate the target's data before encrypting. The hacker then threatens to publicly post the stolen data if the target does not pay.

(b) Double extortion - hackers are going after 2 ways to get paid (1) to decrypt and unlock all the files and (2) to not publicly post stolen data.

(c) Triple Extortion – same as double extortion but the hackers also go after the clients, patients, customers, or anyone else that might be interested in making sure that the data the hackers obtained doesn't go public.

d) Generative AI (GAI) and Social Engineering

(1) Phishing and Smishing – The emails and text messages used in these types of campaigns are greatly improving by using GAI.

(a) The common recommendations to look in the text of the email for inconsistent wording, grammar mistakes, typos, or strange tone, no longer applies.

(b) Which means humans and defense software needs to be better at using other characteristics to identify a phishing email.

(2) AI Generated audio and Deepfakes scams

(a) AI generated audio scams take the voice of a specific person and use it to scam (through blackmail, extortion, ransom) a targeted victim into paying the attacker.

(b) Deepfakes use actual video and audio of a person to create Ai generated video of that person saying and doing something that they never actually did.

(i) Actual case of finance employee sending $25 million to an attacker after that employee had a video conference with who he thought was several members of his company including the CFO. However, they

were all deepfake created using GAI. https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

(c) Only requires a couple minutes of the person's voice to generate an AI generated model of that person which then can be made to say anything

(d) The quality of this technology is improving and the cost of using it is dropping, which has resulted in an increase of these scams.

B. Man-in-the-Middle Attacks
   1. Hackers get access to your email or network and are able to see all traffic on your computer, across your network, and/or through the internet.
   2. Access can be gained out of use of unsecured WIFI, or by unknowingly downloading a program via a link or attachment through email or text messaging, or through business email compromise (BEC).

C. Brute force attack
   1. A bot network is used to target a specific website and try to crack the password using software that quickly and systematically tries to guess the password to the account.

D. Credential Stuffing
   1. A type of brute force attack only rather than trying to randomly guess the password, hackers are using credentials that are already available on the internet usually due to a prior security breach.
   2. Hacker is hoping that they find a target that has reused the same username and password from the hacked credentials on another account so that the hacker could then gain access.

III. Tools and Methods to Protect against Threats

A. Networks, Computer Security, and Backups
   1. Install a firewall.
   2. Use anti-virus software.
   3. Do not use any Internet of Things (IoT) Devices in the office. These connected devices are often designed with little to no security and can be an easy way into the network. Any IoT devices should be connected to a separate network from the main network.
   4. Close any unnecessary open ports in routers.
   5. Get Intrusion Detection and Prevention Systems for your network in order to monitor and prevent penetration attempts.

6. Routinely install network-wide patches (software updates) as they become available.
7. Limit user authorization and access to programs and files to only those with a bonafide business interest to access them.
8. Institute limitations on how long files are stored. Saving confidential information longer than necessary only makes it more at risk for loss.
9. Backups – Recent, reliable, redundant backups
    a) Goal = Automatic, easy, secure and reliable
        (1) Automatic
            (a) In order to become a habit or routine the backup process must be made automatic or as close to an automatic process as possible.
        (2) Easy
            (a) If the process is automatic but is too difficult to replicate by someone less familiar with the process you run the risk of not having backup continuity in the event of the unavailability of the individual who initially setup the backup process.
        (3) Secure
            (a) Backups must be securely stored to prevent loss from fire, water, tornado, theft of physical hardware, and ransomware.
            (b) The data must also be secured.
                (i) Authorization to access the backup data must be limited and controlled.
                (ii) Data must be encrypted at the storage level as well as in transit to prevent unauthorized access.
        (4) Reliable
            (a) The backups must be reliable in that they need to actually be able to provide for recovery and restoration.
            (b) If the backup does not work than there is no point to backing up.
            (c) Be sure to test the backup to make sure that it is reliable.
    b) Be Redundant. Be Redundant.
        (1) Redundancy is the key to reliability and security.
            (a) The more redundancies built into the backup process the greater the likelihood a reliable backup is available when you need it. Also, reduces the risk of data loss from hardware failure.
        (2) 3-2-1 Backup theory

(a) 3 – Three backups of any important file at any given time ensures that data will not be lost
(b) 2 – Two backups exist on at least 2 different forms of backup device. For example, an internal drive plus an external disk, network drive, or cloud backup copy.
(c) 1 – At least one backup offsite which protects against physical loss by theft, fire water, tornado, or ransomware.

10. Encryption
    a) All computers, drives, and mobile devices should be encrypted.
    b) Computers – Both Windows and Apple have encryption built-in but need to make sure it is on
        (1) Windows – BitLocker
            (a) Control Panel > System and Security > BitLocker Drive Encryption > "Turn on BitLocker
        (2) Apple – Mac OS – FileVault
            (a) Security and Privacy>FileVault> "Turn on FileVault"
    c) Mobile Devices
        (1) Encryption available on iPhones and devices running Android.
        (2) iPhone – Turn on Data Protection
            (a) Settings>Face ID & Passcode
            (b) Enter your passcode
            (c) Scroll down to bottom of page and make sure that Data Protection is enabled.
        (3) iPhone alternative available for iOS 17.3 "Stolen Device Protection"
            (a) Settings> Face ID & Passcode
            (b) Scroll down to "Stolen Device Protection" and toggle on the switch to enable.
        (4) Android
            (a) Reasonably new devices released in the last few years will have encryption enabled if you have enabled lockscreen protection via password, pin or pattern.
            (b) To enable a lockscreen go to Settings> Lockscreen and Security
                (i) Then pick how you would like to secure your lockscreen.

B. Passwords and Access

1. Password Best Practices
    a) Strong passwords are extremely important for strong security.
    b) A strong password has the following characteristics:
        (1) At least 12 characters long;
        (2) Utilizes uppercase letters, lowercase letters, numbers, and symbols;
        (3) Should not be easily guessed, so stay away from common words and phrases;
        (4) Never reuse. The password should be used for only one account;
        (5) Passwords should be changed frequently; and
        (6) Passwords should not be kept on a piece of paper or in a place where it can be easily found by unauthorized persons or misplaced by the account owner.
    c) For additional Do's and Don'ts for passwords see Brian Krebs - KrebsOnSecurity blog.
2. Password Managers:
    a) With the number of websites that most people use in their everyday life the only way to meet these standards is to incorporate the use of password manager and password generation software.
    b) This software is designed to securely store all your passwords, autofill the passwords when you need them, and generate new complex and randomized passwords.
    c) You only have to remember your master password to the password manager software, so the password can be longer and more complex.
    d) Examples of some available password managers:
        (1) 1Password - Cloud-based, cross-platform; free version limited to 30 days; business version available for sharing and permissions for employees.
        (2) Bitwarden – Cloud-based, cross-platform; free version available.
        (3) Dashlane - Cloud-based, cross-platform; free version for use on 1 device (Windows or Mac); has a business version for sharing and permissions across employees.
        (4) KeePass - open-source; stored locally; can be synced with other devices; but less user-friendly than the others; a good option if you're tech-savvy and don't want to store your info in the cloud.
        (5) Roboform - offers online or stored locally; oldest password manager out there as it's been around since 1999; has free and business versions
    e) No matter which one you choose, make sure your master password is strong and complicated and turn on Multifactor Authentication (MFA), also known as 2-factor Authentication (2FA), for your password manager account.

3. VPN - Virtual Private Network
    a) Think of a VPN as creating a virtual secure tunnel between your computer, the VPN webserver, and your ultimate destination web address.
    b) Popular examples are: NordVPN, Proton VPN, Surfshark VPN.
    c) Features such as speed, number and location of servers, privacy features, bandwidth during peak hours, vary greatly across VPN providers and should be researched to make sure the service meets your needs.
    d) The benefits of a VPN include privacy and security.
        (1) Privacy - Using a VPN will hide your identity and your IP address while you are on the internet.
        (2) Security – Using a VPN prevents against "man-in-the-middle" attacks where a hacker can intercept your information as it is in transit from your computer to your destination.
    e) A drawback of a VPN is that it can slow down the speed of your connection if you are using it at high traffic times. However, for the more reputable VPNs any slowdowns are negligible. Also, you need to be able to trust the VPN provider is not logging and monitoring your data and activity passing through the VPN.
    f) For these reasons alone, stick with the more popular VPNs and definitely skip any free offerings.
4. Multifactor Authentication (MFA) (also known as 2-Factor Authentication (2FA))
    a) MFA is an important extra layer of security for your online accounts.
    b) Setup MFA for all online accounts that have this option.
    c) When MFA is enabled for your online account, you will need your account username as well as 2 different authentication forms.
        (1) The first is something you know; this is your account password.
        (2) The second authentication required is something that you have; this is your MFA key or code.
    d) This MFA code generally can be generated in 3 different ways (in order from good to best).
        (1) Text or email - The first is by text or email sent to your email address or mobile phone number on record with your account provider.
        (2) Generator Application - The second method is through an authentication code generator app on your smartphone.
            (a) Google Authenticator, Microsoft Authenticator, Authy, Duo Authenticator
        (3) Physical key - The third way is by connecting a physical device key to the computer that once detected will provide the authentication.

(a) Two examples of such devices are:
(i) Yubikey
(ii) Titan Security Keys by Google

e) The idea is that even if your password is compromised your account would remain secure without the MFA key (the 2nd factor for authentication).
f) Of the 3 options, the physical key device provides the greatest amount of security for your account.

5. User authorization and access rules
a) Control who has access to sensitive information by setting user access rules for your network and data.
b) Limit the number of people with access to sensitive information to only those absolutely necessary.

C. Training - Information security behavior training of all law firm employees (at least annually)
1. Phishing and Ransomware Education – Create a "Human Firewall"
a) Behavior when interacting with email, texts, social media:
(1) Be on the lookout for
(a) Urgency: Often will try to scare you into acting.
(b) Fake Links: Altered links to attempt to trick you. To see exactly where a link will take you, simply hover over it. If in doubt, DON'T CLICK IT. Instead, go directly to the source by manually entering (typing, not cut and paste) the website address of the site you want to visit.
(c) Attachments and links: Be cautious with any attachments and links and DO NOT click. Often things like invoices or delivery receipts from parcel delivery services are used to entice the end-user to interact with the communication.
(2) DO NOT login to your account from a link inside of any email or text message sent to you. Go directly to the account website by typing it into your web browser.
(3) Spoofed Sender: Often the hacker will try to impersonate someone that you trust to get you to open the email and click the link.
(4) Be cautious. Independently confirm the email with the sender. Look carefully at the email address it is purporting to be from. Does it look legit?
(a) Implement a policy to get employees to slow down, scrutinize, and decide. (Example: OODA Loop – Observe, Orient, Decide, Act)

(5) View in Plain Text: Often simply changing the email to "View in plain text" will remove enough non-essential graphics etc. that it will more easily reveal suspicious content.

b) Defending against AI Generated audio and Deepfakes
   (1) Be careful of what information is online regarding the firm and the key personnel in the firm as this publicly available information is often used in these types of attacks.
   (2) Have a policy of independently confirming when money is being exchanged.
   (3) Require a multistep process
   (4) Recommend that internal passwords/passcodes be used for such transactions.
   (5)

D. ISP - Have a written Information Security Policy (ISP)
   1. These should include all expectations for the law firm employees regarding behaviors and processes for information security.
   2. Needs to address the following elements of security
      a) Confidentiality – Goal is that all data and information assets must be limited to authorized users to access and not disclosed to others;
      b) Integrity – Goal is to keep the data intact, complete and accurate, and systems operational
      c) Availability – Goal is to have information and systems available to users when needed.
   3. Must have an authority and access policy. This policy's goal is to create a hierarchy within the company that limits access to lower members in the hierarchy and allows access to higher ranking employees that have a bonafide business interest in access to the information. Members at the top of the hierarchy have administrator access and can authorize and control access by lower members in the hierarchy.
   4. Data must also be classified into classes
      a) High Risk - data protected by state and federal regulation (i.e., the Data Protection Act, HIPAA, FERPA) as well as financial, payroll, and personnel (privacy requirements), client information. (Personal Identifiable Information (PII) and Protected Health Information (PHI)).
      b) Confidential – data that isn't protected or regulated under any law but is judged confidential by the company or industry (law firm client data can fall under both High Risk and Confidential)

c) Public – data and information that is allowed to be freely accessed and distributed

5. Other portions of the ISP should cover:
    a) Disaster recovery plan and data breach plan along with lists of procedures and vendors to contact in the event of a breach or potential of a breach;
    b) Email and electronic messaging etiquette and security behavior and document sharing (internal and external);
    c) Physical location, security and storage of data;
    d) Retention and destruction of digital and physical files;
    e) Employee training policy; and
    f) Designate members of the firm as the contact for notification of security threats or breaches.
        (1) Should be made clear that if an employee discovers a suspicious contact with the firm that has the potential to lead to a security breach situation, discovery of that threat will be immediately reported to the designated security contact. This prevents others in the firm from falling for the threat in the event they fail to recognize the potential threat.
6. Educate employees on the contents of the ISP.

E. Physical Security - Set up security procedures for all visitors to the firm.
    1. Have a check-in policy and make sure that all visitors are escorted to the place or person that they are there to visit and hand off directly to that person.
    2. Know all vendors and recurring visitors of the property.
    3. Make sure that server rooms are locked as well as rooms with any physical client files or other sensitive information.
    4. Only one way into the building from the exterior
    5. Secure all physical client files.
    6. Limit employee authorization to provide information.
    7. Be skeptical. Do not be afraid to question strangers.
    8. Confirm legitimacy of claims via a separate method.
    9. Have a policy that no one answers any “surveys.”
    10. Have a policy on reporting of suspicious behavior.
    11. Talk about security.
    12. Implement a policy to get employees to slow down, scrutinize, and decide before they act (Example: OODA Loop – Observe, Orient, Decide, Act)
    13. Keep a list of recognized and authorized vendors that the firm uses. Have those vendors sign Non-disclosure Agreements.

F. Text Messaging and Social Media

1. Create awareness that phishing is not limited to emails and the same scrutiny needs to be applied to social media and text messages as is applied to emails.
2. Only designated employees should be allowed to post updates to social media about the news and happenings of the law firm.
3. Both text messaging and social media are viewed as casual communication methods, which presents a problem where employees let their guard down when using these forms of communication. Therefore, it is important to make clear that all of the ISP provisions and the behavior learned during firm-wide training applies even when using these more causal methods of communicating.
4. Implement a policy on text messaging clients. If text messaging with clients is allowed how will the messages be downloaded and stored for file retention purposes?

G. Insurance - Obtain proper insurance to cover the firm in the event of a data breach or ransomware event that renders the firm unable to conduct business for a period of time.
    1. Know what your business and malpractice insurance covers and, even more importantly, doesn't cover.
    2. Investigate cyberliability insurance to fill gaps in coverage where data breach and computer fraud are not covered.
    3. In recent years availability of cyberinsurance is becoming more difficult to obtain and, if it can be obtained, the premiums are often very high.
        a) Check with the State Bar of Wisconsin discount program offering to members HSBTotalCyber

APPENDIX A

Top 15 (and more) List of
Low to No-Cost Ways to Increase Information Security

1. **Security Culture**: Create a firm with a security and privacy first culture. Start with why. Make sure your employees understand ***why*** security and privacy is so important to the law firm.
2. **Software Patches/Updates**: Keep all software updated.
3. **Strong Passwords**: Use unique, strong passwords. Invest in a password manager to help you do so.
4. **Use 2FA**: Enable 2-Factor Authentication on all accounts that offer it.
5. **Take it Slow**: Slow down and think before you proceed. Remember the OODA Loop Theory. When in doubt independently verify.
6. **Secure Building and Office Access Policy**: Have a physical security access policy.
7. **Limit User Access**: Limit user access to accounts and files with sensitive information so that only necessary personnel have access.
8. **File Retention Policies**: Have time-limit policies on client document storage – physical and digital.
9. **Encryption**: Encrypt mobile devices, computers, and local backup storage.
10. **Password Protect Hardware**: Require passwords on all devices.
11. **Secure Off-network Work Station**: Have a computer workstation that is not connected to the firm network that is dedicated for online research and social media.
12. **Whitelist and Blacklist Websites**: Utilize the ability to create a firm-wide whitelist (websites that are allowed to be visited from network computers) and blacklist (websites that are prohibited) websites.
13. **Recent, Reliable Backups**: Remember the 3-2-1 theory of backups so you have a recent, reliable backup at all times. One of the best ways to defend against ransomware is being proactive and having a good backup.
14. **Written ISP**: Have a written Information Security Policy (ISP) for your law firm. This can be done on your own or with the help of a security consultant.
15. **Secure Sharing of Documents**: Stop sharing documents by email attachment. Sign up for a service that allows the secure sharing of documents through use of a secured portal instead.
16. **Security Behavior Training and Education**: Training and education are key. An educated workforce about the threats out there is your best defense.

Not low-cost or preventative but highly recommended: Obtain Cyberliability Insurance. Helps to fill the holes in your insurance coverage in events of data breach, theft, or loss.

APPENDIX B

"Reasonable Efforts" Analysis for Evaluating Technology Risks and Benefits

See Wisconsin Formal Ethics Opinion EF-15-01 (Revised 2017)

Note: Efforts must be commensurate with the risks presented. Technology changes rapidly so re-evaluation must be conducted. Circumstances of each law practice vary considerably and must be analyzed with the specific circumstances of the firm in mind. Likewise, within a law practice, circumstances will vary from client-to-client and case-to-case.

Factors to consider:

- 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.

APPENDIX C

Reasonable Precautions for Cybersecurity

See Wisconsin Formal Ethics Opinion EF-21-02

- **Require strong passwords to protect data and to access devices.**
  - The more complex the password, the less likely that an unauthorized user will be able to access data or devices by using password cracking techniques or software.
  - NEVER reuse a password for more than one account.
  - Use a password manager.

- **Use two-factor or multi-factor authentication to access firm information and firm networks.**
  - Although requiring an additional authentication step, may seem inconvenient or burdensome, it is a reasonable precaution that greatly increases protection and reduces the likelihood of unauthorized access by providing an additional layer of security beyond a strong password.

- **Avoid using unsecured or public WiFi when accessing or transmitting client information.**
  - Hackers can access unencrypted information on unsecured or public WiFi and can use unsecured WiFi to distribute malware or intercept information entered.
  - Use a personal hotspot. Feature that can be turned on within your mobile phone to use your phones data connection.

- **Use a virtual private network (VPN) when accessing or transmitting client information or logging into any accounts.**
  - A VPN encrypts information and allows users to create a secure connection to another network.

- **Use firewalls and secure router settings.**
  - A firewall controls incoming and outgoing network traffic based on predetermined security rules: it establishes a barrier between a trusted network and an untrusted network.
  - A router connects multiple devices to the internet and connects the devices to each other.
  - Be sure to secure your router by changing the default username and password.

- **Use and keep current anti-virus and anti-malware software.**

- Be sure to set these to auto-update for the most up-to-date protection

- **Keep all software current: install updates immediately.**
  - Updates help patch security flaws or software vulnerabilities, which are security holes or weaknesses found in a software program or operating system.

- **Supply or require employees to use secure and encrypted laptops.**
  - All lawyers and staff should use only firm issued devices with security protections and backup systems and prohibit storage of firm or client information on unauthorized devices. All devices used by members of the firm, such as desktop computers, laptops, tablets, portable drives, phones, and scanning and copy machines, should be protected.

- **Do not use USB drives or other external devices unless they are owned by the firm or they are provided by a trusted source.**
  - USB drives can contain viruses or malware that could infect the computer or network upon inserting it into a drive.

- **Specify how and where data created remotely will be stored and how it will be backed up.**

- **Save data permanently only on the office network, not personal devices.**
  - If saved on personal devices, taking reasonable precautions to protect such information such as passwords to login to the device and encrypting the device.

- **Use reputable vendors for cloud services.**
  - Transmission and storage of firm and client information through a cloud service is appropriate provided the lawyer has made sufficient inquiry that the service is competent and reputable.
  - Ask questions of providers.
    - How is the information encrypted? Both in-transit and at-rest on the vendor's servers?
    - Who has access to that information?
    - Where is the information is stored. What country? Where is the information backed up (country and location)?
    - Has the vendor undergone a 3rd party security audit?
    - What certifications have been acquired by the vendor?
    - How do you get your information back? Are you able to download and backup your information at any time?

- **Encrypt sensitive information sent in emails or use other secure sharing services to protect sensitive information from unauthorized disclosure.**

- **Encrypt all electronic records, including backups containing sensitive information such a personally identifiable information.**

- **Do not open suspicious attachments or click unusual links in messages, email, tweets, posts, online ads.**

- **Use websites have enhanced security whenever possible.**
  Such websites begin with "HTTPS" in their address rather than "HTTP," and encrypt the communication.

- **Establish and implement policies and procedures for cybersecurity practices.**
  - These policies and procedures should be in writing and provided to all lawyers and nonlawyer assistants, and stress compliance.
  - Train everyone in the law firm on these policies.

- **Establish and implement policies and procedures for the training and supervision of lawyers and nonlawyer assistants in the firm's cybersecurity practices.**
  - Training is the most basic step in avoiding a cyberattack at a law firm. In other words, it is extremely important to develop a culture of awareness. The most serious vulnerabilities of a cybersecurity system are not the hardware or software, but rather the people who use it.

- **Establish and implement policies and procedures regarding remote workspaces to mitigate the risk of inadvertent or unauthorized disclosures of information relating to the representation of clients.**
  - Remote workspaces should be private to ensure that others do not have access to phone conversations, video conferences, or case-related materials.

- **Hold sufficiently frequent meetings between supervising attorneys and supervised attorneys, and between supervising attorneys and supervised nonlawyer assistants to achieve effective supervision.**

APPENDIX D

Additional Resources

Verizon 2023 Data Breach Investigations Reporthttps://www.verizon.com/about/news/2023-data-breach-investigations-report

Cofense 2023Annual State of Email Security Report https://cofense.com/wp-content/uploads/2023/03/2023-Annual-Report-Cofense.pdf

Google Phishing Quiz https://phishingquiz.withgoogle.com/

Have I been Pwned? https://haveibeenpwned.com/ (to search web for email or domain associated with a past breach)

Federal Trade Commission

- Business Guidance - https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business
- Start with Security https://www.ftc.gov/startwithsecurity
- Small Business Training https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/quiz
- Protecting Personal Information https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

NIST Small Business Corner https://www.nist.gov/itl/smallbusinesscyber

Cybersecurity & Infrastructure Security Agency

- Resources https://www.cisa.gov/resources-tools/all-resources-tools
- Report cyber incidents https://www.cisa.gov/report

National Cybersecurity Alliance Resources - https://staysafeonline.org/resources/ and https://staysafeonline.org/resources/cybersecurity-for-business/