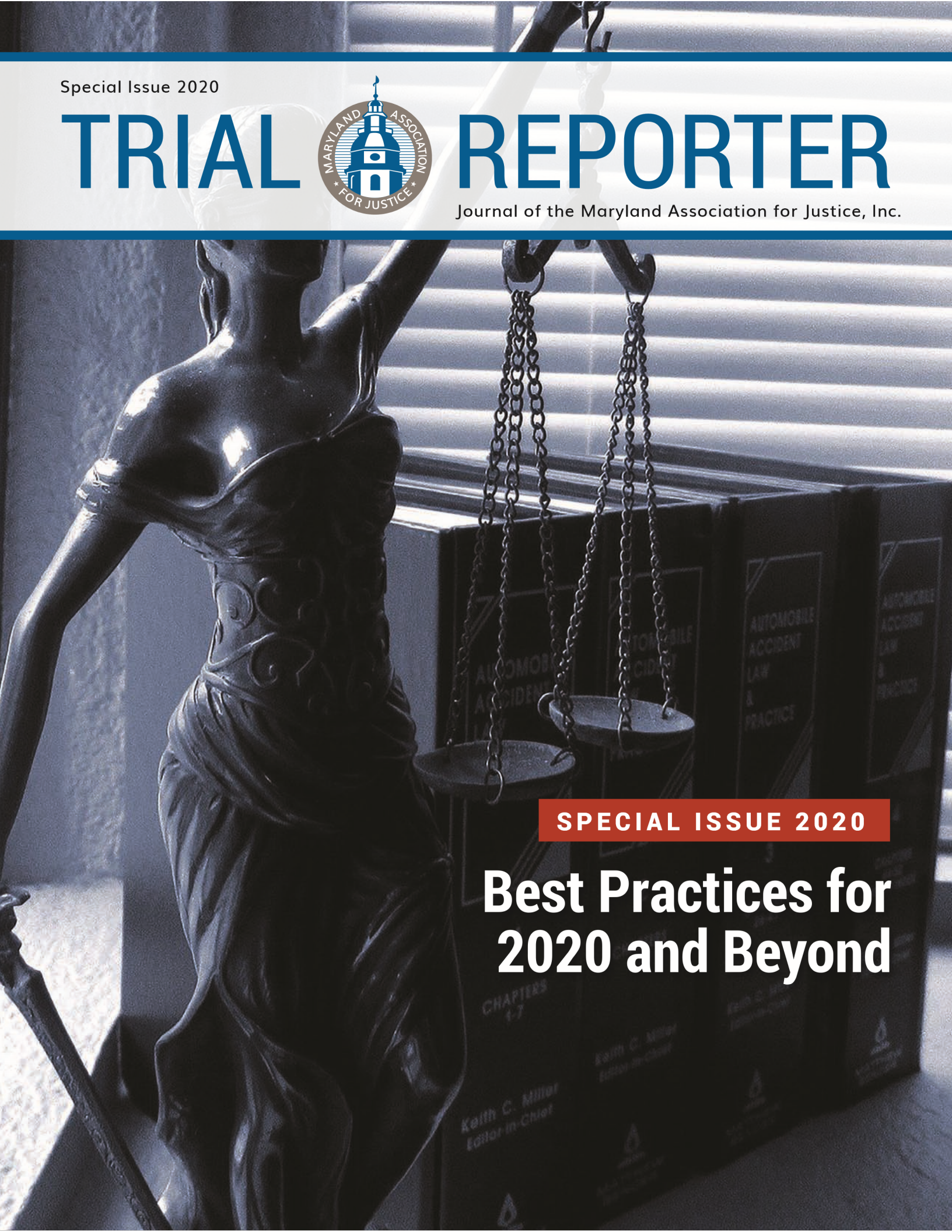
Special Issue 2020

TRIAL REPORTER

Journal of the Maryland Association for Justice, Inc.



SPECIAL ISSUE 2020

Best Practices for 2020 and Beyond

TRIAL REPORTER

Editors-in-Chief

Sheri B. Hoidra
Patrick A. Thronson

Editorial Board

Stephan Y. Brennan
Patrice Meredith Clarke
John J. Cord
Gwen-Marie Davis
David V. Diggs
Jason W. Fernandez
Sara El-Shall
Ellen B. Flynn
David A. Harak
Elisha N. Hawk
Thomas Keilty
Kathleen R. Kerner
Gregg H. Mosson
Richard P. Neuworth
Amy M. Orsi
Eric N. Schloss
Rebecca L. Smith
Sarah Smith
Eric N. Stravitz
George S. Tolley, III
David J. Wildberger

Executive Director
Alison N. Dodge

Director of Communications and Outreach
Brandon W. Corbett

Trial Reporter is a publication of the Maryland Association for Justice, Inc. (MAJ). It is a forum for the bar, bench and others concerned with the civil trial practice and the administration of justice. We encourage your views and opinions. Letters, articles, and proposals may be submitted to the publishers.

Statements and opinions expressed in editorials, articles and commentaries are those of the authors and not necessarily those of MAJ. Publication of any advertiser's claim or of any author's statement, opinion or commentary should not be construed as an endorsement by MAJ. *Trial Reporter* will not be liable for loss or damage incurred from any advertisers published.

Trial Reporter is property of MAJ and its contents may not be reproduced or reprinted without permission from MAJ.

Maryland Association for Justice, Inc.

10440 Little Patuxent Pkwy, Ste 250
Columbia, MD 21044

Phone: (410) 872-0990 | Fax (410) 872-0993
www.mdforjustice.com

Best Practices for 2020 and Beyond

IN THIS ISSUE

6 Cybersecurity Best Practices for Law Firms: Why and How
by Linda Theresa Spradlin

16 Be Smart, Get Help and Don't Be a Jerk – Tips in Responding to the Office of Bar Counsel
By Stephen M. Cornelius and Lauren E. Marini

20 Tips and Best Practices for Litigation and Trial Prep: A New Lawyer Perspective
By Samuel R. Pulver and Kathleen R. Kerner

28 The "Related Specialty" Requirement: Three Recent Examples of This Trap For The Unwary and Best Practices To Avoid It
by Emily C. Malarkey

34 Avoiding Pitfalls in Settlement Agreements that Contain Non-Disparagement and Confidentiality Provisions
By Richard P. Neuworth

38 Cases That Will Change the Way You Practice Immigration Law in Maryland
By Sheri B. Hoidra

42 Ethical Issues Arising at the End of a Case
By Jason Fernandez

48 Uniqueness Not Required for Occupational Disease Claims – Is This the Second Shoe to Drop?
By James K. MacAlister

52 Family Law 2020: A Look Back, A Look Forward and Seismic Change
By Harry B. Siegel

58 Disability Benefits: 2019 Year in Review
By Elliott D. Andalman, Peter Casciano and Matthew DeGioia

IN EVERY ISSUE

2 President's Message
By Ellen B. Flynn

66 Appellate Watch
By Stephan Y. Brennan and Patrice Meredith Clarke

Cybersecurity Best Practices for Law Firms: Why and How

by Linda Theresa Spradlin

Breaches in data information systems are reported in the news daily. Some of the most well-publicized breaches initially were in the retail and hospitality sectors.[1] Cyberattacks in those sectors were easily understandable in that they targeted financial information, usually in the form of payment systems and the types of personally identifiable information typically required to purchase goods and services. Cyberattacks, however, are evolving. Attacks on law firms are rapidly increasing, with attacks first reported by large U.S. and international firms,[2] and more recently, smaller firms.[3] Regulators and clients are responding by mandating assurances that their sensitive data will be protected.[4]

Cyberattacks on law firms are underreported.[5] There are a variety of reasons for underreporting, but with few exceptions,[6] there is no particular federal regulatory regime requiring public disclosure. Often, law firms can contain the release of information about the breach by privately notifying only those clients that have been impacted. The lack of media reports on small, mid-sized and large local firms experiencing a data breach does not mean that cyber criminals are only interested in gleaning information from large national or international firms. Cyberattacks on small law firms with fewer resources and often with less information technology (IT) aptitude, are on the rise.[7] All law firms collect and store confidential, prized corporate and personal information.

A Hacker's Pipeline: Cyber criminals are in the business of sales.[8] Cyber criminals must collect and sift massive amounts of data in order to execute their schemes. Law firms make ideal targets for cyber criminals because information stored by law firms has already been significantly sifted – thereby cutting the amount of work the cyber criminals must do. Hacking schemes to collect the best and most useful information are analogous to going straight to the bottom of a "sales funnel." The term "sales funnel" refers to a marketing concept used by businesses. Sales prospects or "leads" are at the top of the funnel. As customers move from awareness of a product or service down to interest and then down to a desire to purchase, they move towards the bottom of the "funnel." Ultimately, there is a call to action at the bottom of the funnel where the goal is to convert the lead from prospect to sale. As you may imagine, the narrowing of the funnel results in far fewer prospects at the bottom of the funnel than at the top. In the same way, hackers cast a wide net attempting to infiltrate computer systems at hundreds of companies or thousands of corporate divisions, but then have to search through volumes of information (the top of the funnel) to find something of worth. Alternatively, hackers can go straight to sealing the deal by extracting valuable secrets and key personal information stored at law firms (the bottom of the funnel). The latter is becoming the norm because "[e]verything from trade secrets, to sensitive 'market moving' information about a company's finances, to healthcare information and other sensitive non-public information occupy a law firm's servers and data centers."[9]

Legal & Ethical Obligations

Federal Regulations: Law firm cybersecurity procedures are not directly regulated by the federal government. However, in some instances, the nature of the legal work performed for clients in specific industries may subject a firm to federal regulations and processes. The Securities and Exchange Commission provides guidance to attorneys representing public companies before the Commission.[10] Likewise, law firms may regularly represent healthcare organizations, financial institutions or federal agencies. Healthcare organizations are subject to the 1996 Health Insurance Portability and Accountability Act (HIPAA), financial institutions are subject to the 1999 Gramm-Leach-Bliley Act (GLBA) and federal agencies are required to follow the Federal Information Security Modernization Act of 2014 (FISMA). The entities within these industries are required to establish and maintain strict processes and procedures to safeguard certain types of protected information. Attorneys who represent clients in these industries may be required to comply with the same or similar federally mandated cybersecurity standards.

State Regulations: Maryland's Personal Information Protection Act (MPIPA) mandates that businesses (which includes law firms) protect the personal information

of customers, employees and former employees, and establishes data breach notification requirements for companies in Maryland.[11] Personal information includes an individual's first and last name in conjunction with his or her Social Security number, driver's license number, taxpayer identification number or any financial account number (such as a bank account or credit card number).[12] House Bill 1154 went into effect October 1, 2019 and expanded the applicability of MPIPA to those businesses that "maintain" the personal information of Maryland residents.[13] Any business that *maintains* personal information and suffers a data breach must notify the owner or licensee of the information, who in turn has a responsibility to provide breach notification to affected persons. A violation of MPIPA is an unfair, abusive or deceptive trade practice under the Maryland Consumer Protection Act (MCPA), subject to MCPA's civil and criminal penalty provisions.[14]

American Bar Association: In 2012, the ABA "formally approved a change to the Model Rules of Professional Conduct to make clear that lawyers have a duty to be competent not only in the law and its practice, but also in technology."[15] Model Rule 1.1 which pertains to competence was revised in 2012 to add Comment 8, Maintaining Competence: "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." As of November 2019, 38 states have either adopted the attorney duty of technology competence verbatim or with some modification.[16]

In August, 2014, the ABA adopted a resolution on cybersecurity that "encourages all private and public sector organizations [including law firms] to develop, implement and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected."[17]

In May, 2017, the ABA Standing Committee on Ethics and Professional Responsibility released Formal Opinion 477R which provides that "[a] lawyer should understand how their firm's electronic communications are created, where client data resides and what avenues exist to access that information."[18] The opinion also notes, "[l]awyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters."[19]

In October 2018, the same standing committee issued Formal Opinion 483, providing new guidance "on an attorney's ethical obligations after a data breach"[20] and outlining certain "reasonable" steps attorneys should take in the event of a data breach.[21]

Maryland Rules of Professional Conduct

The attorney duty of technology competence under the Maryland Rules is outlined in Rule 19-301.1 and 19-301.6 and the comments thereto.

Comment 20 to Maryland Rule 19-301.6 provides:

> *"When transmitting a communication that includes information relating to the representation of a client, the attorney must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the attorney use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the attorney's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the attorney to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule."*

How to Create and Implement a Law Firm Cybersecurity Plan

While the process of implementing a firmwide cybersecurity plan may seem daunting, failure to plan could expose law firms to significant liability. Aside from potential ethical and legal violations, a data breach may cause a law firm reputational harm and brand damage. Trust and privacy are paramount to clients and the attorney-client relationship. According to the International Association of Privacy Professionals, "the 'responsible' organization will embrace data privacy as a core value, and it will continue to be embedded into corporate culture and process."[22] More precisely, the failure to implement a cybersecurity plan, "reduces the likelihood that a law firm would be able to successfully argue that it had employed 'reasonable security' measures."[23]

The following nonexclusive list of factors should be addressed in a law firm cybersecurity plan:

Designate an Information Security Coordinator (ISC): Someone that can dedicate the appropriate time and effort to security should be designated as the ISC to implement and oversee the firm's data security plan. Additionally, a top-down commitment is necessary for a successful cybersecurity plan.[24] The ISC should set forth the responsibilities of each member of the firm, from the managing attorney to support staff members, and should establish reporting lines. The ISC should also establish procedures for communicating with law enforcement, attorneys general or regulatory bodies, when necessary.

Inventory Information, Access, Hardware and Software: In order to initiate the process of instituting a cybersecurity plan, it is necessary to know what information, hardware, peripherals such as printers and scanners and software the law firm owns. It is difficult to protect information, if a law firm does not realize it has it. This could be due to merger with another law firm, bringing on a new partner and book of business, or having older computers in the office with files worked on by attorneys that have left the firm. In order to protect the data in a law firm, the data must be identified, and an inventory must be created.[25] When creating an inventory, data should be labeled if it is subject to regulatory restrictions[26] such as HIPAA or GLBA. Labeling is important in the event of a data breach because of notification rules that may be triggered under some of the regulatory schemes discussed above. When identifying data, the author and anyone that has access to the data should also be listed on the inventory. Identifying access is an aspect of containment when formulating an incident response plan.

A complete inventory of all devices, including smart devices, should be conducted which includes serial numbers, the location of the device or who has possession of it. All software, including versions, keys and passwords, and licensing information should also be inventoried.[27] Unlike hardware that is visible in the office, software may reside in a variety of places and platforms. The software inventory should identify whether software is located on a particular computer, an external drive, the firm's server or in the cloud.[28]

Assess the Firm's Current Cybersecurity Structure: Ensure the firm's virus, malware and firewall protections are up to date on all devices and networks. Firewalls are a first line of defense by preventing unauthorized access to the firm's websites, mail services and other sources of information accessible from the web.[29] Therefore, attorneys that work from home should also install a

firewall on their home network. The law firm should also be utilizing anti-spam filters, included in most email applications. Anti-spam filters, according to the American Bar Association's 2017 Survey, "can be a strong first line of defense against phishing (malicious emails that try to steal information or plant malware)."[30]

Computers and smart devices should be password protected with the passwords recorded in a secure file.[31] Dual-factor authentication (2FA) is "probably the single most important security precaution" a user can take."[32] 2FA provides a higher level of assurance than simply entering a password for access. When utilizing 2FA, a user enters a password and then a request for a second form of authentication is sent, usually to a device such as a smartphone.[33] Third-party vendors with access to a law firm's computer systems should be vetted and evaluated to determine whether their security certificates are up to date and whether their internal security systems are at the same or higher level than that of their law firm customers.[34] Cybersecurity risk management and breach notification requirements can and should be incorporated into a law firm's contract with outside vendors and contractors.[35]

Use Secure Methods to Transmit and Store Data: Encryption or zipped and password protected files are methods of securely transmitting and storing data. Encryption scrambles data, converting it into an unrecognizable form so cyber criminals and unauthorized viewers cannot read it. Encryption can be used to protect "files and storage devices, as well as data transferred over wireless networks and the Internet."[36] There are a variety of encryption applications available, many are free while others like the popular WinZip software with AES[37] encryption for Windows, macOS, iOS and Android platforms must be purchased. Additionally, both Microsoft and Apple include encryption technology in some or all of their products.[38] However, the sensitivity level of the data and size of the law firm, especially those with offices in multiple locations, would likely require third-party software specifically designed for the firm's purpose.

Establish Policies: A security program should address people, policies and procedures and technology. All three areas are necessary for an effective program.[39] There cannot be effective security if firm members are not trained and do not understand the threats, how to protect against them and the applicable security policies. Naturally, a security plan should also address physical security in addition to access control, meaning those in the firm authorized to view particular data. Finally, a cross-organization team consisting of IT and security personnel, finance, communications, office management, human resources and chairs of practice groups should meet regularly to discuss and coordinate information security issues.

Training and Tabletop Exercises: According to the ABA's 2014 resolution on cybersecurity, training and constant security awareness should be addressed in any security or incident response plan. It is important that law firms, whether large or small, run practice scenarios in the event of a data breach. Just as medical and law enforcement conduct tabletop exercises for natural disasters, cyber tabletop exercises are fire drills for data breaches. It will be excruciatingly stressful if the first time the firm utilizes its calling tree to notify team members of a data breach, the threat is real and few, if any members, have practiced for their roles. Training is an essential step in being prepared to respond to real cybersecurity incidents.[40]

While there are certainly vendors and consulting firms that will organize and help conduct tailored cyber tabletop exercises for law firms, there is also a plethora of white papers on various scenarios that smaller firms may want to consider utilizing for practice. Additionally, the MSBA offers an on-demand CLE entitled "Privacy & Data Security – Before the Incident"[41] to help educate attorneys on how best to protect firm and client data and to develop a strategy for a breach before it happens.[42]

Standard Frameworks: Cybersecurity frameworks are blueprints for building information security programs.[43] Like architectural blueprints, frameworks may be tailored to meet certain specifications, including regulatory compliance. According to IT Governance, the most prevalent frameworks are: PCI Data Security Standard (PCI DSS) (47%), International Organization for Standardization (ISO) 27001/27002 (35%), Center for Internet Security (CIS) Critical Security Controls (32%) and National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Security (29%).[44]

Law firms typically utilize one or a combination of these frameworks to formulate a comprehensive cybersecurity incident response plan.[45] The NIST framework, for instance, "was developed in a manner to promote wide adoption of practices to increase risk management-based cybersecurity across all industry sectors and by all types of organizations"[46] and has been described as a compilation of best practices.[47]

Cybersecurity is ever-evolving. NIST's Special Publication 800 series (SP 800) on cybersecurity is,

therefore, regularly updated to keep cybersecurity standards as current as possible.[48] NIST SP 800 details not only best practices for cyberattack prevention, but also covers the feasibility and cost-effectiveness of the suggested standards.[49] Compliance with the NIST SP 800 series is not as intimidating as it may first appear. An article from "Federal Computer Week" simplified compliance with NIST 800-171 into seven essential steps:[50]

1) Identify systems that contain sensitive information
2) Separate sensitive information from more benign information
3) Limit access of sensitive information only to authorized employees
4) Encrypt all data, including sensitive information
5) Monitor access to sensitive information
6) Regularly train and retrain employees on cybersecurity best practices
7) Regularly conduct security assessments of all systems

Beware of WiFi: Law firm networks should be secure, encrypted and hidden. In contrast, readily available public WiFi in places such as coffee shops, shopping malls and airports, are not hidden or secure and make data vulnerable to interception. Attorneys working remotely, should be using a virtual private network ("VPN") to help protect data. VPN's are typically very affordable and often offered in a package with other security features. Not all VPN's are created equally, however. Research should be conducted in order to choose a VPN that best matches the goals and needs of the firm.

Employ a Reliable Backup Platform: Backup services are essential to fending off ransomware attacks. Even those law firms that have experienced a ransomware attack and have paid the ransom, reported experiencing downtime of hours, days or weeks to get the firm's files and systems back up and running. There are a variety of reliable backup systems. According to the ABA's survey on law firms, "the most frequently reported form of backup is external hard drives (38%), followed by offsite backup (30%), online backup (30%), network attached storage (15%), USB (9%), tape (7%), RAID (7%), CDs (4%) and DVDs (4%)."[51]

Consider Cyber Insurance: Most legal malpractice and general liability policies do not cover cybersecurity incidents or data breaches. Cyber insurance policies provide coverage for both first-party and third-party data losses. Simply purchasing cybersecurity insurance, however and failing to properly plan or implement necessary requirements will not trigger coverage in the event of a compromise. Read policies and exclusions carefully and follow the insurers framework for coverage and reporting.

Business Continuity Plan: A BCP is separate plan. A firm's response to an incident, however, naturally impacts its continuity as a business. Aside from establishing areas of responsibility and emergency contact information, the BCP should include offsite backed up data, backup power, an alternative means of communication, an alternative location to conduct business and essential equipment and services.

Effective security is an ongoing process. All attorneys and law firms should have in place comprehensive, risk-based security programs that include training and constant security awareness.

Biography

Linda Theresa Spradlin is licensed to practice law in Maryland, Florida and Tennessee and focuses her practice on privacy law and data security as CEO of Teri Spradlin, LLC. She earned her bachelor's degree at the University of Maryland, College Park. She received a J.D. and Maritime Law Certificate from Tulane University School of Law, an LL.M. in Cybersecurity Law and Crisis Management from the University of Maryland Francis King Carey School of Law and is a graduate of the University of Virginia's National Trial Advocacy program. She is a Certified Information Privacy Professional (CIPP/US) and is currently working towards certification as a Certified Information Security Manager (CISM).

Endnotes

1 Target, Home Depot, Marriott, Marshalls, T.J. Max, and Equifax. Gary Dinges, REGISTER GUARD, U.S. Retailers Top Target for Cyberattacks, Report Says, Oct. 1, 2019, https://www.registerguard.com/news/20191001/us-retailers-top-target-for-cyberattacks-report-says

2 Nicole Hong and Robin Sidel, WSJ, Hackers Breach Law Firms, Including Cravath and Weil Gotshal, Mar. 29, 2016, https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504; Julie Sobowale, ABA JOURNAL, Law Firms Must Manage Cybersecurity Risks, Mar. 1, 2017, http://www.abajournal.com/magazine/article/managing_cybersecurity_risk

3 David G. Ries, ABA TECH,2018 Cybersecurity, Jan. 28, 2019, https://www.americanbar.org/groups/law_practice/publications/techreport/ABATECHREPORT2018/2018Cybersecurity/

4 Karen Painter Randall and Steven Kroll, ABA, How Clients are Pushing their Outside Counsels Adopt Stricter Cybersecurity Standards and Protections, Aug. 2, 1018, http://www.abajournal.com/magazine/article/clients_outside_counsels_cybersecurity

5 Christine Simmons, *et al., LAW.COM, More Than 100 Law Firms Have Reported Data Breaches. And the Problem Is Getting Worse, Oct. 15, 2019*, https://www.law.com/2019/10/15/more-than-100-law-firms-have-reported-data-breaches-and-the-picture-is-getting-worse/?slreturn=20200009192239

6 *E.g. HIPAA* https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

7 Jay Reeves, LAWYERS MUTUAL, 10 Steps for Sol and Small Firm Cyber-Safety, Feb. 11, 2019, https://www.lawyersmutualnc.com/blog/10-steps-for-solo-and-small-firm-cyber-safety

8 Chris Williams, THE REGISTER, 620 Million Accounts Stolen from 16 Hacked Websites Now for Sale on Dark Web, Feb. 11, 2019, https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/; Danny Palmer, ZDNET, Ransomware: The Number of Victims Paying Up is on the Rise, and That's Bad News, Dec. 20, 2019, https://www.zdnet.com/article/ransomeware-the-number-of-victims-paying-up-is-on-the-rise-and-thats-bad-news/

9 Holly Urban, LAW TECHNOLOGY TODAY, Cybersecurity Standards in the Legal Field, Jun. 13, 2019, https://www.lawtechnologytoday.org/2019/06/cybersecurity-standards-in-the-legal-field/

10 15 U.S.C. §7201 (2002).

11 Md. Code, Com. Law Art. §§14-3501 *et seq.*

12 *Id.*

13 Md. Code, Com. Law Art. §14-3504.

14 Md. Code, Com. Law Art. §§13-101, *et seq.*

15 Robert Ambrogi, LAW SITES, States have Adopted Ethical Duty of Technology Competence, Mar. 11, 2015, https://www.lawsitesblog.com/2015/03/11-states-have-adopted-ethical-duty-of-technology-competence.html

16 Robert Ambrogi, LAW SITES, Tech Competence, 2019, https://www.lawsitesblog.com/tech-competence

17 ABA, Report and Resolution 109, Adopted at the 2014 Annual Meeting in Boston , http://www.americanbar.org/content/dam/aba/events/law_national_security/2014annualmeeting/ABA%20-%20Cyber%20Resolution%20109%20Final.pdf

18 ABA, ABA Formal Opinion 477R: Securing communication of protected client information, June 2017, https://www.americanbar.org/news/abanews/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli/

19 *Id.*

20 ABA, ABA Formal Opinion 483: Lawyers' Obligations After an Electronic Data Breach or Cyberattack, Oct. 17, 2018, https://www.americanbar.org/content/dam/aba/images/news/formal_op_483.pdf

21 *Id.*

22 Paul Jordan, IAPP, Notes from the IAPP-Europe Managing Director, Jan. 2, 2020, https://iapp.org/news/a/notes-from-the-iapp-europe-managing-director-3-jan-2020/

23 Joseph Burton, LPT, 4 Steps to Getting Serious About Law Firm Cybersecurity, Sept. 15, 2014, https://www.lawpracticetoday.org/article/4-steps-getting-serious-law-firm-cybersecurity/

24 Kevin Delay, CISCO, Seven Cybersecurity Tips for 2020, Dec. 9, 2019, https://newsroom.cisco.com/feature-content?type=webcontent&articleId=2038484

25 Nate Lord, DIGITAL GUARDIAN, Law Firm Data Security: Experts on How to Protect Legal Clients' Confidential Data, Feb. 16, 2018, https://digitalguardian.com/blog/law-firm-data-security-experts-how-protect-legal-clients-confidential-data

26 Juliana De Groot, DIGITAL GUARDIAN, What is Data Classification? A Data Classification Definition, Jul. 15, 2019, https://digitalguardian.com/blog/what-data-classification-data-classification-definition

27 Note 30, *supra.*

28 *Id.*

29 Peter Stockburger, DENTONS, New ABA Opinion – Attorneys Must Take Reasonable Cybersecurity Measures To Protect Client Data, May 12, 2017, http://www.privacyandcybersecuritylaw.com/new-aba-opinion-attorneys-must-take-reasonable-cybersecurity-measures-to-protect-client-data

30 David G. Ries, ABA TECHREPORT 2017, Dec. 1, 2017, https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security/

31 LAWYER MONTHLY, Nov. 28, 2018, Top 5 Cybersecurity Tips to Protect Your Privacy, https://www.lawyer-monthly.com/2018/11/top-5-cyber-security-tips-to-protect-your-privacy/

32 Ed Bott, ZDNET, Protect Yourself: How to Choose the Right Two-Factor Authenticator App, Aug. 5, 2019, https://www.zdnet.com/article/protect-yourself-how-to-choose-the-right-two-factor-authenticator-app/; Margaret Rouse, TECH TARGET, Two-Factor Authentication, Aug. 2018, https://searchsecurity.techtarget.com/definition/two-factor-authentication

33 *Id.*

34 Julie Sobowale, Note 2, *supra.*

35 Also known as Vendor Risk. For example, services that are outsourced such as administrative tasks, ediscovery, collections and billing; and vendors that provide point of sale payment systems, remote IT services and advertising and marketing. Michael Volkov, JDSUPRA, Managing Third-Party Vendor Cybersecurity Risks, Sept. 11, 2019, https://www.jdsupra.com/legalnews/managing-third-party-vendor-99769/; Brian Thomas, BITSIGHT, 4 Ways to Minimize the Risk of Third-Party Data Breach, Nov. 20, 2019, https://www.bitsight.com/blog/4-ways-to-minimize-the-risk-of-a-third-party-data-breach.

36 Christensson, P. (2014, November 11). Encryption Definition. Retrieved 2019, Dec 31, from https://techterms.com

37 Advanced Encryption Technology ("AES") uses the Rijndael cryptographic algorithm and is approved by NIST for use by the U.S. government.

38 Windows 10 Pro and Enterprise include Bitlocker which can be used to encrypt the entire hard drive or a partitioned drive, but not just individual files. Apple requires 2FA be enabled on the user's Apple ID and uses end-to-end encryption to secure data in transit. It leaves data in an encrypted format while stored in iCloud or on a third-party server such as AWS or Google.

39 Note 35, *supra.*

40 Note 22, *supra.*

41 Mike Oliver, MSBA, Privacy & Data Security – Before the Incident, 2018, https://www.msba.org/product/2018-advanced-business-law-institute-privacy-data-security-before-the-incident/

42 According to the MSBA's office on Learning and Publications, the course also includes a questionnaire for GDPR implementation and background authority on data breach preparedness.

43 Lee Kim and Axel Wirth, HIMSS, Cybersecurity Frameworks Explained, Aug. 30, 2019, https://www.himss.org/news/cybersecurity-frameworks-explained

44 Melanie Watson, IT GOVERNANCE USA, Top 4 Cybersecurity Frameworks, Jan. 17, 2019, https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks

45 Sherri Davidoff, LPT, Law Firm Cybersecurity Audits: Getting to Good, Feb. 12, 206, https://www.lawpracticetoday.org/article/law-firm-cybersecurity-audits-getting-to-good/

46 Kevin Kimball, NIST, Federal Register /Vol. 82, No. 15, p. 8409, January 25, 2017.

47 CIPHER, NIST Cybersecurity Framework (CSF), https://cipher.com/blog/a-quick-nist-cybersecurity-framework-summary/

48 FTC, Understand the NIST Cybersecurity Framework, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/nist-framework

49 NIST SP 800-171, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

50 Izak Bovee, FCW, 7 Steps for Getting Right with NIST 800-171, May 4, 2018, https://fcw.com/articles/2018/05/04/comment-800-171-compliance.aspx. See also Note 8, *supra.*

51 Note 3, *supra.*