CAN DEFENSE COUNSEL SHOW THEY ARE CYBER SECURE?

By Barry Miller and Curt Graham of Freeman Mathis & Gary, LLP

In the ever-changing world of data privacy, there is a new development in Kentucky of which to be aware. During the 2022 legislative session, Kentucky's General Assembly passed House Bill ("HB") 474, the Insurance Data Security Law (the "Act"). *See* Ky. Rev. Stat. §§ 304.3-750 – 304.3-768. The Act gives insurers and other "licensees" some time to comply with its provisions and most insurers will be ready to do so. But Kentucky insurance defense counsel may not be prepared for the Act's impact.

The Act took effect on January 1, 2023. It gives licensees two years to implement a compliant information security program. A "licensee" is defined as "any person who is, or is required to be, licensed, authorized to operate, or registered pursuant to the insurance laws of [Kentucky]." KRS 304.3-750(6)(a). Beginning on February 15, 2025, licensees must certify to the Kentucky Insurance Commissioner that their plan complies. KRS 304.3-756(9). After that, the statute requires certification yearly, and the Insurance Commissioner will retain enforcement authority to investigate possible violations of the Act. *Id.*

The Act requires insurers' security plans to be "[c]ommensurate with the size and complexity of the licensee," the sensitivity of nonpublic information it holds, and other factors, "including its use of third-party service providers." KRS 304.3-756(2). That's where attorneys come in. Under the Act, a "third-party service provider" includes an individual, organization, or business who contracts with a licensee to "maintain, process, or store nonpublic information" or "[i]s otherwise permitted access to nonpublic information through its provision of services to a licensee." KRS 304.3-750(10). Defense attorneys frequently gain access to medical, financial, and other private information from carriers during litigation, and therefore meet the definition of third-party service providers under the new statute.

Additionally, the Act requires licensees who use third-party service providers (including attorneys) to:

(a) Choose them with due diligence; and

(b) Require the provider to "implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider."

KRS 304.3-756(6).

Reading these parts of the statute together, insurers cannot properly certify their own compliance with the Act without first determining that their defense counsel is protecting nonpublic data accessed from the carrier. Some insurers may require defense counsel to make their own independent certification. Others may send surveys to defense counsel about their cyber precautions. No matter how they ask the question, when insurers make their certification to the Insurance Commissioner, they will be relying upon the answers their defense counsel provided. Accordingly, to respond properly, defense counsel will have to understand what the carriers must certify.

Section 4(4) of the Act provides a comprehensive list of the requirements in an

insurer's security plan. Understanding and meeting these requirements will help a law firm show it has a compliant program.

APPOINT A CISO

Under the Act, each carrier must appoint one person as being responsible for its security program. KRS 304.3-756(3)(a). Corporations commonly refer to this as a "Chief Information Security Officer," or "CISO." The CISO may be an officer, employee, affiliate, or outside vendor.

Who is an appropriate CISO? The position requires expertise in information security. Many CISOs have sought certification by the International Organization for Standardization ("ISO"), most commonly under the ISO 27001 standard, recognized internationally as an appropriate framework for information security. When developing their own compliant program and considering someone for the CISO position, firms should inquire whether the candidate has the ISO 27001 certification (or other appropriate credential). They might also ask whether the candidate has earned a Certified Information Privacy Professional ("CIPP") designation from the International Association of Privacy Professionals ("IAPP"). The two most appropriate IAPP designations would be CIPP/US (certifying the candidate as knowledgeable about privacy laws in the United States), and CIPM (Certified Information Privacy Manager).

Some law firms may have attorneys or technical staff holding one or more of these certifications. Those who do not may want to consider designating an outside law firm or cybersecurity company as their CISO.

CONSIDER THE THREATS TO INFORMATION SECURITY

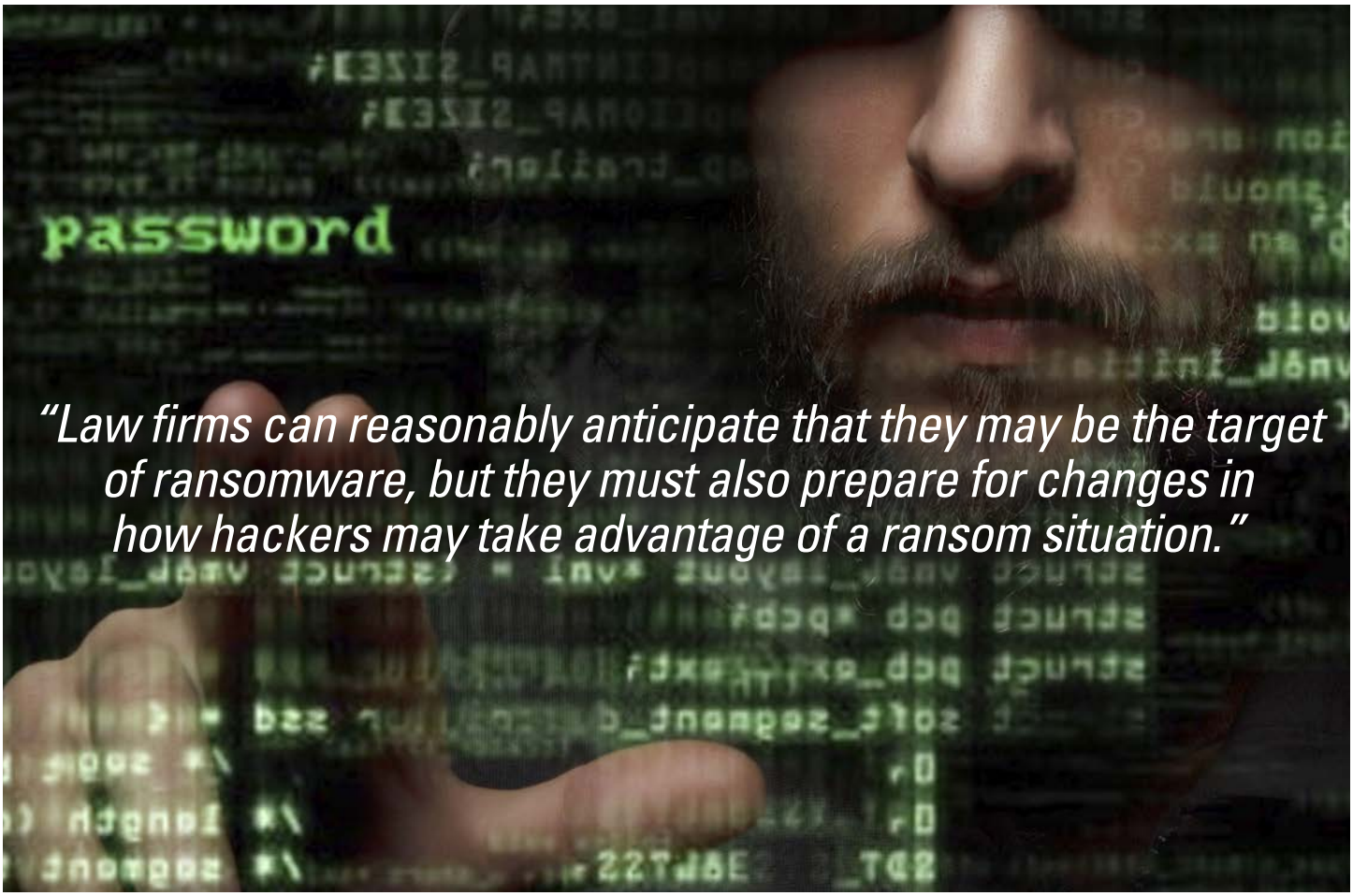
The statute also requires insurers to anticipate "reasonably foreseeable" threats—both internal and external—that might result in unauthorized access to private data. KRS 304.3-756(3)(b). A CISO (or an attorney who stays abreast of such threats) can lead the firm in this exercise.

The American Bar Association's 2020 Legal Technology Survey reported that 29% of the responding firms had experienced a data breach. Another 21% did not know whether they had ever suffered a breach.[1] More than ten years ago, the Federal Bureau of Investigation warned that there were only two kinds of law firms: those that had suffered a breach, and those that would. The problem has only gotten worse since that warning.

Past attacks have come through:

- Broadcast malware links (via emails sent to many users);
- More targeted emails with malware links—often information gained from a broadcast email will give a hacker information to target those in the C-Suite of a corporation, or users who handle wire transfers or other financial transactions for a firm; and/or
- Spoofed web pages or email addresses.

Firms can reasonably anticipate that such attacks will continue. But they must also be aware that the techniques used by hackers change



constantly. Being prepared for last year's (or last week's) methods are not likely to be enough. Firms, or their CISOs, will need to be vigilant for new kinds of attacks.

One example of such change is what has occurred with ransomware over the past few years. In its early days (late 1990s) ransomware used a broadcast technique, at first being put on floppy discs that would install malware on a computer when the disc was used. The next wave saw ransomware being sent directly to thousands or even millions of email addresses. No matter how the malware first got into a victim's computer, the mechanism was the same after that. The malware would encrypt the user's data, making it unintelligible without a decryption key. Ransoms were in the hundreds of dollars, and the chance that a victim would get a usable decryption key in exchange for the ransom was high. Hackers who used this technique often purchased their malware kits from various organized crime groups. The more successful ones used a customer service model, even to the point of setting up toll-free numbers that victims could call for help about obtaining bitcoin to pay ransoms or other assistance.

Around 2015, the criminal organizations supplying ransomware kits determined they could make more money by cutting out the intermediaries. Instead of the broadcasting method, these groups would use social engineering and other techniques to send more targeted emails to specific organizations. In 2016, the Hollywood Presbyterian Hospital paid what was then one of the largest ransoms—$17,000—to regain access to its data.

The latest evolution of ransomware is about as far from the early "customer-service" days as imaginable. Now hackers not only encrypt a victim's data, but they extract data containing personal information of a company's clients and threaten to release that data unless the company pays the ransom within a specific time. Such criminals have released private data to back up that threat. This element of extortion also comes with an increased price. Ransomware demands of $50 million are common now, and security consulting group Unit 42 reports that the average ransomware payment in 2021 was $570,000, compared to $312,000 the prior year.[2]

In 2016, the Moses Alfonso Ryan law firm was hit by the WannaCry malware.[3] It locked the firm's billing system for three months. The firm lost $700,000 in client billings and paid ransom in an undisclosed amount.

Law firms can reasonably anticipate that they may be the target of ransomware, but they must also prepare for changes in how hackers may take advantage of a ransom situation.

ASSESS THE LIKELIHOOD OF THE VARIOUS THREATS AND THE INFORMATION THREATENED

After cataloguing the foreseeable threats, firms must consider how likely they are to occur. They also must weigh that likelihood against the information that particular kinds of attacks may threaten. For example, the information that firms may hold about their employees may differ significantly from the data they gather to conduct their day-to-day business. In its 2022 report, NetDiligence alerted firms conducting real estate business that they will be increasingly targeted, as hackers attempt to gain information that

may allow them to intercept or redirect wire transfers.[4]

A law firm that primarily conducts insurance defense might not deal with wire transfers as often as a real estate firm. Most settlements in insurance defense cases are still accomplished using checks. But wire transfers are sometimes used in such cases, particularly where structured settlements are used. But even if the likelihood of a hacker redirecting a wire transfer may not be as great for an insurance defense firm, the potential impact such an attack might have on a law firm could still make it worthwhile to consider strategies to protect that kind of information. Highly sensitive data requires more protection even when the risk of disclosure is low.

Insurance defense firms also possess a great deal of health care information about the plaintiffs in their cases. Medical information is among the most sought after by hackers, as shown by the amounts such records command in illegal markets. Forbes reported in 2017 that credit card records may be worth as little as 25 cents in such markets, while medical records can be worth hundreds or thousands of dollars.[5] Criminals use the information in medical records for many purposes, including making fraudulent insurance claims or extorting the victim with embarrassing information.

ASSESS CURRENT PROCEDURES

The Act next requires insurers to assess their current procedures and refine them or add new ones where necessary.

Does a law firm train its employees and management on existing threats and how to avoid them? Proper training remains one of the most effective procedures a firm can adopt to keep secure the information it holds. Various vendors offer cybersecurity training videos that can help with training. Mitnick Security (headed by Kevin Mitnick, once a hacker but now a consultant) is one of the better known. A Google search for "cybersecurity training videos for employees" yields many others, some offering videos at low or no cost. The federal Cybersecurity and Infrastructure Security Agency offers a downloadable Workforce Training Guide that can help employers create in-house training programs.[6]

Training is best when it is tested, and many law firms now use services that will send their employees fake phishing emails to identify employees who may be susceptible to such attacks—a technique known as "penetration testing." Employees who click on links in such emails are candidates for remedial training and further testing.

Law firms also should consider their hardware and software design. Can individual employees or attorneys install software on their work-issued computers? Do they bring their own devices to work, or do firm work on their personal devices remotely? The answers to these questions will affect the firm's risk level. Learning these answers may spur the firm to create procedures governing the use of personal hardware and better protect client data where it may be held.

Does the firm's software and hardware design include detection and prevention measures? Remember that in 2020, 21% of law firms reported to the ABA that they did not know whether they had ever been the victim of a data breach. This is opposed to IBM's 2022 reports stating that for "83% of companies, it's not if a data breach will happen, but when. Usually more than once." That same report noted that in 2022 it took an average of

287 days to identify and contain a breach, and the average containment time was 80 days. *Id.* On average, then, it took more than 200 days for the average victim to learn that they had been breached. If a breach cannot be prevented, it must be detected as soon as possible so hackers are not at their leisure to review a firm's data and decide how best to exploit it.

Finally, has a firm identified procedures for how to respond to a breach? Must it notify government agencies? Must it notify its clients? Under what circumstances might it agree to pay a ransom? Does it know how to pay one, if necessary? How will it obtain the use of its data again and remediate its systems? These questions are among those to be answered by an information security plan.

ESTABLISH A PLAN

After determining what threats it might face, what information it holds that might be threatened, and assessing the risk of any of those threats coming to fruition, the law firm and its CISO have the information they need to craft a proper information security plan.

For an insurance defense firm, steps in that plan might include:

Mapping where their data reside: Such a map will include all devices, systems, and facilities that might use data provided by an insurance carrier, or data gathered while defending an insured.

Establishing controls to authenticate users: Proper controls ensure that only authorized persons can view, change, and otherwise use sensitive data. This can include easy-to-implement steps such as requiring multi-factor authentication. Anyone who has logged into an online banking site will be familiar with multi-factor controls. When a user enters the proper password, the bank responds by sending a code, usually by text to the user's cell phone. The requirement to enter that code, which changes upon every use, is the second factor that authenticates the user. Biometric information can also be used to create multi-factor controls.

Putting proper physical restrictions in place: Examples might be locks on server room doors or on paper file rooms that hold sensitive data.

Encrypting nonpublic information: Encrypting the hard discs of computers that access and hold sensitive data is one of the least expensive measures available but also one of the most effective. Microsoft makes this available to all licensed users, as does Apple.

Purging data: Many lawyers are packrats and loath getting rid of old files. But accumulating data and continuing to hold it after a case is finished only makes the firm a more vulnerable target and increases the damage that can be caused by a breach. Establishing procedures to securely dispose of data that is no longer necessary should be part of any information security plan. A CISO or other certified person can help set up procedures that comply with state and federal law.

Testing the plan: Many CISOs or vendors can assist the firm with tabletop exercises, designed to simulate a breach and to test the firm's response to that breach. A firm that has undergone one or more of such exercises is much more prepared if a

real breach occurs.

Knowing who to notify, when, and how: The term "breach" may have a defined meaning under different statutes or regulations. Under Kentucky's breach notification statute (KRS 365.732(2)), for example, a company must notify any Kentucky resident whose personally identifiable information was taken from its computer system, "in the most expedient time possible and without unreasonable delay," although delays for law enforcement purposes may be permissible. But a breach need not be disclosed to consumer reporting agencies or credit bureaus unless it involves the data of more than 1,000 persons. A breach affecting information governed by the Health Insurance Portability and Accountability Act must be reported to the Office of Civil Rights, local media, and affected individuals if unsecured data from more than 500 individuals is involved. 45 C.F.R. § 164.406(a). These different examples provide a glimpse into how complex the laws governing breach notification can be.

ETHICAL CONSIDERATIONS

Finally, understanding data privacy concerns and the implications of Kentucky's new Act may be more than just "good business" for insurance defense firms – it may also be necessary to comply with certain ethical obligations. A few distinct rules come to mind in this context. Ky. Sup. Ct. Rule 3.130(1.1) (Competence) requires attorneys to possess "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." SCR 3.130(1.1). The commentary to this Rule states that "[t]o 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…" SCR 3.130(1.1(6)). It seems clear that the ethical rules also require lawyers – at a minimum – to (1) monitor for data breaches, (2) stop a detected breach and restore their systems if a breach occurs, and (3) determine how the breach occurred.

Also relevant is SCR 3.130(5.1), which requires lawyers with managerial authority to ensure that their firms take reasonable measures to make sure all attorneys and staff conform to the Rules of Professional Conduct, including SCR 3.130(1.1)'s duty to keep abreast of technology changes. SCR 3.130(5.1).

Regarding breach notification specifically, ABA Formal Ethics Opinion 95-398 provides that notice must be given to a firm's clients if a breach of the duty of confidentiality was committed by or through a third-party vendor or other service provider. This duty arises from SCR 3.130(1.4), which addresses communication with clients and provides that "[a] lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." SCR 3.130(1.4). Other ethical rules may apply depending on the context of the breach.

CONCLUSION

To be clear, the Act does not directly regulate lawyers or law firms. It is directed only to strengthening and maintaining insurers' cyber readiness. Some defense counsel may not even notice a difference after the implementation of the statute. But it has been the experience of our firm, in states where similar statutes or regulations have been in place for a few years, that the statute will significantly affect insurance defense firms. Insurers who take the requirements of the statute seriously know they must attest that their vendors are cyber secure. Because the statute is specific about what constitutes the secure handling of private information, it makes sense for defense firms to consider its language when looking at their own cybersecurity. The Act contains other requirements, but the ones listed above are the most important for defense counsel to consider. Keeping the requirements of the Act in mind, defense firms must consider their own security plans to be prepared to answer the questions insurers will be asking to comply with the Act.

Barry Miller (bmiller@fmglaw.com) is a Partner in Freeman Mathis & Gary, LLP, chair of the firm's Lexington office, and a member of its Data Security, Privacy & Technology practice section. He holds the CIPP/US designation from the International Association of Privacy Professionals. He has presented to the KDC on technology issues affecting lawyers and ethical issues related to the use of technology in the practice of law.

Curt Graham (cgraham@fmglaw.com) is a Partner in Freeman Mathis & Gary's Lexington office. His practice primarily focuses on data privacy and governmental liability issues. He is a member of KDC and DRI, and he practices in Freeman Mathis & Gary's government law and torts practice sections.

[1] John G. Loughnane, *2020 Cybersecurity*, AMERICAN BAR ASSOCIATION (Oct. 19, 2020), https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/ (last visited Nov. 28, 2022).

[2] *Ransomware demands soar by 518% in 2021*, GRC WORLD FORUMS (Aug. 13, 2021), https://www.grcworldforums.com/ransomware/ransomware-demands-soar-by-518-in-2021/2357.article (last visited Nov. 28, 2022).

[3] Jeff Peters, *As WannaCry Spreads, Law Firm Reveals Separate Ransomware Cost Them $700,000*, SURFWATCH LABS, INC. (May 17, 2017), https://blog.surfwatchlabs.com/tag/moses-afonso-ryan/ (last visited Nov. 28, 2022).

[4] *NetDiligence Cyber Claims Study - 2022 Report*, NETDILIGENCE.COM, https://netdiligence.com/wp-content/uploads/2022/10/NetD_2022_Claims_Study_1.0_PUBLIC.pdf (last visited Dec. 30, 2022).

[5] Mariya Yao, *Your Electronic Medical Records Could be Worth $1000 To Hackers*, FORBES (Apr. 14, 2017, 10:05 PM), https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/?sh=31453c5950cf (last visited Nov. 28, 2022).

[6] *Cybersecurity Workforce Training Guide*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Workforce%20Training%20Guide_508c.pdf (last visited Nov. 28, 2022). The ABA offers its cybersecurity handbook for sale at a fraction of a consultant's hourly fee. THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS (Jill Rhodes, Robert S. Litt, and Paul S. Rosenzweig, 3rd ed. 2022).

[7] *Cost of a data breach*, IBM, https://www.ibm.com/reports/data-breach (last visited Nov. 28, 2022).

[8] *Device encryption in Windows*, MICROSOFT, https://support.microsoft.com/en-us/windows/device-encryption-in-windows-ad5dcf4b-dbeo-2331-228f-7925c2a3012d (last visited Nov. 28, 2022); Use FileVault to encrypt your Mac Startup disk, APPLE INC., https://support.apple.com/en-us/HT204837 (last visited Nov. 28, 2022).