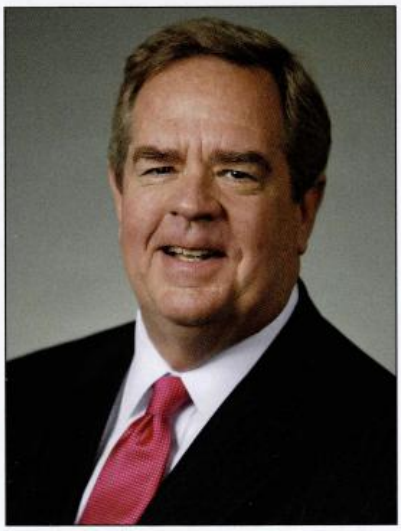

Cyber

You've Been Hacked! You and Your Firm Are Targets

A Cybersecurity Primer for the Mississippi Practitioner

By H. Hunter Twiford, III[1]

Continued on next page



By H. Hunter Twiford, III
Jackson, MS

WHO SHOULD READ THIS ARTICLE?

I'll try to save you some time: take a quick look at this section to see whether you're in the target audience.

If you're one of the 23.6 percent of Mississippi attorneys who practice by yourself, you should definitely read this. There's no one else to make sure your computer systems are protected (except perhaps your IT consultants, and you should be able to intelligently discuss what you need with them). If you're one of the 23 percent who practice with one or two other lawyers, or the 11.5 percent who practice in firms of four to five lawyers, you, too, should probably read it – you can at least nod intelligently at the right places during the firm discussion of cybersecurity. And if you're not the techno-nerd in your firm, you should also designate one of your lawyers to work with your IT consultant to develop a response plan – you're in the fastest growing target group for cyberattacks, and you need to be able to respond quickly and decisively when you're attacked. (By the way, in case you're keeping track, that's a little more than 58 percent of Mississippi lawyers who practice in small firms, defined as firms of five or less attorneys.)

If you're in the 13.3 percent practicing in firms with six to ten lawyers and you don't have an IT resource on staff, you should read this for largely the same reasons as your slightly smaller brethren. Those of you in the larger firms – 8.5 percent in firms of eleven to nineteen attorneys, and 20 percent in firms of more than twenty – almost certainly have in house IT resources who should be on top of this. But read the article (and the others in this edition) anyway so you can intelligently discuss cybersecurity, and perhaps even fend off an attack, particularly a well-focused spear-phishing or a social engineering effort.

If you're among the 23.8 percent of the survey respondents who work for the federal or state government, you can probably skip it. You've already got scads of IT people working on the problems, and they're not going to listen to you anyway – even though the federal government has been hacked more often than a clear-cut forest. (Another aside for you state employees and special assistant attorneys general: a recent report found that Mississippi was one of only two states in the country with a "truly outstanding" IT strategic plan, and credited the strategy of letting people develop the plan who know more about cybersecurity than the politicians. What a novel concept.)

If you're looking for a discussion of our ethical obligations to maintain client confidentiality or potential violations of the Rules of Professional Conduct for failing to do so through a data breach, you won't find it here. Nor will you find a discussion of the minimal technological competence needed to meet ethical muster – that's elsewhere in this magazine. Nor will you find a roadmap to prosecuting or defending a data breach on behalf of a client. What you will find is an introduction to cybersecurity, and some ideas how to avoid a data breach – hopefully, enough to at least get you thinking about the topic.

WHAT IS CYBERSECURITY?

If you're still reading, let's take a shot at defining the subject matter. The U. S. Department of Commerce's National Institute of Standards and Technology (NIST) defines cybersecurity as "the ability to protect or defend the use of cyberspace from cyberattacks." Cyberspace is defined as "a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." And a cyberattack is "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing con-

trolled information."

Now that we've quoted the government's somewhat circular definitions, let's simplify it: Cybersecurity is a measure taken to protect a computer (which includes a computer system or network, including a computer on the Internet) against unauthorized access or attack. So says Merriam-Webster. Generally, the term is used to describe the efforts – the technology, the processes, and the practices – designed to protect data stored on computers, whether standalone or networked, from criminal or unauthorized access, attack, or damage.

THE SCOPE OF THE PROBLEM

Cybersecurity is evolving. It's more than just a technology issue. It's an issue that affects virtually everyone. I've been hacked. So have you, whether you know it or not. I've had my identity stolen (more than once). So have most of you. And that's before the Equifax hack, and the Home Depot hack, and the Target hack, and the other hacks *de jour* added a few million more victims (and potential victims) to the mix.

According to one study of corporate directors and general counsel, over 7,700 data breaches have been made public since 2005, with over 1 billion records breached. And that worries them – data security is now ranked as the number 1 worry of almost 90 percent of corporate directors and over 85 percent of general counsel. 77 percent believe that their company's risk of cyber liability has increased over the last two years. And tellingly, 40 percent lack confidence in their company's response plan in the event of a breach. It's not just large organizations that are susceptible to being hacked: according to The Insurance Journal, 55 percent of small businesses have experienced a data breach, and almost that many – 53 percent – have suffered multiple breaches.

And data breaches aren't just a corporate problem: a 2017 ABA article called it the biggest risk that law firms now face. TruShield, an IT security company, reported that the Legal industry was the second most targeted vertical sector for a cyberattack, second only to the Finance industry. Several of AmLaw 50 law firms have been the victims of major cybersecurity breaches – Cravath Swaine, Weil Gotshal, DLA Piper, Wiley Rein. And the number is growing. If these law firms – some of the largest, most sophisticated, most technologically-advanced (and well-funded) law firms in the world, with scads of IT people spending all of their time trying to strengthen the castle and fend off attackers, can be breached, how can we Mississippi practitioners be safe?

The 2016 TruShield report indicates that small law firms are now the most frequently targeted, and its chief security architect gives the reason for the increased targeting as: "The attackers know law firms process highly sensitive information for their clients, and a lot of the time … attackers also know that law firms and the legal industry in general lack standardization on security program structures, controls, and oversight. This divergence can result in security weaknesses." The report also predicts that email will be the most vulnerable access point for hackers to exploit.

Most law firms simply aren't prepared to react to a data breach. The 2016 ABA Legal Technology Survey Report indicates that only 17 percent of all law firms had an incident response plan in place to address a security breach – and only 50 percent of large law firms (500 or more lawyers) had a plan in place.

Our more sophisticated clients know this, and are now requiring that those law firms who want to represent them concentrate on cyberattack risks. Almost one third (30.7 percent) of all law firms reported that current or potential clients provided them with security requirements – including cybersecurity requirements – that the law firm must follow if they want to represent that client. Our law firm's larger clients, particularly those in the financial services industry, have adopted extremely detailed "vendor" policies we're required to follow, many of which are geared towards protecting their and their customers' data. Examples include: limited access segregated file storage (physical access is limited to only those attorneys and support staff who are actively working on those files, and any access must be logged); "locked door" and "clean desk" policies; limited access to that client's ESI on the firm's computer network (again, access is limited only to those previously-approved attorneys and support staff who are actively working on that particular client's file); software which permits remote wiping of all computers, smart phones, and tablets in the event of loss or theft; automatic encryption of any data downloaded from a firm computer onto an external storage device; encryption of any email or attachment which contains a client's customer's PII (Personally Identifiable Information) (this also applies to PHI (Protected Health Information) for those in the Health Care and Insurance industries); and the immediate deletion of stored electronically stored information (ESI) for that client file as part of the file closing process. And these are only the tip of the iceberg, and more of these requirements are added each year. If you don't want to go to the trouble or expense of complying with these policies, that's fine – they'll just find another firm who will.

Continued on next page

WHAT MUST BE PROTECTED?

Personally Identifiable Information (PII). Examples include:

- Social Security number
- Driver's license number
- Credit/debit card numbers
- Passport number
- Banking records
- Date of birth
- Medical information
- Mother's maiden name

(While not now technically required to be protected, I suspect that the model of your first car, your favorite sports team, and the name of your first pet will probably be added at some future date.)

Protected Health Information (PHI). Examples include:

- Medical records
- Health status
- Provision of healthcare
- Payment for healthcare

(HIPAA is a primary source for PHI scope and restrictions.)

Certain business information, such as:

- Customer lists
- Prospect lists
- Trade secrets
- Business plans and strategies
- Employee lists

Some of these are found in state statutes, such as the Mississippi Public Records Act, MISS. CODE ANN. §§ 25-61-1 *et seq.*, and particularly, § 25-61-9 (certain records furnished to public bodies by third parties containing "trade secrets or confidential commercial or financial information shall not be subject to inspection, examination, copying, or reproduction or dissemination to third-parties" without notice and opportunity to seek a protective order). The Mississippi Uniform Trade Secrets Act, MISS. CODE ANN. §§ 75-26-1 *et seq.*, defines and governs trade secrets and their disclosure. § 75-26-11 also protects trade secrets during litigation. MISS. CODE ANN. §79-23-1(1) likewise protects "commercial and financial information of a proprietary nature required to be submitted to a public body . . . shall be exempt from the provisions of the Mississippi Public Records Act. . . ." This is by no means an exhaustive list of the applicable statutes potentially in play.

HOW (AND WHY) YOU MIGHT LOSE YOUR DATA

You're vulnerable to at least four primary types of ESI data theft: (1) physical loss, such as a lost or stolen laptop, smart phone or tablet, or a lost or stolen jump or thumb drive or other portable media (external storage device) containing PII or other sensitive data; (2) a direct database/server breach, in which an unauthorized person accesses or hacks into your owned or leased data server which stores your and your clients' personal, financial, business, or other sensitive data; (3) data stolen by an otherwise authorized user, in which your employee (or other person with authorized access) downloads or sends personal or sensitive data to an unauthorized location for an improper or criminal purpose; and (4) a vendor/third-party breach as a result of negligence, physical loss, database/server breach, or stolen data at a vendor's or third-party administrator's (licensee) physical location or server (including your cloud provider or other storage vendor). The number one cyber threat to your data – some estimates run as high as 74 percent – is insider theft.

Most data breaches are the result of one (or a combination) of five primary reasons: (1) insufficient planning and preparedness (66 percent), (2) the complexity of business processes (52 percent), (3) insufficient risk assessment (48 percent), (4) the complexity of IT processes (46 percent), and (5) silos and turf issues (44 percent). The average cost of a data breach incident is $4 million, although that figure takes huge data breaches against household name companies into consideration. The recent DLA Piper breach, which required the firm to shut down its networks in multiple countries for several days to contain the threat (with the attendant lost time and productivity costs)

may easily cost that much; however, it's unlikely that the cost to a Mississippi law firm would approach that figure.

WHAT YOU CAN DO TO REDUCE THE CHANCES OF A DATA BREACH

• Be aware of cyber threats. And get educated. You're reading this edition of the Mississippi Lawyer. That's a start. Consider taking an online course to learn more, and have your associates and employees do so, as well. Since your primary vulnerability is through someone with authorized access to your data, make sure they're at least aware of what not to do – like clicking on unknown links or downloading attachments to emails from unknown senders – to avoid a breach, and what to do in the event of a breach. (Hint: don't ignore it, and just hope it goes away. It won't.) Understand all of your firm's vulnerabilities, internal and external, including identifying your weak points. And once again: get educated.

• Keep your operating system up to date, and make sure you install the updates and patches. A hacker can take advantage of operating system or application vulnerabilities which aren't properly patched or updated, which puts all of your data at risk. Also, keep your anti-virus and anti-malware software up to date. Hackers are writing new malware daily, and the software you bought two years ago and haven't updated since may be subject to new known malware.

• Encrypt your data. Most operating systems now have full-disk encryption software built in – it comes as a standard feature. Use it. You can encrypt every file on your drive with a button click or two. If you don't know how, ask your teenager. If you don't have one, find one and ask them. If that doesn't work, call your IT consultant.

• Consider moving your data to the cloud. Cloud computing offers significant benefits to the solo/small firm lawyer. Security is a primary benefit. You get secure online storage (the security is generally far superior to what you can afford to do on your network, and you won't have to locate your server in your unsecured closet, like some politicians), redundant data backup, including 24/7 access, a built-in disaster recovery plan, and a secure client portal to share documents and communications with clients, experts, and co-counsel. You're much less likely to get hacked if your data is cloud-based.

• Use strong passwords. Not your name or your child's name, or your birthday or social security number. Those are easily located through public sources, and unfortunately, too many people use them alone or in combination. The hackers know that, and will start there with their cracking efforts. Don't write the passwords down and tape them to your computer. Or leave them in your desk drawer. Or tape them to the bottom of your desk drawer. Use a good password vault app – most of them are secure. Don't give out your password to anyone (other than perhaps a trusted assistant, or if necessary, your IT person). If you do have to give it out, consider changing it immediately.

• Limit physical access to your computers, especially by delivery persons, the cleaning crew, maintenance personnel, and the like. That guy in the UPS uniform may be a hacker, and you may be getting a dose of social engineering. Secure the workplace. Have all of the computers on your network set to "sleep" or automatically log out after five or so minutes without any keystrokes so no unauthorized persons have access to a workstation while your secretary is on a lunch break.

• Limit the transfer of data to external media, and make sure when it's transferred, the data is encrypted. You might consider limiting or prohibiting remote use of the external media – remember the VA data breach, in which almost 27 million discharged veterans' records were stolen from a VA employee's home after the employee had "improperly" taken the data home.

• Make sure your hardware is physically secure, particularly your laptop, smart phone, or tablet. They're easy to steal. Or lose. And once you do, the sophisticated thief has access to all of your and your clients' data. Remember the VA data breach? (It was only a couple of sentences ago.) Install software that allows you to remotely wipe your computer or phone. (No, Hillary, it's not the same as dabbing Clorox on your computer case with a soft cloth.) If, heaven forbid, you do lose your device or it's stolen, you can remotely erase all of the data.

• And back up your data. Religiously. Like every day. Or perhaps even more often if you've got a bunch of users inputting data all day long. If you're a solo/small firm lawyer, consider buying two or three external hard drives of sufficient size to hold all of your data. Use drive number 1 to do a full system backup every other day, say Monday, Wednesday, and Friday. Use drive number 2 to do a full system backup on the odd days, say Tuesday and Thursday. Take the drive you just backed up off premises and store it. If you won't do off premises storage, at least disconnect it from your system so

Continued on next page

a hacker can't access it, too, and leave you without a backup. (But the external backup could be stolen or destroyed by fire or natural disaster.) Consider using a third drive and taking a full backup once every week or so (or once a month, if you dare), and storing it offsite if you won't take your daily backups offsite. A fire or other disaster could ruin your data, as well as your day. Conduct "test restores" periodically to make sure the backups are working properly. If all of this sounds like too much trouble, you may want to consider backing up in the cloud – it's automatic, secure, and inexpensive. Just make sure you know/trust your provider, encrypt your data before it's uploaded, and don't give the encryption keys to anyone, including your cloud provider. If even that sounds like too much trouble, think about the trouble restoring all of your data in the event of a ransomware attack which locks up all of your data and the thief won't release the key even after he takes your Bitcoins, or the data becomes corrupted by that worm that crawled in through the malware pinhole.

It should go without saying that you must delete all of your data from any computer you're taking out of service. Reformat the hard drive. Make sure there are no remnants of data on the drive. You'd be surprised how many computer users don't bother to wipe the data before sending the old clunker to the junk pile. The Idaho Power Company was probably surprised to see four of their hard drives containing hundreds of thousands of confidential employee documents and information for sale on eBay. Ditto for the Loyola University (Chicago) computer which was discarded before the hard drive containing the PII for some 5,800 students was erased. Woops. Hard to explain either of those little oversights.

Finally, have a data breach response plan so you can immediately take the right steps to contain – or at least, minimize – the damage. Include your IT consultant and your staff in both the development and implementation of the plan. Plan in advance on what sort of notice you might have to give. Consider having a provision in your fee agreement letters with your clients discussing data security and beach notice.

FEDERAL DATA BREACH LAW SUMMARY

There are some fifty federal statutes addressing data protection or privacy protection standards and requirements ranging from antitrust to military/defense to RICO to the PATRIOT Act, and everything in between. It's far beyond the scope of this article to go into all of them – there are some good summaries available online – but here are some examples to get you thinking.

Most states, including Mississippi, have enacted legislation which requires the breached entity to give notice of security breaches involving PII (in all of its forms) to its affected customers. Typically, the residence of the affected individual determines the applicable notice law, regardless of the residence of the breached entity or whether it has a physical location or conducts business within that state.

- There are at least three separate federal acts that deal specifically with identity theft: the Identity Theft Enforcement and Restitution Act of 2008 (ITERA) (targets identity theft, phishing, and spam, and focuses on "botnets" (networks of infected computers used in various identity theft-related schemes)); the Identity Theft and Assumption Deterrence Act of 1998 (ITADA) (provides that identity theft is a federal crime, provides penalties, and directs the Federal Trade Commission to record and refer complaints under the act); and the Identity Theft Penalty Enhancement Act of 2004, (ITPEA) (establishes penalties for aggravated identity theft).

- The Gramm-Leach-Bliley Act of 1999 (GLB) which requires financial institutions to protect the security and confidentiality of their customers' personal information. GLB also authorized the adoption of federal regulations by various agencies to further the stated purpose of the act.

- The Sarbanes-Oxley Act of 2002 (SOX), which requires covered firms to report annually to the Securities Exchange Commission on their internal financial controls, including information security.

- The Fair and Accurate Credit Transactions Act of 2003 (FACTA) requires the Federal Trade Commission and other agencies to develop guidelines for identity theft prevention programs in financial institutions, including "red flags" which may indicate possible identity theft.

- The Federal Information Security Management Act of 2002 (FISMA) which creates the federal information systems cybersecurity framework (with emphasis on risk management), and requires agency-wide information security program implementation. Oversight responsibility goes to the Office of Management and Budget (OMB).

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which includes the requirement that the Secretary of Health and Human Services (HHS) establish security standards and regulations which protect the patient's individually identifiable health information, and requires covered health care providers to protect the security of that confidential information.

If you're eyes aren't glazed over by now, go online and see how many more federal laws you can find involving cybersecurity. There's no prize for the winner except the personal satisfaction of knowing more about cybersecurity than 99.96 percent of the lawyers in the country.

INTERPLAY BETWEEN FEDERAL AND STATE DATA BREACH LAW

Most states, including Mississippi, have enacted legislation which requires the breached entity to give notice of security breaches involving PII (in all of its forms) to its affected customers. Typically, the residence of the affect-

ed individual determines the applicable notice law, regardless of the residence of the breached entity or whether it has a physical location or conducts business within that state.

Congress has failed to adopt recently proposed federal breach notification laws designed to supersede state laws for widespread breaches, despite arguably good reasons for preemption – it's clearly more cost, time, and effort efficient for a breached entity to give notice to three or four million affected customers under a single federal requirement, rather than having to comply with the laws of fifty states (well, actually forty-eight states at time of this writing), the District of Columbia, and who knows how many territories and foreign countries. However, there is no such federal law (yet). Last year, H.R. 3806, the Personal Data Notification and Protection Act of 2017, was referred to committee, where it languished. Similar bills were introduced in the 113th and 114th Congresses and met similar fates. As of March 12, 2018, there has been no related bill information received for H. R. 3806. Thus, at least for the foreseeable future, a breached entity should plan to give notice to its affected customers under their residence state's data breach law.

MISSISSIPPI DATA BREACH LAW SUMMARY

MISS. CODE ANN. §§ 75-24-29, adopted in 2013, applies to "any person who conducts business in Mississippi" (we'll call them the "Target") who, in the ordinary course of business, owns, licenses, or maintains the personal information of any Mississippi resident. The statute contains the following relevant definitions:

- "Breach of Security" is defined as the "unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state [we'll call them the "Victim"] when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable."

- "Personal Information" includes a person's first name or first initial and last name, in combination with any of the following: Social Security number, driver's license number (or state identification card number), account number, or credit/debit card number (in combination with any required security code, access code, or password). Publicly available information which the general public can lawfully access from federal, state, or local government records or widely distributed media is not Personal Information under the statute.

The breached Target must disclose any breach of security to all affected individuals "without unreasonable delay." The Target's timing of the disclosure to the Victim(s) is subject to certain enumerated exceptions, including the Target's opportunity to complete an investigation to determine the nature and scope of the incident, or to identify the affected individuals (the potential Victims), or to restore the reasonable integrity of the data. Subsection (3) of the statute provides a potential out for the Target: "notification shall not be required if, after an appropriate investigation, the [Target] reasonably determines that the breach will not likely result in harm to the affected individuals." The Legislature, in its wisdom, has left it to the courts to sort out the parameters of an "appropriate investigation," what's reasonable, and what constitutes harm to the Victim.

If the data is maintained as "computerized data" and includes personal information of the Victim, the Target must immediately notify the Victim as soon as practicable after discovery of the breach, if the personal information was or is reasonably believed to been acquired by an unauthorized person for fraudulent purposes. Notification required by § 75-24-29 may be delayed for a reasonable period of time if a law enforcement agency is investigating and determines that the notification will impede a criminal investigation or national security. Delayed notification must be made to the Victim as soon as the law enforcement agency determines that notification will not compromise its criminal investigation or national security.

Notice may be provided by any of the following methods: (a) written notice, (b) telephone notice, (c) electronic notice (if the primary means of communication between the Target and the Victim is by electronic means), and (d) substitute notice, provided that the reporting company demonstrates that the cost of providing notice by the other allowed means would exceed $5,000, or that the class of affected persons to be notified exceeds 5,000 potential Victims, or the Target not have sufficient contact information for the Victims. The statute also specifies approved methods of substitute notice.

Subsection (7) of the statute provides a safe harbor for the Target upon its demonstration of compliance with the statutory requirements, including the notice timing requirements. A failure to comply constitutes an unfair trade practice to be enforced by the Mississippi Attorney General. Interestingly, the Legislature specifically provided that the statute does not create a private right of action against the Target for its failure to report or to comply with the statute, leaving the Victim without a meaningful legal remedy under the statute.

Continued on next page

MISSISSIPPI CYBERCRIME PENAL LAW

MISS. CODE ANN. §§ 97-45-1 *et seq.* provide criminal penalties for various offenses against or involving computers and computer users. Section 97-45-1 contains the definitions applicable to the chapter, such as "computer," "computer network," "computer program," "computer software," "computer system," etc.

Section 97-45-3 defines "computer fraud," which occurs when a computer (including the computer, the computer system, or the network) is accessed with the intent to (a) defraud, or (b) to obtain something of value (money, property, or services) through false conduct, representations, or practices, or through false or fraudulent alteration, deletion, or insertion of programs or data, or (c) to insert or attach programs or data that is intended to acquire, alter, damage, delete, disrupt, or destroy property or otherwise use the services of computer program (think malware and ransomware). Subsection (6) defines the term "computer network" as including the internet (as defined by federal law).

If the damage or loss amount is less than $1,000, the offense is punishable by a fine not to exceed $1,000 or by imprisonment for not more than six months in the county jail or both. Third and subsequent offenders where the value is not less than $500 may be imprisoned for up to three years or fined up to $10,000 or both.

If the damage or loss is more than $1,000 but less than $5,000, the fine may be up to $10,000, or imprisonment in the state penitentiary for not more than five years, or both. For damage or loss between $5,000 and $25,000, the maximum fine remains up to $10,000, but the term of imprisonment increases to not more than ten years, or both the fine and imprisonment. If the loss or damage exceeds $25,000, the fine is still up to $10,000, or incarceration not more than twenty years, or both.

Section 97-45-5 criminalizes certain intentional acts against computer users, such as denial of use or access to authorized users, or unauthorized disclosure of passwords or other means of computer access without consent. The penalties are similar to those in the preceding paragraph, and are enhanced based on the value of the loss or damage amounts.

Other sections of Title 97, Chapter 45 specifically prohibit tampering with computer equipment, identity theft, online impersonation, cyberstalking, and similar offenses.

CYBERSECURITY INSURANCE COVERAGE

Effective cyber risk-mitigation strategies include securing comprehensive cyber insurance coverage. Some twenty-five insurance companies now offer cyber coverage for both first-party and third-party losses. The coverages and exceptions vary widely, and a good broker can help you determine what's the right coverage for you.

A good cyber insurance policy should cover your and your law firm's liability for a data breach involving sensitive consumer information – their PII and PHI, their Social Security numbers, credit and debit card numbers, account numbers, driver's license numbers, and health records. The information may be in your client's records furnished to you as part of your representation. It may be part of a party's records received in discovery. The source is immaterial; the duty (and any actionable breach) is not. The policy should also cover the costs associated with a cyber claim, including the cost of defense.

The first-party coverage should include theft, fraud, destruction, or loss of your data as the result of a criminal or fraudulent cyberattack, including theft or unauthorized transfer of your regular or trust account funds. Other first-party coverages might also include forensic investigation, business interruption, extortion/ransomware attacks, and restoration of lost or corrupted data. In addition to third-party liability coverage to defend any lawsuits over the loss of your client's data, you might need coverage to pay for the costs of notification and credit monitoring for your affected clients. Depending on your area of practice, you might also need regulatory response coverage to assist you in responding to governmental regulators' inquiries following a cyberattack, particularly if you practice in the Financial or Insurance sectors.

You should carefully study your cyber insurance policy, and understand insurance policy variations and associated implications. Assess potential policy gaps and blind spots. Compare the cyber coverage to the coverage under your regular errors and omissions policy, and look for overlaps. Look closely at the cyber policy exclusions. A typical cyber insurance policy should cover your legal fees and expenses in the event you're sued for the breach. It should also cover most or all of the cost of notifying the affected persons about the data breach, restoring their personal identities, recovering any compromised data, and repairing any damage to your computer system. It should also provide coverage for data breaches or misconduct of your outside vendor if you outsource data processing or storage, as is almost always done in cases involving large e-discovery/ESI volume.

The insurance industry is slowly moving towards an industry-standard cyber insurance policy with standard coverages, but until then, gaps between first- and third-party coverage under existing policies may leave you holding the proverbial bag for uncovered losses. You and

your insurance broker should conduct a comprehensive review of your E & O policies to determine what cyber risks (if any) are covered, and which of the four typical cyber liability insurance policies – data breach and privacy management coverage, multimedia liability coverage, extortion liability coverage, and network security liability – should be purchased.

You should ask your broker or E & O carrier at least these key questions:

- Does my insurance cover a cyber event? Are there any exclusions?
- What cyber liability insurance policies should I consider purchasing?
- Is my firm properly managing third-party vendors who have access to my cyber environment, and am I covered for their breach?
- Is the cyber policy I'm considering (or you're recommending) triggered by date of loss or is it a claims made policy? How does that square with my regular E & O policy? Do I have any gaps in coverage?

Then, ask for a sample policy, and read it. Make sure it covers what you want and need. And when you purchase a cyber policy, don't throw it in the drawer or tell your assistant to file it, and wait until you have a breach to dig it out and read it (even if that's what you usually do with your E & O policy).

And for the 25 percent of you who don't have professional liability insurance, please, please, please don't continue to go naked. Get the E & O coverage. And add the cyber coverage, too. You can't afford a major claim. Your clients will thank you. The Mississippi Bar will thank you. And your dependents may thank you, too.

OTHER RESOURCES

The ABA is working to give us lawyers more guidance – the second edition of the ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals is scheduled be published in August. (The first edition was published in 2013, and is available through the ABA, and at physical and online booksellers, if you can't wait for the second edition.) The ABA Cybersecurity Task Force is now focusing on small firms, and plans to develop another cybersecurity handbook aimed primarily at small firms. The Association of Corporate Counsel (ACC) and a group of its members have developed an excellent publication, the Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information to help in-house counsel coordinate and set expectations with their outside vendors, including their outside counsel, on the data security controls which should employed to protect company confidential information. And there are a number of good blogs and online articles discussing cybersecurity for lawyers. The Mississippi Bar Technology Committee will continue to focus on the subject, and we'll hopefully be able to assemble additional materials and make them available online. Stay tuned . . . ■

---

1 H. Hunter Twiford III is a member of McGlinchey Stafford, resident in its Jackson office. Hunter is the head of the Firm's Complex Commercial Litigation Group, the Mississippi Commercial Litigation section, and chairs the Firm's e-Discovery team. His practice is exclusively devoted to litigation, primarily in federal court, with emphasis on class action defense, complex commercial litigation, and complex lender liability litigation. Hunter was also a founding member and a two-term chairman of the Mississippi Bar's Technology Committee (1999-2000, 2000-2001), and has served on its Executive Committee since inception.

2 The Mississippi Bar 2016 Economic Survey, https://www.msbar.org/media/3354/2016-economic-survey-report-revised-12-18-17.pdf. All of the percentage figures for the various firm sizes cited in this paragraph are taken from the 2016 Economic Survey, the most current survey available.

3 *See* Brookings Blog, *How State Governments Are Addressing Cybersecurity*, G. Dawson and K. Desouza (3/5/15), available at https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/ *See also* https://motherboard.vice.com/en_us/article/d73kmv/mississippi-and-idaho-have-the-strongest-cybersecurity-in-the-us-report-says

4 *See Glossary of Key Information Security Terms*, NISTIT 7298 (Rev. 2), available at https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. All of the NIST terms in this paragraph are defined in the Glossary.

5 *See Data Breaches*, available at *See* https://www.privacyrights.org/data-breaches

6 *See Law in the Board Room in 2015*, Corporate Board Member & FTI Consulting, Inc., http://www.fticonsulting.com/insights/reports/law-in-the-boardroom-in-2015.

7 See http://www.insurancejournal.com/news/national/2014/11/24/347795.htm

8 J. Sobowale, *Law Firms Must Manage Cybersecurity Risks*, ABA Journal, March 2017, also available at http://www.abajournal.com/magazine/article/managing_cybersecurity_risk.

9 *See* N. Ahmed, *Cyberattacks – A 2015 Industry Breakdown* (3/10/16), available at *https://trushieldinc.com/cyber-attacks-a-2015-industry-breakdown/*

10 *See, e.g.*, J. Sobowale, *Six Major Law Firm Hacks in Recent History*, ABA Journal, March 2017, also available at http://www.abajournal.com/magazine/article/law_firm_hacking_history/

11 *See* K. Rattigan, *TruShield Report Says More Cyber-Threats in 2016 than Ever Before* (3/14/16), available at https://www.dataprivacyandsecurityinsider.com/2016/03/trushield-report-says-more-cyber-threats-in-2016-than-ever-before/

12 *Id.*

13 *Id.*

14 *See* 2016 ABA Legal Technology Survey Report, https://www.americanbar.org/groups/law_practice/publications/techreport/2016.html

15 *Id.*

16 *See, e.g.*, The Ponemon Institute, Second Annual Study of the Cyber Resilient Organization, http://info.resilientsystems.com/ponemon-institute-study-the-2016-cyber-resilient-organization. An Executive Summary of the study is also available at https://cdn2.hubspot.net/hubfs/427640/IBM_Resilient_Branded_Content/Infographics/IBMresilience_GlobalCyberResilienceGap_infographic%20FINAL-1.pdf

17 *Id.*

18 *Id.*

19 *See, e.g.*, http://fortune.com/2017/06/29/dla-piper-cyber-attack/

20 *See, e.g.*, https://www.epic.org/privacy/vatheft/

21 *See, e.g.*, https://www.computerworld.com/article/2555144/security0/idaho-utility-hard-drives---and-data----turn-up-on-ebay.html

22 *See, e.g.*, https://www.scmagazine.com/5800-loyola-university-chicago-students-at-risk-for-id-theft/article/556515/

23 *See, e.g.* Congressional Research Service, E. Fisher, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation* (12/12/14), available at https://fas.org/sgp/crs/natsec/R42114.pdf

24 18 U.S.C. § 1030.

25 18 U.S.C. § 1028.

26 18 U.S.C. §§ 1028, 1028A.

27 15 U.S.C. Chapter 94, §§ 6801 – 6827.

28 15 U.S.C. § 7262.

29 P. L. 108-159, 117 Stat. 1952, *see* 15 U.S.C. § 1601 nt. for affected provisions.

30 44 U.S.C. Chapter 35, Subchapters II and III, 40 U.S.C. § 11331, and 15 U.S.C. § 278 g-3 & 4.

31 42 U.S.C. § 1320 d et. seq.

32 See, e.g. https://www.congress.gov/bill/115th-congress/house-bill/3806/related-bills

33 The Mississippi Bar 2016 Economic Survey at p. 26, https://www.msbar.org/media/3354/2016-economic-survey-report-revised-12-18-17.pdf.

34 The ACC Model Controls are available at http://www.acc.com/advocacy/upload/Model-Information-Protection-and-Security-Controls-for-Outside-Counsel-Jan2017.pdf?_ga=2.18008698.2105555974.1496154508-4598426.1496154508