Editor’s Note:
The results of the American Bar Association’s TECHREPORT 2019 are in — and attorneys and law firms aren’t making the grade. The gloomy findings released this fall illustrate how much the profession needs to advance to meet today’s information privacy and security needs, not to mention ethical obligations: “The 2019 Survey results show that, while some progress has been made in some areas, law firms have further to go in designing and implementing appropriate solutions,” the report reads. (Read more at: www.americanbar.org/groups/law_practice/publications/techreport/)

According to the report, more than 25 percent of respondents across the country have reported a security breach at their firm, and more than a third have had systems infected with viruses, spyware and malware. Only 31 percent of respondents reported having an incident response plan and less than half use file encryption or email encryption.

The TECHREPORT also shows how slowly the needle is moving on these issues. So, how can solo attorneys and small firms best prepare for modern cybersecurity challenges? In this space, we offer expert advice from practicing attorneys and technology professionals on issues including email encryption, regulatory changes, and much more, will help you prepare for these new challenges to your practice in 2020.

Table of Contents
II. Cameron Shilling
A Pragmatist’s Solution for Information Privacy & Security
III. Jason Sgro
Let’s Talk About Email
IV. Lisa Sgro
Cybersecurity Best Practices for Lawyers and Law Firms
Ryan Barton
Leading Change: Creating a Culture of Cybersecurity at Your Firm
V. P. Bill Cheng & John F. Weaver
The Art of Managing a Cyber Security Breach

A Pragmatist’s Solution for Information Privacy & Security
By Cameron G. Shilling

Information privacy and security can seem complex and confusing. Breaches are common, impacting even sophisticated and well-financed corporate giants like Marriott, Equifax, Anthem, and Yahoo!, and leaving small and mid-size companies wondering if they stand any chance of protecting themselves. Adding to that sense of hopelessness, divergent laws emanate from foreign jurisdictions like the European Union, Great Britain, and Canada, as well as populous states like Massachusetts, California, Illinois, and New York. To make matters more difficult yet, there are relatively few experienced attorneys capable of helping clients properly address these issues.

What are businesses to do? What should we do as attorneys for our clients and our own law firms? Here is a pragmatist’s solution.

Rise Above Regulatory Turmoil
Just a couple of years ago, far fewer regulations existed addressing information privacy and security, and the ones that existed typically governed niches, like HIPAA for health care and FERPA for public schools. Expansion began when a number of states — following the lead of Massachusetts — adopted laws requiring businesses to conduct risk assessments and implement safeguards to prevent the loss and theft of certain personal information. Those regulations extend territorially to all businesses that possess such information about residents of those states. Adding to that growing list of security statutes, states began enacting privacy laws, which afford individuals rights with respect to specific categories of information, like biometric and financial data; medical information; and biometric and financial data; and transactional records.

The movement gained momentum in 2018 with the implementation of a broad privacy law in the European Union called the General Data Protection Regulation (or GDPR), and its extension into Great Britain. GDPR applies to United States businesses that are not based in the United States but that have employees in Europe, furnish goods or services to European residents in Europe, or sign a contract (typically at the behest of a European customer or vendor) agreeing to comply with GDPR. Not to be outdone, California recently adopted a similar privacy law that takes effect in January 2020, called the California Consumer Privacy Act (or CCPA), and comparable legislation is pending in several other states.

Unlike prior privacy regulations, GDPR and CCPA are not limited to specific categories of information, but instead encompass broad swaths of personal information, including simply an individual’s name, address, email, etc. These laws also extend extra-territorially, requiring businesses that possess information about residents of those jurisdictions to provide notice and (in some situations) obtain consent from individuals when gathering and before using protected information about them.

The regulations also grant individuals certain rights with respect to such information, like the right to limit a business’ use of their information, obtain a copy of it from the business, require the business to provide it to another business, and mandate that the business erase all information about them, known as the “right to be forgotten.”

Privacy and security laws differ greatly with respect to the information regulated, individuals protected, and obligations imposed on businesses. It is impractical (if not impossible) for organizations to differentiate between the varied rules that apply to the different information they have about numerous individuals. Organizations simply to not retain or use information in such a rigidly categorical way. As a result, business leaders often opt for a more pragmatic approach, by applying industry accepted processes.

Top Tips

“...It is common for businesses engaging in this process for the first time to need several years to address the issues identified in the report. That is ok, because the basic principle of information privacy and security is not that businesses must be perfect or impenetrable, but rather better — with privacy procedures and security safeguards reasonably tailored to the resources of the organization and the magnitude of the risks.”
— Cameron Shilling

“Normal email is not encrypted, which means it can be intercepted by a third party and read. Emails are not inherently protected during transmission or during storage.”
— Jason Sgro

“[In Advisory Opinion #2012-13/4, the New Hampshire Bar Association Ethics Committee stated that] ‘competent lawyers must have a basic understanding of the technologies they use’ and stay abreast of changes, including privacy laws and regulations.”
— Lisa Thompson

“The challenge is that security is not a tool and it’s not an initiative. It’s an ongoing, holistic discipline. And that requires change. Change is never easy. And effective change must always be led.”
— Ryan Barton

“Most meaningful information security breaches will spark the interest of local or regional news outlets and politicians. Preparing astute press releases, informative company web pages, turn-key media inquiries, and legal experts to respond to ‘frequently asked questions’ are crucial steps to prepare for and preempt media inquiries.”
— P. Bill Cheng & John F. Weaver

SOLUTION continued on page VII
Let’s Talk About Email

By Jason Sgro

In today’s world, cybersecurity isn’t just the practice of protecting your client’s confidentiality, it’s also about protecting your name, your future, and your firm. The client relationship is one based on trust — and not just any trust — trust with some of the most sensitive discussions of your client’s lives. The work we do at ATOM protects our clients as well as the public trust in the technology we use to keep us safe and get our jobs done. Cybersecurity isn’t just about technical implementation, though; it’s about organizational behavior. It’s about striking a balance between convenience and responsibility, between productivity and risk.

At ATOM, www.theatomgroup.com, located in Portsmouth, NH, we believe in helping leaders build a future we can trust. For our legal and law firm clients, that future is most jeopardized by data sharing and storage. Today, we’d like to take a moment to discuss how to share data internally and externally, protect data while you’re on the go, and understand how your clients are most often breached.

First, we need to talk about email. It’s very common for documents of a sensitive nature to be shared via email with clients, colleagues, and third parties. This is not a good practice because email has a few major flaws. The first flaw is that it isn’t traceable. You send an email with a sensitive attachment and you don’t really know where it went. Yes, it goes to the mailbox of the recipient — but is that mailbox accessed on a laptop, a cellphone, a public computer? What if the cellphone is lost? The data is lost with it. Remember, too, it’s not just the recipient’s mailbox. It’s your mailbox, too. Your sent items are on your laptop, cellphone, and tablet as well. If your devices are lost, copies of those sensitive emails are lost, too.

The second issue with email I’d like to discuss is more fundamental: it’s a lack of encryption. Normal email is not encrypted, which means it can be intercepted by a third party and read. Emails are not inherently protected during transmission or during storage. Think about sending your physical mail items in clear see through mailers. Not ideal, right? You have no way of knowing who saw it when it was on its way to the recipient.

At ATOM, we recommend the following actions be taken as a best practice when sending or receiving sensitive data.

1. Don’t use email to send sensitive data. Use an application designed for it. We use a Citrix product called Sharefile (www.sharefile.com). It’s not expensive and provides encrypted transport and storage of files so you can easily reference them and use them without having them in your insecure email.

2. Keep a strong password on your email account (generally 10 characters or more) with one number, one capital letter, and one special character. We often recommend using a longer password (like a sentence — space characters are allowed!) so it is easy to remember but also very secure. Length beats complexity when it comes to security.

3. Turn on encryption on your laptop drive. If you have a PC or a Mac, most have built-in encryption technologies. Windows 10 has an application called Bitlocker (https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption) and Mac OS X has an application called Filevault (https://support.apple.com/en-us/HT204837). They are both free, built-in encryption programs that encrypt all of the data on your laptop so that if you lose it, nobody can read the data.

4. Keep as little data on your cellphone and tablet as possible. Most email clients and applications will allow you to download only the last two weeks’ worth of email and data on those devices. This is convenient for current communications, but you will have to go to your laptop or desktop for full history. Storing massive historical data on your easy-to-lose cellphone is not a best practice. In fact, cellphones are the number one method of breach of sensitive data for ATOM legal clients between 2018 and 2019.

5. Safely archive old files. Having all of your working data accessible to you is important, but having all the data from years past is a risk. We highly recommend moving archived data to offline storage, and, at the very least, doing a monthly cleanup of your computer and cellphone to remove any unneeded files.

Data hygiene is a great way to protect your name, your future, and your firm. The work we do at ATOM protects our clients as well as the public trust in the technology we use to keep us safe and get our jobs done. Cybersecurity isn’t just about technical implementation, though; it’s about organizational behavior. It’s about striking a balance between convenience and responsibility, between productivity and risk.

6. Perform a data risk assessment and external penetration test every year. These two assessments help you identify gaps in your security and make remediations on an ongoing basis. While these are just a few of the recommended controls we help clients put into place, we hope you have found these tips useful. If you have any questions about cybersecurity or specific behaviors in your organization, we’re always happy to discuss.

Jason Sgro is a Sr. Partner at ATOM and Sr. Advisor to the NH State Legislature. With over 20 years in start-ups to fortune 500 companies, he has dedicated his career to helping leaders in healthcare, legal, financial, and emerging technologies build a future we can trust.

McLane Middleton’s Privacy and Information Security team assists clients throughout the region with the mitigation of information privacy and security risks. Services include:

• Privileged information privacy and security risk assessments and reports
• Due diligence and contract negotiations with vendors and third parties
• Immediate and effective breach management and remediation
• Compliance with information privacy laws from other jurisdictions, including the California Consumer Privacy Act, the European Union GDPR, and the Canadian PIPEDA

McLane Middleton: Manchester | Concord | Portsmouth
Massachusetts: Woburn | Boston

McLane.com

*admitted in MA and FL only
Cybersecurity Best Practices for Lawyers and Law Firms

By Lisa N. Thompson

Technology is profoundly transforming the practice of law—not only how lawyers’ practice but where they practice. The automation of tasks such as billing, document management and legal research have provided significant savings in time and resources. Moreover, cloud-computing and mobile devices have given lawyers the flexibility to access information anytime, from multiple devices and from any location. While technological innovation has allowed lawyers to practice more effectively and efficiently, it has also created new threats to the confidentiality of client information. Law firms possess a plethora of confidential information, which makes them prime targets for hackers.

As large-scale data breaches continue to make headlines, law firms and lawyers must be proactive, not reactive, about cybersecurity to keep pace with the constantly evolving threats and tactics of cybercriminals. Lawyers tend to be technology-adverse and law firms often lack the resources and IT staff to implement organizational safeguards to protect themselves from the ever-increasing risk of a cyberattack. A data breach can have major implications and the costs of a law firm can be high, from the intangible effects on a law firm’s reputation and client trust, to the tangible costs of business interruption, breach notification, lawsuits, and regulatory fines. The bottom line is that to stay competitive in the digital economy, lawyers must proactively pursue technological competence.

In addition, many corporate clients, especially those in regulated industries, are subject to federal privacy regulations, such as HIPAA, GLBA, FINRA, FCRA or SOX, which require organizations to employ security safeguards to protect confidential information from loss, theft and unauthorized access. The risks associated with violating these regulations can be severe. As a result, many corporate clients are demanding that law firms have detailed cybersecurity policies and procedures in place, and some may even require that a law firm pass a security audit as a condition of engaging the firm. Furthermore, pursuant to Rules 1.1 and 1.6 of the New Hampshire Rules of Professional Conduct, law firms have an ethical obligation to protect confidential client information and must take reasonable efforts to prevent unauthorized access or disclosure of client information. Additionally, both the New Hampshire Rules and ABA Model Rules impose a duty on lawyers to maintain technological competence. For example, in Advisory Opinion #2012-13/4, the New Hampshire Bar Association Ethics Committee stated that “competent lawyers must have a basic understanding of the technologies they use” and stay abreast of changes, including privacy laws and regulations.

Cybersecurity encompasses education, processes, standards and technology to protect confidentiality, privacy, data, and reputations. Lawyers must proactively pursue best cybersecurity practices. This work outlines key challenges, potential solutions, and practical guidance for promoting and practicing cybersecurity.

Password Policy

One of the most important steps a law firm can take to prevent a data breach is establishing and enforcing a password policy for all firm employees. Employees should create unique hard-to-guess passwords for each account, computer, or mobile device, with at least 10 characters, containing a mix of upper- and lowercase letters, numbers and symbols. The same or similar passwords should never be used for different accounts.

Leading Change: Creating a Culture of Cybersecurity at Your Firm

By Ryan Barton

We all know we need to do more to address cybersecurity threats.

Most of us have a sense of why — we are connecting more devices that can hacked, generating more data, and living on a global Internet that is growing by a million people per day worldwide. Adding to these risks, hackers’ skill is rapidly increasing.

We may even have a grasp of what. Access to helpful articles is mounting — including Lisa Thompson’s article, above, which outlines encryption, multi-factor authentication, policies, updates, training, and the like. Extensive resources such as the NIST Cybersecurity Framework are available free at nist.gov. There is a path to follow, and if you follow it, it largely works.

The pressing question is often: how? In the midst of the whirlwind of daily demands, resistance from corporate culture, limited budgets, and overworked IT resources, how do we actually impact security?

The challenge is that security is not a tool and it’s not an initiative. It’s an ongoing, holistic discipline. And that requires change.

Change is never easy. And effective change is rarely achieved all at once.

Our experience tells us that organizations of any size can achieve manageable cybersecurity risk. With thanks to John Kotter, author of the seminal book, “Leading Change,” the following steps can guide an organization through the hard business of actually making themselves more secure:

1. Establish a sense of urgency.

2. Create your team.
   Change cannot be addressed alone. We recommend that cybersecurity risk is managed and reported on the board/partner level, the same as financial or legal risk. Leaders within the organization need to be on the same page about the reality of this risk, and have the wisdom to mitigate it.

3. Develop vision and strategy.
   The team must expand to include experts in information security (organization-wide practices) and expertise in IT security (technical controls). Assess your organization and its current partners: Do you have the depth of expertise and availability that gives you confidence? Do you have both information security and IT security competence in enough degrees, or at least have staff with the time, commitment, and attention to detail to learn all they need? If not, engage with those who have the experience and knowledge to work with you through this. Keep in mind: this is not an IT responsibility. IT plays an important part but asking IT to lead Information Security rarely works. Firms are successful because effective management, IT, and Information Security are engaged together.

4. Communicate the change vision.
   Communicate with shareholders, managers, and the full team. Emphasize the why, explain the what, and guide them through the how. Our experience is that employees are quick to adopt new security practices with not just training, but context. Develop a team-wide understanding of the actual risks, the potential impact to each individual and the firm, and the current vulnerability behavior is likely.

5. Budget separately.
   Information Security costs should not go in the “IT” budget line item. In large organizations, the Information Security & Compliance department is a separate team, with separate responsibilities and budget. This methodology is wise, regardless of firm size. Create a separate line item for Information Security. It is a new risk, and it will require new costs to overcome.

CULTURE continued on page V
The Art of Managing a Cyber Security Breach

By P. Bill Cheng and John F. Weaver

A cyber security breach can be terrifying for any company. Most business leaders and attorneys lack experience with this type of crisis, and few companies have prepared or practiced incident response procedures before a breach occurs. Complicating the situation is the fact that no foolproof playbook for handling a cyber security breach, and doing so well is more art than science. Each breach response must be tailored to a multiplicity of variables (such as the specific business involved, information compromised, number and type of individuals affected, governmental regulatory agencies interested, local political and media climate, etc.), bringing to bear both skills and intuition developed from experience handling cyber breaches.

The response to an actual or potential breach must be instantaneous — action must be taken within hours, not days. It is imperative for the business to immediately retain an experienced cyber security attorney, in order to secure the protections of the attorney-client communication and work-product privileges throughout the breach response.

One of the immediate tasks in breach response is to determine if the business has an applicable insurance policy and, if so, the scope of coverage. Insurance for a breach of information differs from coverage for cyber financial theft, and carriers oftentimes can be persuaded (with the right leverage) to pay for the costs of breach investigation even if the policy may not cover the underlying liability. Navigating the shoals of insurance is additionally risky, since securing coverage may require developing evidence that a breach occurred, whereas such evidence may be harmful with respect to the business’ rights and obligations vis-à-vis the individuals affected, governmental regulators, customers, vendors, and other third parties.

Retaining a qualified technology expert may be another immediate first step in the breach response process, if the circumstances warrant such forensic examination. If so, it is critical that an experienced information security attorney retains and directs the expert, to ensure that the forensic examiner’s report and any measures taken to mitigate the breach remain privileged (particularly if the review reveals that the business failed to take reasonable measure to avoid the breach).

Depending on the type of breach, immediate forensic work may be imperative to ensure the preservation of key evidence, like server and operating system log files. Prompt and accurate initial communications with the company’s board and bank customers and vendors, and regulators, as necessary, is another important early step in breach response process. While these communications are important to ensure that the later steps in the process proceed smoothly, information provided to them may or may not remain confidential, can facilitate either assistance or resistance from others, and will result in either a nasty and expensive governmental audit or avoid a regulatory response altogether.

Most meaningful information security breaches will spark the interest of local or regional news outlets and politicians. Preparing astute press releases, informative company web pages, turn-key media interviews, thoughtful telephone scripts, and thorough answers to “frequently asked questions” are crucial steps to prepare for and preempt media inquiries. Similarly, forerunning with likely interested political figures can convert potential antagonists into allies.

The most important aspect of the response is prompt notification to the individuals affected by the breach, and positive interactions with them thereafter. While no one is happy to learn that his or her personal information was lost or stolen, a cyber breach is a problem that a business can transform into an opportunity. A call/email center staffed by knowledgeable and (actually) helpful representatives is imperative.

Similarly, if the breach involves sensitive personal information, offering credit and identity restoration insurance (not just monitoring) to the affected individuals can mitigate or prevent harm to them entirely. In fact, an effective breach response can significantly reduce, if not completely eliminate, the risk and damages of lawsuits and claims asserted by affected individuals.

Cyber security breaches are terrifying primarily because most businesses are not ready for them. Preparing and practicing incident response procedures before a breach occurs is imperative. Likewise, if a subject to a breach, a business should retain an experienced information security attorney to manage a privileged breach response process, bringing to bear the skills and intuition that is developed only from handling these crises.

Bill Cheng and John Weaver practice in the Privacy and Data Security Group at McLane Middleton. Cheng can be reached at bill.cheng@mclane.com at 781-904-2715. Weaver can be reached at john.weaver@mclane.com or at 781-904-2683.

The New Hampshire Bar News will launch a regular column devoted to cybersecurity and information privacy. Stay tuned to find out more or contact news@nhbar.org to contribute.

Culture

6. Generate immediate wins.

Once you have your urgency, team, vision, culture, and resources in alignment, you are primed to generate quick-wins. Many high impact security layers take very little time. In the first one to three months, expect meaningful risk reduction and change in the culture. Identify clear and easily identified measures that convey momentum and track progress.

7. Transition to ongoing governance and produce more change.

After the first three months, move into an “ongoing governance” model, generate a multi-year plan, and track progress. Gather the team every three months, or perhaps more often at the outset, and review both current controls and progress towards the ideal.

8. Anchor security in your culture.

With the full support of all managers and employees to anchor and evolve security in the culture. Ensure new processes are being followed and reward good security behavior. If you have a Human Resources team, work with them on screening, training, expectations, and disciplinary actions. Evolve the training program every year and talk about security at all staff meetings. Integrate good security deeply with your culture in as many rhythms and communication methods as you can.

With the news of breaches making headlines, it can be easy to feel like cybersecurity is a hopeless battle — it isn’t. While no one is invulnerable, effective change leadership can turn cybersecurity into a managed risk that’s just another part of the business and culture.

It’s a change that must be led but is well worth the effort.

Ryan Barton is the founder and CEO of Mainstay Technologies. Mainstay provides IT and Information Security services to organizations throughout northern New England, with a focus on both deep expertise and on warm personal relationships. Mainstay follows the tenets of Conscious Capitalism and measures success by the degree it strengthens its clients, team, company, community, vendors, and environment. It has received multiple awards as a company, including Best Companies to Work For, Business of the Year, Business Excellence, and the Torch Award for Marketplace Ethics. Barton is a devoted husband, father of three (ages 2, 3, and 4), and an insatiable reader.
and mobile devices. Encryption is a way to keep law firm data and network systems secure.

Multi-factor Authentication
Since passwords are easy to crack, a password alone is not enough to protect firm network systems from unauthorized access. Implementing multi-factor authentication is an easy way to keep law firm data and network systems secure.

Multi-factor authentication is a security enhancement that requires a user to supply additional information besides just a username and password before being allowed to login to an account or gain access to a network system. Even if a password is cracked or stolen, access is thwarted because of multi-factor authentication. In order for the authentication to be complete, a user must enter their login/password and when prompted provide a passcode or security code, usually a temporary code sent by email or text (it can also be a fingerprint) to gain access.

Multi-factor authentication is highly recommended whenever employees request remote access to firm networks and systems. While many apps and programs such as Office 365 already support multi-factor authentication, it is important not to overlook law practice management programs and other critical software programs that manage calendars, contacts, emails, etc. Law firms can install multi-factor authentication apps such as Google Authenticator, Microsoft Authenticator, or Salesforce Authenticator, or hire third-party vendors such as Duo Security or Pin2ID that offer cloud-based multi-factor authentication services.

Encryption
Law firms routinely use laptops, USB drives and mobile devices to store and transmit sensitive data through e-mail, instant messaging, and other forms of digital communication. Lost or stolen laptops, USB drives and mobile devices that contain unencrypted data are a main cause of data breaches. While a password can prevent someone from logging into a lost or stolen laptop or mobile device, other means can be used to access and copy stored files and data. Encryption is an easy way to safeguard against unauthorized access to confidential data breaches when a laptop, USB drive or mobile device is lost or stolen. Newer desktop computers, laptops and mobile devices come with operating systems that offer ways to fully encrypt stored data.

Stay Current with Updates
 Routinely installing security updates as soon as they are released is an essential component to any cybersecurity program. Cybercriminals are constantly scanning for security vulnerabilities to exploit so that they can gain access to valuable law firm data. Law firms that do not regularly install all security updates on all devices, hardware and applications (e.g., antivirus software, browsers, desktop computers, laptops, mobile devices, operating systems, printers, routers, etc.) are vulnerable to attack.

It only takes a single computer or device to be compromised to bring down an entire organization’s computer network or system. In order to protect their entire network, law firms need to implement a comprehensive incident response plan. An incident response plan is a plan that law firms can use to recover operations in the event of an on-premise or offsite disaster. An incident response plan is critical to prepare for and respond to cyber incidents.

Vendor Security
Most law firms rely on third-party service providers and other vendors for a wide range of services. Unfortunately, the cybersecurity practices of vendors are often overlooked when firms outsource. Outsourcing can pose a major cybersecurity risk to a firm since it exposes the firm to an extension of the firm. Firms must diligently assess, identify and manage risks and liabilities whenever they engage third-parties that have access to confidential client information.

Pursuant to N.H. Rule 5.3, lawyers have a duty to supervise the work and conduct of non-lawyers ensuring the work is delegated to “competent people and organizations” and performed in a manner consistent with the lawyer’s professional responsibilities. For example, Advisory Opinion #2012-13/4 noted that cloud computing is a form of outsourcing and that lawyers are responsible for reasonably ensuring that sensitive client information held or stored by others e.g., cloud computing service providers, is adequately protected and remains confidential and secure. Law firms should routinely conduct risk management reviews and vet all third-parties that have access to any confidential data and that interact with firm networks, verifying that they are capable of ensuring effective and complying with the same data security standards that the firm does.

Firms should impose contractual obligations on vendors, requiring compliance with all data security laws as well as law firm obligations, prompt reporting of potential cyber incidents, cooperation in investigating an incident and preserving relevant evidence, etc. Advisory Opinion #2012-13/4 also provides a list of issues which lawyers must consider before using a cloud computing service provider, including assessing the provider’s reputation and security measures, etc. As part of their ongoing third-party due diligence, law firms should evaluate vendors for compliance and risk on an annual basis.

Incident Response Plan
In addition to educating employees and establishing policies to prevent cyberattacks, law firms should develop a comprehensive incident response plan to maintain business continuity in the event of a cyberattack or other disaster. An incident response plan should be a document that is updated annually to ensure that it can be implemented to ensure that, if there is a cyberattack or breach, the firm can respond quickly and effectively to limit any damages.

Vendor Security
Most law firms rely on third-party service providers and other vendors for a wide range of services. Unfortunately, the cybersecurity practices of vendors are often overlooked when firms outsource. Outsourcing can pose a major cybersecurity risk to a firm since it exposes the firm to an extension of the firm. Firms must diligently assess, identify and manage risks and liabilities whenever they engage third-parties that have access to confidential client information.

Pursuant to N.H. Rule 5.3, lawyers have a duty to supervise the work and conduct of non-lawyers ensuring the work is delegated to “competent people and organizations” and performed in a manner consistent with the lawyer’s professional responsibilities. For example, Advisory Opinion #2012-13/4 noted that cloud computing is a form of outsourcing and that lawyers are responsible for reasonably ensuring that sensitive client information held or stored by others e.g., cloud computing service providers, is adequately protected and remains confidential and secure. Law firms should routinely conduct risk management reviews and vet all third-parties that have access to any confidential data and that interact with firm networks, verifying that they are capable of ensuring effective and complying with the same data security standards that the firm does.

Firms should impose contractual obligations on vendors, requiring compliance with all data security laws as well as law firm obligations, prompt reporting of potential cyber incidents, cooperation in investigating an incident and preserving relevant evidence, etc. Advisory Opinion #2012-13/4 also provides a list of issues which lawyers must consider before using a cloud computing service provider, including assessing the provider’s reputation and security measures, etc. As part of their ongoing third-party due diligence, law firms should evaluate vendors for compliance and risk on an annual basis.

Incident Response Plan
In addition to educating employees and establishing policies to prevent cyberattacks, law firms should develop a comprehensive incident response plan to maintain business continuity in the event of a cyberattack or other disaster. An incident response plan should be a document that is updated annually to ensure that it can be implemented to ensure that, if there is a cyberattack or breach, the firm can respond quickly and effectively to limit any damages.

The first step in developing an incident response plan is conducting a risk assessment to identify current firm vulnerabilities. If a firm cannot identify its cybersecurity vulnerabilities it cannot expect to effectively defend against them. The National Institute of
Standards and Technology (NIST) has created a voluntary Cybersecurity Framework that consists of guidelines and recommended practices to manage data security risk. Firms should consider using resources like the NIST cybersecurity framework when developing an incident response plan. For example, Formal Opinion 483 also provides that lawyers should “consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach. The decision whether to adopt a plan, the content of any plan and actions taken to train and prepare for implementation of the plan should be made before a lawyer is swept up in an actual breach.”

An incident response plan is a set of procedures designed to identify, investigate and respond to a cybersecurity incident in a way that reduces the impact and in what order an incident, to limit damage and minimize recovery time. Important elements of an incident response plan include identification of the cause of the incident, assessing what data was compromised, contact information for internal resources, notifying affected parties and outside organizations, contact information for pre-approved external resources (e.g., professional liability or cyber insurance carriers) and evaluating weaknesses to avoid future incidents. It is also recommended that firms test their incident response plan annually.

Additionally, Formal Opinion 483 provides that “lawyers must notify current clients of a data breach before lawyers update them on the findings of any investigations into that breach. This is important for lawyers to evaluate and address all reporting requirements under federal and state laws, agreements, and any ethical obligation to report breaches under the Rules. For example, New Hampshire’s data breach notification law requires that notice be provided to individuals whose personal information was compromised by any security breach of unencrypted computerized data. See NH RSA 359-C:20. Additionally, New Hampshire firms doing business with residents in other states must be aware of the specific data breach notification laws applicable to those states.”

Cyber Insurance

As cyberattacks become more sophisticated, despite preparation and employee training, firms’ networks and systems can be compromised, and personal information was compromised by unsecured vulnerabilities. However, one way that firms can offset some of the risks and limit their exposure is through cyber insurance or cybersecurity insurance.

It is important to note that cyber insurance is intended to complement, not replace, a law firm’s cybersecurity risk management program. Furthermore, cyber insurance will not remove the threat of a cyberattack, but it can help cover the costs arising from a data breach. Most cyber policies can be customized based on budget and need, covering costs up to predetermined limits including breach notification, regulatory fines, forensics, legal fees, and other expenses. As with other types of insurance, cyber policies often contain a variety of exclusions buried in the policy that can limit coverage. It is important to pay attention to whether the firm is in full compliance with the requirements of its cyber insurance policy and carefully evaluate all exclusions. For example, if employees use personal devices to access firm data, the policy will only cover the firm if it can prove that it had sufficient controls in place to prevent unauthorized access.

Conclusion

As lawyers and law firms leverage new technologies, it is critical to understand not only the new security risks that go with them but the ethical and legal obligations as well. Cybersecurity is not something that a law firm does once and then is done, rather it is a permanent state of vigilance. Cyberattacks are becoming more sophisticated, lawyers should look at cybersecurity as the new normal. Lawyers and law firms must continuously update their defenses based on the latest developments in technology and current cyberthreat trends — as technology evolves so should law firm cybersecurity.
Are You Taking Full Advantage of Your Bar Association Membership?

MEMBER SERVICES

Affordable, local CLE seminars
Convenient CLE formats, including live, online, webinar and podcasts
Dispute Resolution (Mediation/Arbitration Service)
Ethics Guidance
HeinOnline Archive of Bar News and Bar Journal
Law Office Backup Designation Form
Lawyer Referral Service

NEW - TechConnect
Legislation Watch NH bill tracking website
Member ID cards
Modest Means Referral Service
NHBA e-Bulletin newsletter
NH Bar News monthly member newspaper
Online membership directory
Pro Bono Referral Program
SOLACE Support Network

BENEFITS & DISCOUNTS

ABA Retirement Program
Casemaker (updated) - subscription access for members fully sponsored by Bar
Clio – 10% lifetime discount
ESQSites website services – 25% discount off set-up fees

FREE conference and meeting space
LawPay – 3-month free trial
MyCase – 10% lifetime discount on monthly fees
NHBA•CLE Club Discount
Sections and email lists

Our Job Is To Support You To learn more about how to make the most of your NH Bar Association membership features, check out the Upcoming Events column and Resources tab on NHBA website. Logging into your MyNHBar portal also provides information exclusive for members. Questions? Contact memberservices@nhbar.org.

The NH Bar Center is located at 2 Pillsbury St., Suite 300, Concord, NH 03301
www.nhbar.org • (603) 224-6942 • Member Hotline: (603) 715-3279

KEEP UP WITH NH BAR ONLINE
facebook.com/NHBar
@NHBar
linkedin.com/company/new-hampshire-bar-association