dri™ The Voice of the Defense Bar

Data and Security Dispatch

The newsletter of the
Cybersecurity and Data Privacy Committee

10/04/2018 Volume 4, Issue 2

Committee Leadership

Chair
James H. Kallianis, Jr.
Hinshaw & Culbertson LLP
Chicago, Ill

Vice Chair
Alexander E. Potente
Clyde & Co US LLP
San Francisco, CA

Publications Chair/Newsletter Editors

Heyward Dodkin Bonyata
Nelson Mullins Riley & Scarborough
Columbia, SC

Wendy B. Degerman
Nelson Mullins Riley & Scarborough
Columbia, SC

Click here to view entire Leadership

In This Issue

Leadership Note

From the Chairs 2

Feature Articles

SEC Provides 35 Million Reasons to Focus on Cybersecurity Disclosures 2

Managing Your Law Firm as a Business

Mitigating the Cost of Data Breach 5

Leadership Note

From the Chairs

By James H. Kallianis, Jr., and Alexander E. Potente


If you're not frightened yet, you will be! The two terrific articles in the summer installment of the *Data and Security Dispatch* describe the potentially dire consequences of suffering a data breach or being the target of a cyberattack. Fortunately, the authors also provide you with the means to avoid or, at least, reduce the risk of an attack and explain what must be done in the event you or your client suffers a breach or other cybersecurity incident. We again want to thank Heyward and Wendy for their dedication to producing a terrific publication. Both articles also reinforce the importance of attending our Cybersecurity and Data Privacy Seminar on September 5–7 in Chicago. This year the seminar kicks off with a special DRI Tech Summit on the afternoon of September 5 that addresses some of the most important technology issues facing lawyers today, including cloud computing, artificial intelligence, and law firm security. We look forward to seeing everyone in Chicago in September.

Jim and Alex

James H. Kallianis, Jr., is a partner at Hinshaw & Culbertson LLP in Chicago. Among his areas of specialty is representing insurers in matters involving directors and officers, cyber, employment practices, general liability and professional liability policies. He currently chairs DRI's Cybersecurity and Data Privacy Committee.

Alexander E. (Alex) Potente, a partner of Clyde & Co US LLP in Cleveland, is an experienced trial lawyer who represents insurers in complex commercial insurance litigation matters including disputes pertaining to general liability and professional liability policies, with an emphasis on bad faith litigation and coverage issues arising from claims involving class actions, product defects, public sector liability and environmental and other long-tail insurance coverage disputes. Alex currently is the vice chair of DRI's Cybersecurity and Data Privacy Committee.

Feature Articles

SEC Provides 35 Million Reasons to Focus on Cybersecurity Disclosures

By Eric McKeown, Stephen Hackman, and Stephen Reynolds



In February 2018, the Securities and Exchange Commission (the "SEC" or "Commission") issued updated interpretative guidance (the "Guidance") stressing the importance of cybersecurity-related disclosures by public companies. SEC, Commission Statement and Guidance on Public Company Cybersecurity 5-6 (2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf. The Guidance "provides the Commission's views about public companies' disclosure obligations under existing laws" and warns that companies may run afoul of those obligations if they fail to promptly disclose material cybersecurity risks and incidents, such as significant data breaches. (The Guidance significantly updated the SEC's prior 2011 guidance regarding the disclosure of material cybersecurity risks and incidents, including data breaches. *See* SEC, SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018), https://www.sec.gov/news/press-release/2018-22.) The Guidance also outlines a variety of factors that companies should consider in assessing the materiality of cybersecurity risks and incidents.

The SEC's increased focus on this issue was highlighted by the recently announced settled enforcement action imposing a $35 million penalty against the entity formerly known as Yahoo! Inc. (the "Yahoo Settlement"). SEC, Altaba, Formerly Known as Yahoo!, Charged with Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million (Apr. 25, 2018), https://www.sec.gov/news/press-release/2018-71. The SEC's enforcement action against Yahoo, which arose

from a 2014 data breach involving the compromise of hundreds of millions of user accounts, was the first of its kind against a company based on failure to properly disclose a cybersecurity incident. The SEC investigation of Yahoo was conducted by the Cyber Unit of the SEC's Enforcement Division, which was created in September 2017 to focus on cybersecurity enforcement matters. SEC, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors (Sept. 25, 2017), https://www.sec.gov/news/press-release/2017-176.

In light of this increased focus on cybersecurity by the SEC, the Guidance offers key insights for companies in determining what sort of cybersecurity disclosures are required, whether in periodic reports, registration statements, or current reports. In addition, the Guidance encourages companies to maintain comprehensive internal policies and procedures related to cybersecurity risks and incidents. Finally, the Guidance reminds companies of important insider-trading considerations and their duty to refrain from making selective disclosures of material nonpublic information about cybersecurity risks and incidents.

Importance of Cybersecurity Disclosures

The Guidance explains that cybersecurity disclosures have grown in importance as the frequency and magnitude of cybersecurity incidents have increased in recent years. Companies now face a wide range of cybersecurity threats on a daily basis, including stolen access credentials, malware, ransomware, phishing, and other types of attacks, which can be perpetrated by both third parties and malicious insiders. Guidance at 2–3. Moreover, cybersecurity incidents often result in substantial costs and other negative consequences for companies, including, among other things, (i) remediation costs, (ii) increased cybersecurity protection costs, (iii) lost revenues from stolen proprietary information and/or customer losses, (iv) increased insurance premiums, (v) reputational damage, and (vi) litigation and legal risks. Guidance at 3–4.

In light of the increase in the frequency, magnitude, and cost of cybersecurity incidents, the Guidance explains, it is important for public companies to "take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion." Guidance at 4. Such disclosures may be required in:

- *Periodic reports*, including both annual reports on Form 10-K and quarterly reports on Form 10-Q, where "[c]ompanies must provide timely and ongoing information . . . regarding cybersecurity risks and incidents that trigger disclosure obligations,"
- *Registration statements* under the Securities Act of 1933 and the Securities Exchange Act of 1934, as such statements "must disclose all material facts required to be stated therein or necessary to make the statements therein not misleading," and
- *Current reports*, including current reports on Form 8-K or Form 6-K, which the Guidance encourages companies to use "to disclose material information promptly, including disclosure pertaining to cybersecurity matters."

Cybersecurity Disclosures and Materiality

The Guidance further explains that cybersecurity risks and incidents should be evaluated using the general standard for materiality—whether "there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision." Guidance at 10 & n. 32 (citing *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976)). Thus, the materiality of cybersecurity risks or incidents "depends upon their nature, extent, and potential magnitude," which requires consideration of the type of compromised information and its relationship to the company's business.

For example, the Guidance explains, the materiality of a compromise involving personally identifiable information (PII) depends on both the nature of a company's business and the scope of the compromised information. Guidance at 11 & n. 33. The same would be true for a compromise involving trade secrets or confidential business information. Presumably, such an event would be more likely to be material if the company's business model and/or reputation were dependent on safeguarding customers' PII and if the scope of the compromise were significant.

In evaluating materiality, the Guidance advises, companies should also consider the range of potential harms that could result from a cybersecurity incident. Such harms may include, among other things:

- Reputational harm;
- Impact on financial performance;
- Relationships with customers and/or vendors; and
- Potential litigation or regulatory investigations.

Guidance at 11.

Critically, material cybersecurity incidents, such as significant data breaches, may require prompt disclosure in order to ensure that prior disclosures do not become materially misleading. Indeed, the Guidance emphasizes that companies may have a duty to (i) correct a prior disclosure that the company determines was untrue, or omitted a

material fact necessary to make the disclosure not materially misleading, at the time it was made, or (ii) update disclosure that has become materially inaccurate after it was made. Guidance at 12, although the Commission notes the current disagreement among several Federal Circuits with respect to the duty to update prior disclosures as a result of subsequent events. See Guidance footnote 37. Therefore, when investigating a cybersecurity incident, such as a significant data breach, companies should carefully consider whether updates to prior disclosures are required. *Id.*

Internal Policies and Procedures

The Guidance further encourages companies to assess the adequacy of their internal disclosure controls and procedures to properly process and report cybersecurity incidents. Guidance at 18–19. Under Exchange Act Rules 13a-15 and 15d-15, companies must maintain and evaluate the effectiveness of their disclosure controls and procedures. *See id.* Such controls and procedures should provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents. Guidance at 4.

Moreover, the Guidance advises that disclosure controls and procedures are most likely to be effective when a company's leaders, including directors and officers, are promptly informed about cybersecurity risk and incidents. *Id.* Accordingly, disclosure controls and procedures should ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications. *Id.* at 18. This requires open communications between technical experts and disclosure advisors to ensure that timely and appropriate disclosures take place. *Id.* at 20.

Insider Trading, Regulation FD, and Selective Disclosure

The Guidance further advises that companies and their directors, officers, and other corporate insiders should be mindful of insider trading risks in connection with cybersecurity risks and incidents. *Id.* at 21. Information about a company's cybersecurity risks and incidents may constitute material nonpublic information, triggering the risk of insider trading. Accordingly, companies should consider implementing measures to guard against the risk of corporate insiders trading on the basis of material nonpublic information during the time period between the discovery of a cybersecurity incident and public disclosure of such an incident. Guidance at 5. This may require companies to update their codes of ethics and insider trading policies to address cybersecurity risks and incidents. *Id.* at 21–22. In short, the Commission states that "companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure." *Id.* at 22.

Related to the previous recommendation, the Guidance encourages companies to promote full and fair disclosures via compliance with Regulation FD. *Id.* at 22–24. This regulation tackles the issue of companies making selective disclosures of material nonpublic information to certain investors prior to making the information known to the general public. The Guidance advises companies to avoid making selective disclosures in connection with cybersecurity risks and incidents, and further reiterates that the Commission expects companies to have policies and procedures in place to ensure selective disclosures are prevented. *Id.*

The *Yahoo* Settlement

The importance of prompt disclosure is illustrated by the SEC's settled enforcement action against Yahoo. SEC, Order Instituting Cease-and-Desist Proceedings, *In re Altaba, Inc., f/d/b/a Yahoo! Inc.* (Apr. 24, 2018), https://www.sec.gov/litigation/admin/2018/33-10485.pdf. The SEC charged Yahoo with misleading investors under the federal securities laws by failing to timely disclose a December 2014 data breach (the "Breach") that compromised hundreds of millions of user accounts. This information included what Yahoo's information security team referred to internally as "the company's 'crown jewels': usernames, email addresses, phone numbers, birthdates, encrypted passwords, and security questions and answers for hundreds of millions of user accounts." SEC, *Altaba, Formerly Known as Yahoo!, Charged with Failing to Disclose Massive Cybersecurity Breach: Agrees to Pay $35 Million* (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71.

According to the settled administrative order—the allegations of which Yahoo neither admitted nor denied—although Yahoo's information security team learned of the Breach within days of its occurrence, and although the Breach was reported to members of Yahoo's senior management and legal department, the company failed to disclose the Breach for more than two years. *Id.* Moreover, according to the order, the company did not property investigate the circumstances of the breach, nor did it adequately consider whether disclosure to investors was required. *Id.*

The SEC found that Yahoo, among other things: (i) failed to disclose the data breach or its potential impact in quarterly and annual reports for more than two years, (ii) failed to properly assess the company's disclosure obligations by sharing information about the breach with auditors and/or outside counsel, and (iii) failed to maintain disclosure controls and procedures designed to ensure that internal reports of data breaches were properly and timely assessed for potential disclosure. *Id.*

In connection with announcing the Yahoo Settlement, Steven Peikin, Co-Director of the SEC Enforcement Division, noted that the SEC does "not second-guess good faith exercises of judgment about cyber-incident disclosure." However, he warned, "a company's response to such an event could be so lacking that an enforcement action would be warranted," and this was "such a case." *Id.*

The SEC noted that in the two-year period following the Breach, the company's quarterly and annual reports never disclosed the Breach or its potential implications, but instead stated "that it faced only the risk of, and negative effects that might flow from, data breaches." *Id.* In light of the Guidance and the Yahoo Settlement, it appears that such generic disclosures are unlikely to be sufficient where a company experiences a massive data breach that compromises information integral to the company's business model. Companies may face more difficult disclosure decisions for data breaches that are smaller in scale but still carry the risk of negative business repercussions.

Conclusion

The SEC has increased its focus on companies' obligations to disclose material cybersecurity risks and incidents, and the Yahoo Settlement illustrates the risk of failure to properly disclose. In light of the Guidance and the SEC's attention to this issue, companies should carefully consider and evaluate:

- The potential materiality of cybersecurity risks and incidents in making required disclosures in registration statements, periodic reports, and current reports;
- When investigating significant cybersecurity incidents, such as data breaches, whether prompt disclosure is required;
- The adequacy of internal policies and procedures in place to ensure cybersecurity risk and incidents are promptly reported internally and evaluated for potential disclosure; and
- The adequacy of internal policies and procedures for preventing selective disclosures regarding cybersecurity risks and incidents.

Steve Hackman is a partner in the Ice Miller Business Group who regularly counsels clients regarding disclosure issues, corporate governance matters and compliance with the rules of the Securities and Exchange Commission and various stock exchanges.

Stephen Reynolds, a former computer programmer and IT Analyst, is co-chair of Ice Miller's Data Security and Privacy Practice.

Eric McKeown, a former software developer, is a member of Ice Miller's Data Security and Privacy Practice, and has extensive experience with SEC investigations. Ice Miller's Data Security & Privacy Practice helps clients assess risks and implement strong data security and privacy programs.

Managing Your Law Firm as a Business

Mitigating the Cost of Data Breach

By Darius Davenport and James Chapman


Imagine coming to work and being greeted by a sign on the door instructing you not to turn on your computer because your firm is experiencing a major data security incident. Once inside, you are told that any work that you do will have to be done manually, with pen and paper, until IT professionals rebuild all of the firm servers and computers. You have pending deadlines, but you cannot access your calendar. You start to call opposing counsel regarding a looming deadline only to discover that the phone system is also down. Your firm administrator has also collected your firm-issued cell phone because the applications on your phone must be wiped and rebuilt. At

this stage, you don't know what data has been lost, what confidential information might have been exposed, how much it will cost to restore data, how long it will take to restore the network or how much revenue will be lost while you wait.

If you think this could never happen to you, it is only because you have been living under a rock. The effects of a data breach can extend far beyond the loss or compromise of data. The monetary costs can be severe. To mitigate your risk and limit those costs, you need to establish a comprehensive team to assess your network security, develop cybersecurity incident response plans and employee policies and insure your firm for potential losses. Firms must look beyond their traditional IT department to develop a complete cybersecurity solution to mitigate potential financial liability.

Cost of Data Breaches

According to the IBM Security and Ponemon Institute study, the average cost of a data breach was $3.62 million dollars in 2017. *2017 Cost of Data Breach Study*, IBM Sec. & Ponemon Inst., 10 (June 2017); *See* http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf?t=1510933508399. (Last accessed June 1, 2018). Among the 419 companies that participated in the survey, on average, a data breach cost $141 per lost or stolen record. *Id.* The figure includes the cost of breach remediation efforts such as a data forensic investigation, breach victim notification, credit monitoring and legal fees. *Id.*

From those figures, you can roughly estimate the cost of remediating a data breach of your law firm by multiplying the number of data records containing personal information of any type (name, social security number, personal health information, etc.) by $141. Don't forget to include former clients and employees whose information is still stored electronically on your network. The total is the estimated cost of a data breach for your firm.

Another potential cost associated with a data breach is governmental penalties. Most of the states have enacted data breach notification laws. These laws typically define personally identifiable information, what constitutes a data breach and victim notification requirements in the event of a breach. However, some states also impose a civil penalty if the breach resulted from the organization's negligence. For example, the Attorney General of Virginia may impose a civil penalty up to $150,000 for every network breach of an organization's computer system. §18.2-186.6, Code of Va., 1950, as amended. In short, firms may also be responsible for these penalties in addition to the remediation cost.

One of the more troubling findings from the Ponemon study is that the average size of a data breach has increased since 2016. That likely means that the cost to remediate a data breach will continue to grow if more data files continue to be exposed year after year. That finding is just one more reason for your law firm to take action to limit its liability and deal with the real threats posed by hackers.

As then FBI Director Robert Mueller famously quipped in 2012, "I am convinced that there are only two types of companies: those that have been hacked and those that will be." Robert S. Mueller, III, Director, FBI, Address at the RSA Cyber Security Conference San Francisco, CA (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies. (Last accessed June 1, 2018). In 2014, his successor, James Comey told CBS' *60 Minutes* that "[t]here are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese." James Cook, *FBI Director: China Has Hacked Every Big US Company*, Bus. Insider (Oct. 6, 2014, 6:24 AM), http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10. (Last accessed June 1, 2018). Unfortunately, Ponemon's findings have corroborated these statements, reporting that the probability of an organization experiencing a data breach in the next 24 months increased from 25.6 percent in 2016 to 27.7 percent in 2017. *2017 Cost of Data Breach Study*, *supra* note 1, at 25. This means that it is very likely that one in four of your colleagues will experience a data breach within the next 24 months. Since the costs are real, attorneys need to take action to protect their firms.

What Can You Do To Protect Your Law Firm

ABA Model Rule 1.6(c) states that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Many states have adopted some form of the ABA model rule and have added additional guidance regarding securing client data. Comment 20 to Virginia Rule of Professional Responsibility 1.6 establishes the key guiding principle to help all attorneys address today's growing cybersecurity threats. It states that, "[a] lawyer or law firm complies with [the rules of professional responsibility] if they have acted reasonably to safeguard client information by employing

appropriate data protection measures for any devices used to communicate or store client confidential information." The Comment does not specifically prescribe what firms need to do or require attorneys to become IT experts. It simply requires attorneys take reasonable actions to address cybersecurity based on the needs and scale of their law firms. Three reasonable steps that every law firm needs to take are outlined below.

Adopt a Security Framework

The first step is to adopt a security framework for your firm. The U.S. Institute of Science and Technology (NIST) defines a cybersecurity framework as a "policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks." National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, 14 (April 16, 2018). Frameworks "provide a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes." *Id*. There are a host of different frameworks to choose from (ISO, NERC, CISQ), but one of the most popular frameworks for businesses is NIST Special Publication 800-171.

Unlike other NIST frameworks that were designed for government computer systems, NIST 800-171 was designed specifically with private businesses in mind. Its requirements are non-prescriptive and allow businesses the flexibility to meet the required security controls on their own terms. It is relatively easy to understand and provides a sound roadmap to begin developing a robust cybersecurity infrastructure.

NIST 800-171 is also the required framework for defense contractors that provide services for the federal government. Because of its popularity, it is rumored that NIST 800-171 will eventually be the cybersecurity framework required for all federal government contractors. The NIST framework is broken down into five key functions (Identify, Protect, Detect, Respond and Recover). Each of the five key functions has sub-categories that help guide organizations through the process of assessing their organization's cybersecurity posture.

While a NIST framework may not be the best solution for your firm, the key is to adopt a security framework. Selecting the right framework may seem daunting because the average attorney is not an IT expert. However, the rules of professional responsibility allow attorneys to enlist the services of an IT/cybersecurity vendor to assist you in selecting the framework and network security design that is right for your firm.

The next step is broken down into two parts: (1) establish a cybersecurity incident response plan and (2) establish an employee cybersecurity policy.

Incident Response Plans

Every firm needs a cybersecurity incident response plan. In the event of a data breach, an incident response plan does four key things:

1. It defines the different kinds of data security incidents and how to respond to each accordingly. For example, a firm will respond to the exfiltration of data very differently from how it will respond to a ransomware attack. The incident response plan establishes the different steps to be taken based on the type of data incident that is taking place and delineate what resources are required to deal with an incident depending on the incident's severity.

2. An incident response plan defines the members of the firm's incident response team and defines their roles. At a minimum, the firm's incident response team should be comprised of the firm's IT director, human resources director, key firm leaders and your outside breach counsel. The extended members of your incident response team should include individuals like crisis communications professionals, data security and forensics firms, call centers, and mass mailers that can send breach notifications to victims.

   One of the most important members of an incident response team is your outside breach counsel. Breach counsel is an important role because he or she is responsible for initiating the breach investigation and keeping it confidential. Courts have held that counsel-initiated data forensic investigations are privileged and protected by the work-product doctrine when they are initiated in anticipation of litigation. *See In re Experian Data Breach Litigation*, C.D. Cal. No. SASCV1501592AGDFMX, 2017 WL4325583, at 1 (C.D. Cal. May 18, 2017). Utilizing outside counsel engaged from the start, specifically for the purpose of managing a data security incident, helps the courts distinguish between an investigation conducted in the course of ordinary business, which is not protected as work-product if the confidentiality of the investigation is ever challenged. *Id*. at 4. This is important to mitigate the risk that an adverse party will be able to discover the con-

tent of a non-flattering data forensic investigation during litigation.

When possible, it is recommended that your breach counsel draft or assist in drafting the firm's incident response plan and employee policies. Just as you have intimate first-hand knowledge of your client's organizational structures, operations, people, policies and plans, having your selected breach counsel draft your incident response plan and employee policies will give him the working knowledge about your business to effectively represent you when you are in the midst of a crisis. It is essential that the attorney who manages your breach response know the members of the incident response team and how the plan is to be carried out.

3. The incident response plan can also establish a communications plan for your firm. Firm leadership may need to communicate with clients, employees and government regulatory agencies. The plan should identify who makes what communications and when.
4. The incident response plan must mandate testing and must be updated at least annually. This is traditionally done through table-top exercises where the firm's key stakeholders gather to simulate mock data breach scenarios to test the effectiveness of your plan. Your plan is a living document, and should be updated as necessary following testing or changes in your firm practices, leadership, technology or evolving cybersecurity threats.

Cybersecurity Employee Policies

Cybersecurity policies cover a gap that traditional employee policies usually do not cover in one comprehensive document. Many of the electronic tools that employees use when performing their business-related functions have security vulnerabilities that can be exploited if employees are careless or not trained appropriately. Therefore, firms must implement policies that give employees notice and govern how employees access firm networks, use email, remotely connect to your network, and store (and destroy) data, just to give a few examples.

Developing employee cybersecurity policies alone is not enough. Employees must also be trained on these policies at least annually and any time that the policies are updated as technology and cyber threats change.

Buy Cyber Insurance

The final step is to obtain cybersecurity insurance to protect your firm from the liabilities. According to IBM Security and the Ponemon Institute, approximately 28 percent of data incidents are caused by human error. *2017 Cost of Data Breach Study*, *supra* note 1, at 13. While you can buy and deploy the best hardware and software, develop the best employee policies and have the most cyber-educated employees, there are still employees who will click on a malicious link, lose a portable device filled with sensitive information or commit some other act that exposes personal or sensitive firm information. This is where your cyber-insurance kicks in to further protect your firm. There are a host of considerations when purchasing cyber-insurance and to address them all would require more space than allotted. However, here are a few important points to consider.

Be sure that the coverage allows for ransomware payment in cryptocurrencies. The language of some early policies did not anticipate the use of cryptocurrencies, like Bitcoin, to become an acceptable currency to pay a ransom. Coverage issues have occurred where the use of cryptocurrencies was not specifically enumerated in the terms of the policy.

It is also important to be aware of retroactive date exclusions in policies. According to the Ponemon Institute, a hacker can be lurking in your network for months before they are detected or a data incident occurs. *Id* at 27. If your insurance coverage begins after a hacker gains access to your network, the data incident that results could be considered an event that occurred prior to the policy period and would therefore be excluded from coverage. Make sure that coverage extends to incidents or events that are unknown prior to the beginning of the policy period.

Check whether the policy covers dependent business interruption. This is coverage for losses and expenses incurred as a result of the interruption of your computer systems due to the breach of systems operated by a business upon which your firm depends. For example, if your firm's cloud service provider's system failed due to a data breach that negatively impacted your business operations, your firm would still be protected even though your firm's IT system was not breached.

Be sure that your policy has an expanded definition for employees. Many policies define employees as a full-time, part-time or temporary employee performing work within the scope of your firm's business. This limited definition leaves a gap that may not cover volunteers, interns,

independent contractors, seasonal employees, and parties that you expressly agree in writing to add as an additional insured. Because twenty-first century la w firms utilize the services of many different labor sources to provide legal services, it is important that firms are covered for all of the various labor sources and service providers it utilizes.

Above all, you should consider the needs of your firm, research policy options thoroughly and have a robust discussion with your broker.

Additional Cybersecurity Planning Benefits

There are a several additional benefits from limiting your cybersecurity risk through planning. Incident response plans and policies can be used to demonstrate your cybersecurity posture to clients. As mentioned above, reasonable cybersecurity planning can keep you from violating the rules of professional responsibility. Insurers are often willing to discount your firm's premium because you have taken steps to mitigate the likelihood of a data breach and effectively manage it if one occurs.

Conclusion

The reputational and financial costs associated with data breaches are real. Law firms of all sizes are grappling with how to best protect themselves and limit the potential for liability. The steps in this article are intended to give you a roadmap to get started or improve what you have already developed. In taking those steps, it is important to realize that cybersecurity is not just an IT issue. A comprehensive cybersecurity plan for your firm requires the collaboration of a team to address IT security, incident response plans, employee policies and insurance coverage. The key is starting now, taking the first steps and getting the right players on your team.

Darius Davenport leads the Cybersecurity and Data Privacy Practice Group of Crenshaw, Ware & Martin. His practice focuses on data privacy laws and regulations, helping clients mitigate cyber risk, and dealing with the legal and practical problems resulting from cyber incidents. His cybersecurity counsel to businesses and municipalities includes drafting and review of incident response plans, cybersecurity employee policies, technology contracts and conducting cybersecurity and breach response exercises. He is frequently invited to speak on cybersecurity and data privacy issues.

James L. Chapman IV is chair of the Crenshaw, Ware & Martin's Litigation Practice Group. His primary practice areas include admiralty, business, cybersecurity, data privacy, railroad/transit, and unmanned systems. Jim has tried over 100 cases to jury verdicts for clients involving a broad range of legal disputes. He advises governing boards and senior leadership regarding risks and resolution strategies in high-profile cases. His service as general counsel to companies, and as a director and officer of several non-profit organizations, helps clients resolve difficult challenges and plan strategically.