CYBERSECURITY DOCKET
GLOBAL CYBERSECURITY AND INCIDENT RESPONSE REPORT

LAW FIRMS AND CYBERSECURITY: A COMPREHENSIVE GUIDE FOR LAW FIRM EXECUTIVE COMMITTEES

By John Reed Stark*

John Reed Stark is President of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Mr. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, the last 11 of which as Chief of its Office of Internet Enforcement. He has also served for 15 years as an Adjunct Professor of Law at the Georgetown University Law Center, where he taught several courses on the juxtaposition of law, technology and crime. He also served for five years as managing director of a global data breach response firm, including three heading its Washington, D.C. office.

Forget credit card numbers, social security numbers and medical records, law firms are currently under what could become the most significant cyber siege in history. Why? Because law firms possess a lucrative cache of data that makes them incredibly attractive to cybercriminals.

Law firms provide a "back door" for a treasure trove of cherished electronic material for cyber criminals eager to gain an edge in the stock market or capture a particularly sensitive batch of data to sell or ransom, including:

- Secret and sensitive information about corporate client's finances;
- Documents relating to confidential corporate deals;
- Valuable information relating to patented, original and invaluable intellectual property and trade secrets;
- Key evidence pertaining to bet-the-company litigation; and
- Gigabytes (perhaps even terabytes) of emails involving the most intimate, delicate and private details of their client's personal and professional lives.

Is this highly confidential and imperative electronic data hard to locate and identify on the devices and networks of law firms? Not at all. The most critical and important documents, presentation decks, PDFs, spreadsheets and the like are typically (and conveniently) labeled in folders and directories named "hot docs," "confidential info," "top secret" or other similar sequestered nomenclature.

Introduction. Last year, the American Bar Association reported in its annual Legal Technology Survey that one in four firms with at least 100 attorneys have experienced data breaches involving hackers, website attacks or stolen or lost smartphones, tablets or laptop computers. Forty-seven percent of respondents said their firms had no response plan in place to address a security breach. Among the largest firms of 500 or more attorneys, 55 percent had a security breach response plan in place. More than half of attorneys, 58 percent, said their firms did not have a dedicated Chief Information Security Officer (CISO) or another staff member charged with data security, while 34 percent said their firms did. Clearly, law firms are significantly behind the curve, despite law enforcement agencies and cybersecurity firms issuing repeated warnings about the risks of attacks by insiders, fraudsters, hacktivists, unscrupulous competitors and nation-states.

This month, cyber thieves reportedly broke into a slew of national law firms, including two New York law firms, Cravath, Swaine & Moore and Weil Gotshal and Manges, who represent Fortune 500 companies and financial institutions all over the world. Cravath said the incident, which occurred last summer, involved a "limited breach" of its systems and that the firm is "not aware that any of the information that may have been accessed has been used improperly." The firm said its client confidentiality is sacrosanct and that it is working with law enforcement as well as outside consultants to assess its security. Weil Gotshal declined to comment.

This month, news also broke concerning the law firm data breach surrounding the so-called Panama Papers, thus far involving more than 11.5 million documents detailing how hundreds of wealthy people hid money in offshore banks and investments to avoid paying taxes, causing international headlines, a presidential resignation and celebrity embarrassment. The head of the Panamanian law firm, Mossack Fonseca, which specializes in setting up offshore companies, denied any wrongdoing, and said his firm has fallen victim to "an international campaign against privacy."

On March 3, meanwhile, the FBI's cyber division issued a Private Industry Notification, warning law firms that "in a recent cyber criminal forum post, a criminal actor posted an advertisement to hire a technically proficient hacker for the purposes of gaining sustained access to the networks of multiple international law firms," Bloomberg reports. This is not the first time interested parties have used hacking to gain access to private data – the Rupert Murdoch phone hacking scandal of several years ago was similarly scandalous.

Even not prompted by the latest headlines, every law firm executive committee realizes that its law firm can (and probably will) fall victim to a cyber-attack, and even worse, that the executive committee will need to clean up the mess and superintend the fallout. Just like the role of the corporate boards of directors has begun to evolve to embrace

cybersecurity oversight responsibilities, law firm executive committees now have to do the same.

As cyber-attacks continue to proliferate, more and more law firm executive committees will come to realize that cybersecurity risks now actually trump most (if not *all*) other business risks - and not just because technology and networks touch every aspect of a legal enterprise. For law firms in particular, this is the dawning of a new era of data breach and incident response, where trying to avert a cyber-attack is like trying to prevent a kindergartener from catching a cold during the school year. The nature, extent and potential adverse impacts of these risks call for a proportionate response.

But cyber-attacks can be extraordinarily complicated and, once identified, demand a host of costly responses. These include digital forensic preservation and investigation, notification of a broad range of third parties and other constituencies, fulfillment of a confusing constellation of state and federal compliance obligations, potential litigation, engagement with law enforcement, the provision of credit monitoring, crisis management, a communications plan – and the list goes on. During the aftermath of a data breach, a law firm's notification responsibilities alone involve a lengthy list of relevant constituencies, including clients, vendors, joint venturer's, employees, affiliates, insurance carriers and a range of other interested parties.

And besides the more predictable workflow, a law firm is exposed to other even more intangible costs as well, including temporary or even permanent reputational and brand damage; loss of productivity; extended management drag; and a negative impact on employee morale and overall law firm performance.

So what is the role of a law firm executive committee amid all of this complex and bet-the-company workflow? For certain, simply receiving regular reports on a law firm's cybersecurity risk management is no longer enough. Both a law firm's clients and employees now expect law firm executive committees to make a substantial effort to understand and oversee cybersecurity, even though the typical law firm executive member has limited IT experience. But how? The answer lies in this cybersecurity guide, specially tailored for law firm senior executives.

Within this guide, law firm leaders will find a hefty catalogue of cybersecurity considerations that provide a bedrock of inquiry to help take their responsibilities seriously, specifying the requisite strategical framework to engage in an intelligent, thoughtful and appropriate approach to reducing a law firm's cybersecurity risks.

By following this guide, law firm leaders can not only become more preemptive in evaluating cybersecurity risk exposure, but they can also successfully elevate cybersecurity from an ancillary IT concern to a core enterprise-wide risk management item, at the top of a law firm executive committee's oversight agenda.

NIST Cybersecurity Framework. A good starting point for a law firm executive committee, when kicking off its efforts to assess internal cybersecurity measures and

develop a comprehensive cybersecurity risk management plan, is to review the *Framework for Improving Critical Infrastructure Cybersecurity*, released by the National Institute of Standards and Technology ("NIST") in response to President Obama's issued Executive Order 13636, titled "Improving Critical Infrastructure Cybersecurity."

The NIST Cybersecurity Framework is intended to provide companies, including law firms, with a set of industry standards and best practices for managing their cybersecurity risks. The Framework is a user-friendly text, which does not require a computer science degree in order to understand its basic and fundamental notions. NIST also provides a "Roadmap for Improving Critical Infrastructure Cybersecurity," which is a nine-page companion to the Framework, discussing NISTs next steps with the framework and identifying key areas of development, alignment and collaboration.

While the Framework is aimed at security of critical infrastructure, it is "principles based," using generally accepted security principles that can apply to all kinds of businesses and enterprises, including law firms. It provides a structure that organizations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programs.

The Framework sets out five core functions and categories of activities for companies to implement that relate generally to cyber-risk management and oversight. The five core functions are: *Identify, Protect, Detect, Respond and Recover*. This core fundamentally means the following: law firms should (i) identify known cybersecurity risks to their infrastructure; (ii) develop safeguards to protect the delivery and maintenance of infrastructure services; (iii) implement methods to detect the occurrence of a cybersecurity event; (iv) develop methods to respond to a detected cybersecurity event; and (v) develop plans to recover and restore the companies' capabilities that were impaired as a result of a cybersecurity event.

The Framework provides law firm senior executives with a controls paradigm to use as the foundation of a cybersecurity program. Law firm clients, especially larger and more sophisticated clients, may send their own list of cybersecurity recommendations and law firm managers may be tempted to base cybersecurity programs on these specific client requests. This is a mistake. Multiple clients will send their own cybersecurity requests and standards, which will not only create an undue burden on a law firm's IT staff but the burden will be continuous, because clients will be constantly changing and updating their security standards, requiring annual confirmation that robust cybersecurity is in place.

For law firms in particular, using the NIST framework not only saves time and money but will also avoid the unnecessary management drag of customized client security solutions. Moreover, law firm clients will ultimately appreciate a law firm's use of a common Framework, which their respective regulators always encourage.

ISO 27001. Another potentially important standard for law firms is ISO 27001:2013, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC

subcommittee, ISO/IEC JTC 1/SC 27. Developed to provide an international model for establishing, implementing, operating, monitoring and maintaining an information security management system, ISO 27001 is widely recognized as the highest security standard in the industry for examining the efficacy of an organization's overall security posture.

Reportedly, at least a dozen Am Law 200 and Magic Circle firms have attained ISO 27001 certification to demonstrate their dedication and commitment to protecting their documents and communication systems from security breaches, and at least 21 more are in the process of seeking the certification.

Kansas City law firm Shook, Hardy & Bacon achieved ISO 27001 certification in 2013 and described the standard as a key selling point for their firm. "We wanted to make sure we had the processes in place so our clients had confidence that we were doing the best we could," said the firm's chair, John Murphy. Goodwin Proctor also achieved ISO 27001 certification and trumpeted the standard in a press release, stating, "At Goodwin, protecting the security and confidentiality of client and personal information is a top priority." David Fleming, the firm's Chief Information Officer, also stated, "We are pleased to be recognized among the small group of law firms that are certified against the stringent ISO 27001 standards." According to Shook CIO John Anderson, Shook spent about $30,000 in 2013 and another $30,000 in 2014 on consultants and auditors to earn the certification; on top of additional cybersecurity-related spending to support the law firm's security strategy.

The ISO 27001 certification process is rigorous, often taking as much as 6-12 months to complete, and includes:

- Creating/executing comprehensive information security management system;
- Drafting detailed policies and specific strategies in compliance w/ ISO standards;
- Taking inventory of firm's electronic information/storage locations; and
- Selecting and implementing the appropriate security controls.

But while SO 27001 certification can: reduce insurance costs; enable a law firm to produce an objective, thoughtful and meaningful response to a client's security questionnaire or audit requests; and improve a law firm's overall cybersecurity posture (especially internationally) -- it is not a panacea. In fact, ISO-27001 may not satisfy a firm's biggest clients, especially financial institutions, which are being pressured by regulators t, demand adherence to even tougher standards to guard against cyber-attacks.

Further, ISO-27001 is process oriented i.e. becoming ISO 27001 certified means that a law firm has processes and protocols in place to keep confidential information secure. The certification is not a technological tool nor a cybersecurity solution, leading one commentator to warn law firms about confusing compliance with security. Becoming ISO 27001 certified arguably provides little comfort regarding the actual readiness and ability of firms to protect the confidential information entrusted to them. ISO 27001 dictates how to go about managing the cybersecurity function but leaves all of

the actual execution to the law firm. Moreover, the lengthy and tedious process of becoming ISO 27001 certified can complicate, delay and distract firm management from well-defined steps that can and should be taken in the short term.

The bottom line on ISO-27001: It is an internationally recognized, certifiable, information security standard that formally specifies an information security management system to bring information security under explicit management control – which is obviously an added benefit for any law firm.

Moreover, ISO 27001:2005 (the predecessor to ISO 27001:2013) certification was the gold standard for many years for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented data security management system within an organization or data center. (N.B. the key changes in the 2013 revised standard relate to: improved handling of IT security risks, such as identity theft, mobile device threats and online vulnerabilities; improvements and consolidations of security controls; and allowing companies to have an integrated management system, rather than distinct separate ones.)

Finally, at present having ISO-27001 is (at least for now) a unique market differentiator for law firms (who reside in a fiercely competitive space). Moreover, because the certification requires organizations not only to uphold specific standards but also to review continuously, and improve, their security postures, the certification plainly evidences a law firm's bona fide commitment to cybersecurity.

Penetration Testing/Risk and Security Assessments. Just like an annual physical check-up by a physician, a law firm should undergo a risk and security assessment of its inner cybersecurity workings. Implementing cybersecurity solutions requires a comprehensive risk assessment to determine defense capabilities and weaknesses and ensure the wise application of resources. What works best is a disciplined yet flexible methodology that incorporates a law firm's organizational culture, operational requirements and tolerance for risk, and then balances that against current technological threats and risk. Since data breaches are inevitable, a proper risk and security assessment quantifies risk, develops meaningful risk metrics and conveys the effectiveness of risk mitigation options in clear and concise terms.

To begin with, consulting firms and cybersecurity shops market a myriad of services: penetration testing, risk and security assessments, data security audits, application security evaluations, code reviews and other similarly described services. Even the consultant jargon is unclear. For purposes of this guide, all categories will fall under the label of penetration (or "pen") testing, which is standard parlance and also considered the lowest common denominator for evaluating cybersecurity.

Common types of pen testing for law firms should include: an external penetration test or vulnerability scan to assess Internet-facing computers, including firewalls, VPNs and other online gateways; an internal penetration test or vulnerability of a law firm's internal network, such as desktops, laptops, servers, printers, VOIP phones and other online devices; a web application assessment to analyze a law firm's website security; and

social engineering testing to assess the "human firewall" of a law firm, and reconnoiter law firm staff cybersecurity awareness. In addition, law firms should conduct an unannounced spear-phishing tests. Spear-phishing tests help determine employee resistance to one of the most common methods of remote compromise. The tests also help gauge the risks associated with permissive egress filters, targeted malware, the establishment of remote command and control channels, and the susceptibility to undetected bulk data exfiltration.

A law firm's pen tester should have substantial technological abilities, including expertise in testing web applications, mobile applications and devices, software products, third-party service providers, cloud solutions and IT infrastructure.

One mark of a good pen tester is to be a thought leader in the infosec community – authoring theoretical publications, giving peer conference presentations, contributing to open source projects, writing blogs or publishing vulnerabilities. It also helps if a pen tester has so-called "blue team" experience, (that is, he or she has managed networks or systems or developed applications).

Good pen testers mimic the methods used by sophisticated attackers to identify vulnerabilities before they can be exploited. That is best achieved by using specialized, manual testing, not by running automated tools. Automated tools do have a place (it's a good practice to run them internally looking for low hanging fruit) but custom tools will typically prove far more effective. No two pen testing engagements are ever the same; even the same vulnerability can vary wildly in different environments, and having a proprietary set of tools evidences a pen tester's ability to venture off-script and improvise when necessary. Proprietary tools also typically allow for a more detailed explanation of the so-called "kill chain" or path of an attack.

There exists no standardization about pen testing (like some sort of emissions or DNA test), so law firm executives should give careful consideration to who should conduct a law firm's pen testing and how to best interpret the results. Before conducting any test or assessment, law firm leaders should make sure IT departments document all cybersecurity policies and procedures, not just to get credit for good behavior and practices, but also because documentation is a beneficial compliance exercise.

Law firms will want to avoid engaging pen testers who present deliverables that provide a written laundry list of problems in need of solutions or a so-called "heat map," which identifies the most serious potential weaknesses. The reason? Because the reality is that most companies will not be able to cure all weaknesses (because of cost concerns, logistical impossibilities, practical barriers, etc.).

Though intended for a law firm's benefit, heat maps and laundry lists can also unfortunately provide regulators, law enforcement, class action lawyers and other disgruntled parties with a handy and helpful roadmap for liability. Thus, the primary deliverable for any pen test should begin with a briefing, where law firm executives can discuss the format of any ultimate deliverable with the pen testing results.

One final note on choosing the right pen tester. When I was three years old, my family moved into a new house. To manage our home's HVAC, electrical, security, and other related systems, my late father hired a small company called Systematic Control, run by a superstar engineer named Neil Carbone. But Neil was not just a repair ace; he also became a part of our family. For the next 40 years, Neil's phone number was posted on our refrigerator door and we called him when anything went wrong. Neil became our most dependable and trusted adviser; he cared for our home (and our family) like it was his own.

When Neil stopped by annually to develop new ideas to make our house better, safer, more fuel efficient, and so forth, he never brought a checklist. Instead, Neil took a holistic approach toward servicing our home, observing not just how our family lived, but also incorporating how our house's environment was changing.

These two lessons from Neil are probably the most important for selecting a pen tester. First, good pen testers not only possess bona fide technological chops, an ethos of dedication, and a philosophy of service. Just like Neil, they also strive to become a law firm's trusted adviser. Second, threat landscapes, activists, random hackers, and state-sponsored actors constantly evolve, refining their techniques, altering their motivations, and shifting their resources. Just like Neil, good pen testers take a holistic approach to their works, carefully considering changing threat actors, advance network telemetrics and emerging attack vectors.

So when checking the references of pen testers (a must, by the way), in addition to considering common recommendations and caveats, consider most of all, my late father and Neil Carbone. Together they kept our home and family safe and prosperous for more than 40 years.

Top Down Commitment. Strong cybersecurity is a business imperative, yet too often cybersecurity is too far down on a law firm executive committee's priority list or because it is so complex, simply delegated to lower level technical personnel. Some questions for law firm executive management: Is there a commitment from the top down, both culturally and financially, to rigorous cybersecurity? Who in leadership is driving the cybersecurity agenda? Is it a C-level accountability and part of the day-to-day business focus? Do current reporting lines and assigned areas of responsibility make sense? Given the responsibilities and accountability needed to execute the incident response plan, are the right employees, possessing the appropriate skillsets, adequately empowered? If the team charged with overseeing cyber-defense the same team who reports up the chain about breaches and who would oversee any response, that dual-role indicates an inherent conflict of interest.

Effective security awareness demands top-down commitment and communication, a characteristic that is often lacking at law firms, especially where legal practices (and partners) are "siloed" or otherwise isolated. Law firm executive committees should enforce the notion that the firm has an institutional commitment to protect client data reflected by involvement and engagement by senior firm leaders - not just IT. In the least, law firm executive committees should establish a cross- organizational team

(including practice chairs, procurement, finance, human relations, communications, office management, IT and security personnel) that regularly convenes to discuss, coordinate and communicate information security issues.

Drills and Table-Top Exercises. Tabletop exercises enable organizations such as law firms to analyze potential emergency situations in an informal environment, and are designed to foster constructive discussions among participants as they examine existing operational plans and determine where they can make improvements. Such exercises are a natural fit for information and physical security, because they provide a forum for planning, preparation and coordination of resources during any kind of attack.

Most cybersecurity firms and pen testing firms offer some form of table top exercise program, which in order to be successful, should: involve detailed preparation; include multiple parties throughout the law firm; leverage resources from within the law firm industry and government; and will be timely and realistic. Law firm executive committees should also reach out to law enforcement agencies such as the FBI and request for a federal agent to participate as well. The FBI supports this participation and collaboration with U.S. companies, especially law firms, and can provide valuable insight throughout the drill.

Incident Response Plan. Having an incident response plan is a notion that has been preached over and over again to every law firm, retailer, manufacturer, financial organization or otherwise, but still warrants a quick mention nonetheless. When contemplating cybersecurity, most companies allocate significant resources to fortifying their networks and to denying access to cyber-attackers. However, it is now a cliché, well founded in reality, that data breaches are inevitable. As cybersecurity experts have noted, "There's a saying in the cybersecurity industry that there are two types of businesses today: Those that have been breached and know it and those that have been breached and just don't know it."

Along those lines, just like a fire evacuation plan for a building, a law firm should have a plan in place to manage data breaches; an art form less about security science and more akin to "incident response." In the least, an incident response plan specifies the:

- Members/titles/contact details of the response team responsible for each of the functions of the plan (management, IT, information security, human resources, compliance, marketing, etc.);
- Communication lines in the event of a cyber-attack;
- Notification protocols and priorities (including law enforcement, regulators, customers, joint venture partners, vendors and anyone else who might require or contractually be entitled to, notice);
- Documentation and logging plans in the event of a breach;
- Contact list of relevant outside parties such as outside counsel (who specializes in data breach response), outside digital forensics experts, local law enforcement agents, PR firms and relevant financial firms (including the firm's bank and insurer);

- Law firm employees who have authority to speak and make certain decisions about the investigation;
- Cyber insurance information;
- Containment, remediation, recovery, training, and testing plans; and
- The nature and location of any data that is covered by other legal obligations like medical records under HIPAA; financial records covered by the Graham Leach Bliley Safeguards Rule or specific client contractually created data protection/breach notification requirements.

Law firm executive management should understand their current incident response plans; when the plan was last updated (and how often); who prepared the plan; who approved the plan; and the general approach and general principles of the plan. There should also exist an accurate and current network topology diagram that is adequately documented, and periodically re-assessed and revised as internal systems and external factors change.

Law firm executive committees should also avoid using templates for incident response plans. While templates can serve as a decent starting point, no two law firms are identical and all have different business processes, network infrastructures and types of data-sets. Along these lines, NIST has published a Computer Security Incident Response Guide that can help law firms develop appropriate policies and procedures and provide a useful reference for law firm executive committees when meeting with IT department heads. The abstract for the NIST guide states:

> "Computer security incident response has become an important component of information technology (IT) programs. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. This publication assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications. "

One unintended benefit of a strong incident response plan is that it can serve as an effective business development tool. In addition to promulgating security procedures, incident response plans for law firms (and many other professional service providers) can also serve as effective powerful collateral. More and more, clients and insurance companies are asking to review law firms' incident response and factoring the value and efficacy of an incident response plan into the calculus of their hiring and procurement processes.

Preservation Challenges. Every cyber-attack response begins with the simple notion of preservation, *i.e.* collecting and preserving, in a forensically sound and evidentiary

unassailable manner, any "electronically stored information" (ESI), devices, logs, etc. that could become relevant to the cyber-attack.

Unfortunately, preserving ESI after a cyber-attack can quickly become a challenging, costly and resource intensive task. Most law firms have ESI in so many locations (both physical and virtual) that, after a cyber-attack, it becomes an onerous struggle to locate and preserve relevant ESI and to piece together information about sometimes complex and disparate systems – all under the intense pressure of an active digital forensic investigation (with serious consequences for error or omission).

By way of background, preservation is a critical work stream during a cyber-attack because incident responders will be scrutinizing every byte of data, especially any fragments, artifacts or remnants left by the attacker in all sectors of any relevant device (including within "deleted recoverable files," "unallocated and slack space" or the boot sector.) These artifacts can include: Internet addresses; computer names; malicious file names; system registry data; user account names; and network protocols.

The most effective investigative methodology of a cyber-attack is one based on targeted incident response practices and does not solely rely on "signature detection" technologies, such as antivirus software. Rather, careful investigators employ an iterative process of digital forensics, malware reverse engineering, monitoring and scanning.

As analysis of known or suspected compromised systems identifies new so-called *Indicators of Compromise* ("IOCs), investigators will examine network traffic and logs, in addition to scanning hosts for these IOCs. When this effort discovers additional systems, those systems are forensically imaged and analyzed, and the process repeats. Armed with the information gathered during this phase of "lather, rinse, repeat," a victim law firm can begin efforts to remediate the malware, rebuild compromised systems, reset compromised account credentials, block IP addresses and properly initiate network and host monitoring in an effort to detect additional attempts by the attacker to regain access.

Preservation is also critical because investigators will likely need to scour all ESI in search of so-called *personally identifiable information* or "PII." The search for PII is necessary to determine whether the attacker exfiltrated (removed from a corporate IT environment) any data containing personal information relating to any individuals, who may require notice of the cyber-attack, credit monitoring services and other remedial action.

Protecting PII relating to individuals from identity theft has become a significant focus of U.S. state and federal agencies, and of new state and federal laws and regulations. In the U.S., laws and regulations vary from state to state, and between state and federal law, as to exactly what information comprises PII. Generally, the definition requires both a name and some additional item of information that could be used to steal a person's identity or access his or her financial accounts (or, in some cases, healthcare information) without authorization. N.B. that for purposes of this article, we refer generally to protected information about an individual as PII, even though some state or federal statutes may use a different nomenclature or categorizations.

Finally, just about every cyber-attack response also involves the forensic imaging and reviewing of emails and other relevant communications from laptop computers, desktop computers, network servers, backup tapes, mobile devices, tablets and other systems. The cyber-attack investigation may have sprouted from a customer who complained that his or her data was used for a fraud; from a report that a computer system was found to be communicating with an unscrupulous Internet address; from the FBI, U.S. Air Force Office of Special Investigations; US Secret Service or other law enforcement agency notifying a law firm of a possible cyber-attack into its systems; or a slew of other sources.

Under any circumstance, investigators will first analyze whatever initial information is presented and use the preliminary evidence to help identify the likely locations of additional evidence. An investigator will consider all computer devices as likely locations to target for investigation. These devices will typically include: law firm laptops and workstations; network storage servers; firewalls; intrusion detection systems; webservers; customer databases; and e-mail servers.

It can even take days after learning of a cyber-attack before a law firm realizes that they maintain an electronic purging process that deletes data (such as relevant logging information) on a regular schedule. Without having proactively made the effort to understand information sources, assets and their key characteristics, these purging schedules can become unintended and latent causes of spoliation.

Data-Mapping. Given the challenges of preservation discussed above, law firms should probe their own data practices carefully. Where information relevant to identifying and describing potentially accessed/target/exfiltrated systems has never been data-mapped, establishing a strong and effective incident response plan for addressing cybersecurity risks can become challenging. Without any sort of responsible system overview or asset classification exercise, law firms not only make mistakes in their cyber incident response plans, but law firms can also make mistakes in allocating available resources to the investigation.

In addition, law firm executive committees should press to identify and understand the most critical datasets of law firm information. What are the law firm's most valuable intellectual property assets and consumer/customer based informational assets, and how are they currently being protected? Where are these assets stored or located -- internally, at a third-party data center (in the U.S. or overseas), or in a cloud-based environment? Asking these and other similar questions will help a law firm executive committee better understand the law firm's posture with respect to securing its virtual assets and inform what additional steps, if any, management can take to improve such practices.

Law firm executive committees should also consider implementing a sophisticated and intelligent data classification scheme. For example, consider parsing data sets into: 1) general use data, such as information published on the law firm website and included in public releases or disclosures; 2) internal use data, such as non-confidential internal communications; and 3) confidential data, such information carrying a legal confidentiality obligation like attorney-client work product or privileged attorney-client communications.

Confidential data in particular can be organized into narrower classifications such as: 1) information subject to protection under specific government statutes or regulations, including medical records protected under HIPAA or financial records under SEC Regulation S-P; 2) commercially sensitive information about clients, such as trade secrets, future business plans or negotiation strategies; 3) contractually protected information subject to a particular client agreement regarding that client's data; and 4) other confidential or sensitive information such as evidentiary data pertaining to active or closed litigation engagements.

Law firms with offices in countries that are members of the European Union (EU), or who handle and store protected personal information pertaining to citizens of the EU that they have received from or on behalf of their clients, are under special requirements to take measures to ensure the security of that information. Currently, this is an indirect result of the EU's broad data privacy regulations, special directives and other increasingly strict and rigorous data-related rules and requirements.

PCI Responsibilities. Executive committees at law firms should determine whether the law firm has any PCI compliance issues and if so, that those PCI-related concerns are being addressed.

By way of background, when a cyber-attack targets electronically transmitted, collected or stored payment card information, so-called Payment Card Industry Data Security Standards (PCI-DSS) compliance is often one of the first aspects investigated. The Payment Card Industry Security Standards Council is the international organization founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. in 2006, which develops and manages certain credit card industry standards, including the PCI-DSS. PCI-DSS is a set of requirements created to help protect the security of electronic payment card transactions that include PII of cardholders, and operate as an industry standard for security for organizations utilizing credit card information. PCI-DSS applies to all organizations that hold, process or pass credit card holder information and imposes requirements upon those entities for security management, policies, procedures, network architecture, software design and other critical measures that help to protect customer credit and debit card account data.

If a cyber-attack against a law firm involves credit cards or other similar modes of payment and triggers PCI-DSS compliance, the workflow involving the PCI-DSS can be extremely costly, cumbersome and disruptive. For instance, merchants are responsible for all costs associated with any system modifications required to achieve PCI-DSS compliance and the card brands may levy significant fines and penalties on merchants that are not in compliance with PCI-DSS. Such penalties and fines, imposed separately by each card association, can include:

- Hefty fines (in multiples of $100,000) for prohibited data retention;
- Significant additional monthly fines (can be $100,000 or more per month depending on the nature of the data stored) assessed until confirmation is provided indicating that prohibited data is no longer stored;

- Separate fines (in multiples of $10,000) for PCI-DSS non-compliance;
- Additional monthly fines (likely $25,000 per month) assessed until confirmation from a qualified security assessor that the merchant is PCI-DSS compliant;
- Payment of monitoring (can be as high as $25) and reissuing (up to $5) assessments for each card identified by the card association as potentially compromised; and
- Reimbursement for any and all fraudulent activity the card association identifies as being tied to a security data breach.

In addition, when an organization suspects a PCI cyber-attack, the card brands' PCI-DSS require hiring a PCI-approved forensic investigator (also known as a PFI) from a small list of card brand approved vendors. When a breach is suspected, a PFI is required to perform a specified list of investigative work including writing a final report that is issued to both the client and the various credit card companies, which is then used by the card brand companies to calculate potential fines that will be levied against the acquiring banks. These fees are then passed along to the victim company in the form of indemnification. Further, after a breach, a merchant's classification or "tier" may be adjusted upwards, resulting in the imposition of further obligations and potentially even greater fines and penalties should another breach occur.

Data Loss Protection. Law firms should work towards adopting security mechanisms such as data loss protection (DLP) systems (also known as "data leak prevention systems"), to help detect and prevent the potential unauthorized transmittal of confidential information by employees. DLP systems aim to prevent end users from sending sensitive or critical information, such as attorney work product or privileged attorney-client communications, outside a law firm's network.

Such systems classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could place the organization at risk. For instance, by installing data loss prevention technologies that "tag" certain files, phrases, and code names, a law firm could block or flag transmissions of those tagged files, with the aim of preventing sensitive information from leaving the firm's network.

Third Party (Including Local Counsel) Due Diligence. Outsourcing of services (such as IT, payroll, accounting, pension and other financial services), which typically involve the transfer of, or allowing access to, PII from a law firm to its vendor, has become increasingly common for law firms. Both law firms and service providers, including local counsel in litigation and other corporate matters, must contend with a matrix of obligations governing the disclosure of personal information under federal and state laws and regulations, common law privacy principles and industry guidelines and standards.

Thus, law firm executive committees should be concerned if any third party vendor has access to a law firm's networks, customer data or other sensitive information -- or if there exists any sort of other cybersecurity risk of the outsourced function. Law firm executive committees should also understand that third-party risk management is a security function as well as a compliance requirement. If a cybersecurity plan focuses only on

internal security, a law firm misses a substantial risk. Numerous studies have shown that third parties represent between 40% to 80% of the risks associated with data breaches.

Given that cyber-attackers will often traverse across a law firm's network and into the networks of its vendors or vice versa, cyber-attacks can also result in disputes as to the culpability for an attack. As a result, in most data breach scenarios, vendors and law firms can end up pointing the finger at one another for their respective cybersecurity failures.

Vendors who become entangled in the cyber-attack of a customer that includes PII of, for example, their customers' employees, can be subject to claims by those whose information is lost, as well as by their client. For example, in Caudle v. Towers, Perrin, Forster & Crosby, a federal judge dismissed claims for negligence and breach of fiduciary duty brought by an employee against his employer's pension consultant whose laptop containing PII of employees was stolen. The judge dismissed the negligence claim in the absence of evidence that the information had been accessed or used. It also dismissed the claim for breach of fiduciary duties, again on the ground that the plaintiff had not shown he had suffered any damages. The court did allow the claim for breach of contract to proceed to allow discovery on the issue of whether the employee was a third-party beneficiary of the contract between his employer and the vendor under the terms of the contract.

Similarly, in Ruiz v. Gap, Inc., where a company's vendor was sued for losing its client's personal information when a laptop was stolen containing information with job applications, a federal judge dismissed the claims for lack of requisite appreciable harm (because the plaintiff had not been a victim of identity theft but rather was claiming increased risk of future identity theft and seeking credit monitoring costs).

In addition, law firm executive committees should understand if and how the law firm incorporates requirements relating to cybersecurity risk into its contracts with vendors, which can, for example, trigger notification responsibilities. In the event of a data breach, corporate vendors will want to know all relevant facts relating to the cyber-attack, especially: if their data has potentially been compromised; if services will experience any disruption; the nature of remediation efforts; if there are any official or unofficial findings any investigation; or if there is any other information which can impact their operations, reputation, etc.

Vendors may also request images of malware and IOCs or to visit/inspect the law firm with its own investigation team. Venders may ask for weekly or even daily briefings and may demand attestations in writing with respect to any findings pertaining to their data. Some customers may also have contractual language establishing their rights when a cyber-attack occurs, which can range from notification, to on-site inspections, to the option of an independent risk and security assessment of the victim law firm (at the victim law firm's, and not the vendor's, expense).

Moreover, if third party vendors conduct remote maintenance of a law firm's networks and devices, in the event of a cyber-attack, the law firm should confirm it can obtain copies of any relevant logs, as well as access the third party system to scan for IOCs.

Law firm executive committees should inquire about the practices and procedures with respect to the cybersecurity of local counsel in particular, asking about information security procedures (including training) and outside access to the third party's own internal network. Big firms working with local litigation counsel may risk making themselves just as vulnerable as their less protected co-counsel. Just like with other vendors, the mantra underlying local counsel cybersecurity concerns is simple: *Any attack upon a law firm's local counsel can easily become an attack on the law firm itself.*

Buy Cyber-Insurance. Just like with other hazards of doing business, law firms have begun taking into account cybersecurity concerns when considering overall enterprise risk management and insurance risk transfer mechanisms. Clearly, cyber insurance will eventually become yet another basic element of a law firm's insurance coverage, just like property insurance for companies and health insurance for individuals. For law firms, their clients will also likely (if they have not already done so) demand that their law firm carry cyber insurance as a matter of good business practice.

According to insurance brokerage Aon, more than 60 out of the 250 medium and large law firms that it services have purchased cyber insurance within the last two years. Insurance broker Marsh has reported that close to 40 percent of its roughly 100 large law firm clients have purchased the insurance, up from 20 percent two years ago.

Interestingly, law firms who maintain cyber insurance might also have the best cybersecurity policies and practices, probably because before obtaining cyber insurance coverage, a law firm is typically subjected to a fairly rigorous underwriting process. Just like the physical exam typically required by insurance companies before issuing life insurance, which can prompt better personal wellness practices, a cyber insurance exam might trigger or prompt better law firm cybersecurity wellness. Moreover, while it has been suggested that having insurance encourages companies to slack off on security, some research suggests the opposite i.e. that those companies with good security practices are more likely to purchase insurance.

Just like many corporations, law firms are finding that their professional liability insurance, general liability insurance and property insurance does not cover many of the costs associated with cyber-attacks. Factors depend on the nature of the breach, the relationship of the parties, the type of the information in issue (such as personal information, intellectual property, trade secrets, and emails), the precise form of the operative policy and, if related to third-party liability claims, the allegations asserted and the type of damages sought.

Meanwhile, though the market for cyber insurance continues to evolve and grow dramatically, there still has not materialized any form of standardized cyber insurance policy language, and whether standard property casualty provisions even cover losses relating to cyber incidents often remains an open question. Stand-alone cyber insurance

policies offer broader coverage and should be explored by every law firm executive committee, along with an evaluation of the sufficiency of the law firm's liability insurance program.

Indeed, relying on a general property insurance policy for cyber-attack coverage is risky and law firms should not rely on commercial general liability policy to cover a data breach, as it most likely will not. For example, in the data breach involving Sony, the breach reportedly exposed the personal information of tens of millions of users, and Zurich American stated in court papers that as a result, Sony was the defendant in over 50 class action lawsuits. Because the Sony policy required the policyholder (Sony) to perpetrate or commit the act of publication of the personal information, the judge stated, "Paragraph E (oral or written publication in any manner of the material that violates a person's right to privacy) requires some kind of act or conduct by the policyholder in order for coverage to present." This decision highlights the hazards of relying on traditional CGL coverage policies for potential data breach coverage.

Indeed, the case law concerning general property insurance and cybersecurity is all over the map. Some examples in favor of the insured:

- *Computer Corner, Inc. v. Fireman's Fund Ins. Co.* (holding that loss of the pre-existing electronic data was tangible property damage covered by CGL policy where computer store repairing customer's computer permanently lost all the data);
- *American Guar. & Liab. Ins. Co. v. Ingram Micro*, Inc. (holding that computer data permanently lost during a power outage constituted "direct physical loss or damage from any cause" covered by first-party insurance policy);
- *Southeast Mental Healthcare Center, Inc. v. Pacific Insurance Company* (finding a direct physical loss occurred where the insured's pharmacy computer data was corrupted due to a power outage.);
- *NMS Services Inc. v. Hartford* (characterizing the erasure of vital computer files and databases as direct physical loss or damage to property for purposes of business income coverage); and
- *Hartford Casualty Insurance Company v. Corcino & Associates et al* (where the District Court of the Central District of California ruled that there is coverage under a GCL policy for a data breach involving hospital records of some 2,000 patients.)

However, not all courts have found that damage to data constitutes "direct physical loss of or damage to property" under property insurance policies For example, in Ward General Insurance Services Inc. v. Employers Fire Insurance Co., the insured was updating its computer data when the operator inadvertently pressed the "delete" key on the keyboard, wiping out critical data. The insured sought coverage for labor expenses to restore the database, in addition to income lost during the recovery period. The trial court found that the losses were not covered and the appellate court affirmed, stating:

> "Here, the loss suffered by plaintiff was a loss of information, i.e., the sequence of ones and zeros stored by aligning small domains of magnetic material on the

> computer's hard drive in a machine readable manner. Plaintiff did not lose the tangible material of the storage medium. Rather, plaintiff lost the stored information. The sequence of ones and zeros can be altered, rearranged, or erased, without losing or damaging the tangible material of the storage medium."

Other similar judicial decisions finding in favor of the insurance company include:

- America Online, Inc. v. St. Paul Mercury Ins. Co. (holding that America Online, Inc. is not entitled to insurance coverage for claims that software that it supplied to its customers damaged their computers.); and
- *State Auto Property & Cas. Ins. Co. v. Midwest Computers & More* ("Alone, computer data cannot be touched, held or sensed by the human mind, it has no physical substance. It is not tangible property.).

Under any circumstance, the question of how to design a stand-alone cyber insurance policy is nonetheless a difficult one. The actuarial challenges of predicting/gauging both the probability and the impact of a cyber-attack can in turn, make it difficult to match a cyber insurance policy with the unique risk profiles of today's global and technologically sophisticated companies. These are difficulties faced not only by insurance analysts but also by even the most experienced law firm executive committees.

Cyber-attack damages are multifaceted and unique – much more so than fire, flood, health and other more traditional insurance scenarios and models – that there is no normal distribution of cyber-attack outcomes on which to base the probabilities of future effects. As a result, there are now a dizzying array of cyber insurance products in the marketplace, each with its own insurer-drafted terms and conditions, which can vary dramatically from insurer to insurer – some effective and comprehensive and others replete with loopholes, exclusions and other troubling features.

Even the U.S. Department of Homeland Security has officially acknowledged that the cyber insurance market remains confusing for most companies and can be overlooked for all of the wrong reasons, stating in a recent report:

> "Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cybersecurity insurance market could help reduce the number of successful cyber attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection. Many companies forego available policies, however, citing as rationales the perceived high cost of those policies, confusion about what they cover, and uncertainty that their organizations will suffer a cyber attack."

To make matters worse, as opposed to disasters like fires, floods and tornadoes, today's companies who experience a cyber-attack should not expect any assistance or even compassion from the government. In fact, companies should expect quite the opposite for several reasons.

- First, the U.S. government is overwhelmed with protecting the nation's own infrastructure and does not have a SWAT team or a rescue team standing-by to assist U.S. companies after a cyber-attack;
- Second, given the many differing state privacy statutory regimes and a growing range of federal agency jurisdiction (each wielding their own unique set of rules, regulations, statutes and enforcement tools), instead of a helping hand, cyber-attack victims should expect subpoenas, enforcement actions and an onslaught of litigation. For instance, forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving PII; and
- Third, the public's (and Congress's) view of cyber-attack victims has sadly become not a view of understanding or empathy but rather a view of suspicion, skepticism and even vilification.

Traditionally, purchasing insurance coverage begins with a policy review, a risk breakdown and a range of other risk-related analytics. Law firms should, however, make sure management also considers a different "reverse-gap" approach towards that calculus.

Law firms should ask if internal insurance procurement teams have considered reviewing actual cyber-attacks, analyzing and scrutinizing the typical cyber-incident response workflow that follow most cyber-attacks. By analyzing and revisiting the realities and economics of this workflow, a law firm can then collaborate with their insurance sales representatives and originators to allocate risk responsibly and determine, before any cyber-attack occurs, which workflow costs will trigger coverage; which workflow costs will be outside of coverage; and which workflow costs might be uninsurable.

It is also crucial that law firms conduct the necessary due diligence to be sure that the cyber insurance carrier their law firm uses has a good claims paying and claims handling history and has a proven history of rapid and supportive response. When a cyber attack occurs, too often there are doubts as to coverage, which can impact incident response.

Cyber insurance polices can also differ dramatically in their goals and objectives. For example, some policies (such as the Beazley Data Breach Response policy) are designed to cover HIPAA and PCI violations, as well as other regulatory non-compliance. Other policies are geared more for direct financial losses due to wire transfer fraud. If a law firm manages trust accounts on behalf of clients, the law firm will likely require insurance coverage for direct cash losses in the event of a network intrusion that results in the unlawful transfer of funds.

Whatever the type of insurance held by a law firm, an insurance claim will undoubtedly follow, and insurance adjusters will scrutinize all invoices pertaining to the incident response and will require briefings and documentation regarding all investigative efforts. For maximum objectivity, credibility and defensibility, rather than the law firm itself, law firms will need to engage an independent digital forensic firm to investigate the breach, and at the direction of counsel, to lead any briefings with insurance carriers. Law firm

executive committees should make sure the engagement of data breach response experts is covered.

Also, when negotiating cyber insurance policies, some insurance policies will seek provisions mandating use of a specific "panel of digital forensic experts" (even if the victim firm already has a prior existing relationship with a particular firm). Law firms should consider such a provision carefully; much like choosing one's own surgeon for a heart procedure, a law firm might want the same freedom of choice when it comes to selecting a digital forensics/data breach response firm.

As an aside, law firms should also make sure that during any sort of data breach response, a professional on the incident response team, preferably counsel, maintains carefully written documentation of all efforts of the response. This will help later on when gathering the "documentation package" to present to an inquisitive insurance adjuster when seeking an insurance reimbursement for the costs of the breach.

Logging Capabilities. A law firm's logging capabilities evidence how a law firm is actively hunting for indications of compromise and whether the law firm is retaining sufficient system logs to recreate attacker behavior and determine the scope of exposure in the event of a breach incident. After a data breach, in addition to user systems like laptop and desktop computers, servers, etc., the logs of other systems such as firewalls and intrusion detection systems will also require analysis.

Exactly what logs are available relating to a cyber-attack depends on a law firm's overall cybersecurity policies and practices. Logging retention can differ dramatically among law firms – and some law firms may not have any log management system that aggregates logging information, which means that its logging information will be scattered and disorganized. Also, some companies may only preserve logs for a short period, such as thirty days, before "rolling over them" and thereby deleting the logs permanently.

Deficiencies in logging can become a major source of consternation for data breach first responders. According to the SANS Institute,

> "Deficiencies in security logging and analysis can allow attackers to hide their location, malware, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records, victims can remain blind to the details of the attack and to subsequent actions taken by the attackers. Sometimes logging records are the only evidence of a successful attack and without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Many organizations keep useful logs for compliance purposes, but attackers rely on the fact that such organizations might only rarely review their logs, and never discover that their systems have been compromised. Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files."

Logging information can include logs relating to events occurring with firewalls, operating systems, applications, anti-virus software, LANDesk, web servers, web proxies, VPNs, change auditors, DHCPs and a broad range of other audit files.

Most free and commercial operating systems, network services and firewall technologies offer logging capabilities and can contain a treasure trove of relevant evidence requiring investigative analysis and resources. Also, actual correlation and aggregation tools such as "Security Incident Management" (SIM)" or "Security Event Management" (SEM) solutions can make audit logs far more useful for subsequent manual inspection and can be quite helpful in identifying subtle attacks.

For the best results, such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required. Operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, law firms should periodically scan through its logs and compare them with the asset inventory assembled in order to ensure that each managed item actively connected to the network is periodically generating logs.

However, SIM/SEM analytical solutions for reviewing logs can only provide value, when the right expert is conducting the analysis. These tools are neither a cure-all nor a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand what is gleaned from log files.

Logging information can be of critical use during a cyber-attack response, and it is too often something management overlooks as a priority; thus, law firm executive committees should probe IT personnel about logging practices and procedures and make sure that an expert (internal or outsourced) is analyzing whatever logging information the law firm is amassing.

The Cloud. Reportedly, the cloud is now used by 64% of lawyers in their practices, which is only going to increase. Cloud storage has many potential advantages for law firms, including cost savings, scalability, increased mobility and easier collaboration. However, when a lawyer stores firm and client information in the cloud, that information is essentially stored off site, possibly in another country, and law firm executive committees should make sure their respective law firms are using cloud providers that can reasonably protect and provide assurances on overall data security.

Important due diligence questions along these lines include whether the cloud data is encrypted (in transition and in motion); who holds encryption keys; whether the cloud data is subject to search and seizure (both domestically and internationally); the nature of data protections used by the cloud firm; whether law firm clients have for the cloud data approved cloud storage; what logging exists and how long are logs maintained; how and

when cloud data is destroyed; can cloud data be technologically subject to a litigation hold; what auditing is permitted of the security capabilities of the cloud company; what types of pen testing are undertaken by the cloud firm; and what are the specific security policies and procedures of the cloud firm.

Along the same lines, cloud-based file sharing services, such as Dropbox, Box, and others, are another way confidential information leaks out of a firm. For instance, according to the American Bar Association, Dropbox saw a dramatic increase in law firm usage, going from 4 percent in 2012 to 58 percent in 2013. However, unbeknownst to many law firm executive committees, cloud services like Dropbox are often used through personal accounts (despite many large firms prohibiting, as a matter of policy, the use of such services for these purposes.) Some law firms also block access to such services from the firm's desktop computers with effective security controls, while other law firms are less sophisticated or simply resist the notion of becoming the automated "data nanny" for their employees.

Encryption. Encryption seems to be a no brainer for law firms for information transmitted as well as stored, as well as of laptops, cell phones, tablets and other mobile devices (encrypting devices in particular is a relatively easy step which can dramatically mitigate the risk to critical firm or client data). If a computer or device is encrypted, even if the laptop or device is lost or stolen, the information is arguably not accessible. Yet, surprisingly, according to a recent "ABA Tech Report," a mere 42 percent of law firms are using file encryption. This obviously needs to change.

With respect to email, there are many encryption products available – from the super technical to the more basic and there is absolutely no technical reason for not encrypting law firm data. (Even operating systems, including for Macs, come with encryption options, Apple, for example, makes it simple: just turn on FileVault.) These options include utilizing a third party service to encrypt the content of your messages, encrypting email database/file systems and encrypting emails in transit. All law firm file access should also be logged, analyzed and reported for unauthorized use or unusual activity or anomalies.

Of course, just encrypting your sensitive data is not enough. The type of encryption is of equal importance. There are a plenty of weak and easily cracked encryption implementations in the marketplace. Not much is accomplished when a law firm encrypts client data and then an attacker easily brute forces encryption keys because of an outdated or flawed algorithm.

The implementation is also critically important. For instance, a law firm could choose the most robust encryption algorithms and yet unknowingly expose the encryption keys somewhere else (e.g., in an insecure keystone or an easily crackable encrypted Excel spreadsheet) and allow an attacker to access and exfiltrate sensitive client data. Law firm executive committees should be sure to consult with a trusted encryption expert before any encryption implementation, procurement or rollout.

Spam Filters, Anti-Virus and Host Intrusion Protection. These tools should be basic for all law firms, and should be centrally managed and updated regularly. Spam filters in particular need to be kept current if they are to do an adequate job of intercepting malware laden email, a popular social engineering tactics used in cyber-attacks against law firms.

Social engineering schemes which target personal workstations (which often have the least amount of protection) through email are particularly prevalent in law firm cyber-attacks, as the attackers hope that a careless, distracted or bleary-eyed employee will click on a bogus link, allowing the hacker entry. This poses a widespread risk, considering the size of law firms today and their international and work-at-home operations. In fact, end user computers have become much more likely law firm targets for attackers, who would rather employ a simple social engineering scheme rather than try to work their way through a web server or other external-facing protections.

Law firms should also centrally run analysis programs, often called host-intrusion protection (HIP), to detect anomalies and malware that antivirus programs can often miss. This includes network monitoring as well as security software installed on desktop, mobile devices and servers.

But monitoring and security software is useless if the programs are constantly generating alerts that no one has the time to analyze. Law firm executive committees should ensure that IT departments have enough resources to staff cybersecurity monitoring and a third party to detect and respond to alerts. Outsourcing these types of responsibilities while sometimes costly, typically makes the most sense for law firms and can enable meaningful cybersecurity partnerships with long term benefits.

Indeed, outsourcing has often become the norm for most law firms, unless a law firm can have the benefit of a *Security Operations Center* capable of (1) inspecting all traffic, (2) classifying it as benign, malicious, or questionable, (3) analyzing questionable traffic rapidly to determine whether it is malicious, (4) curtailing malicious traffic (which can require reverse engineering the malicious code), and (5) taking the necessary steps to remediate any damage.

Patching and Updating. Of course, the need to update software when a patch is issued to address exposed software security flaws seems as basic as the need to take out the trash at the end of the day – and may not at first glance, seem worthy of specific law firm executive committee oversight and enforcement.

Yet, many security breaches still occur because software was not updated in a timely manner. In other words, software versions with known security vulnerabilities continue to be used by law firms, in spite of their risk. Basic procedures to update software with patches offering the latest protection are a necessity and basic expectation of all law firm stakeholders – so it is worth, at least, probing management about its software patching practices.

The recent Panama Papers hack was most likely accomplished via an outdated and unpatched version of Drupal and/or WordPress. The Mossack Fonseca site contained outdated, unpatched, and vulnerable versions of both types of software that could have been leveraged to compromise the Internet reachable servers.

No technical solution can be effective if not kept up to date. The number one reason that law firms get compromised is because of a failure to apply patches. When law firms fail to patch their operating systems and software (a typically inexpensive and routine exercise), they are inviting a cyber-attack.

Internal Threats. Recent data breaches like the *Panama Papers* breach are not just cautionary tales about the need to secure stored data or block exfiltration. The root cause and risk can just as easily be unauthorized access. Law firms must always remain acutely aware of insider threats and double-down in their due diligence of new hires, as well as re-screen them on a regular basis. Law firms executive committees might also consider using behavioral software solutions to surveil employee email, using algorithms and other technologies to detect threatening, disruptive or sloppy client data handling behavior among employees.

BYOD. Many law firms allow their employees to "bring your own devices" or "BYOD," especially given client expectations of 24-7 communication lines as well as the travel demands made upon lawyers. But BYOD also creates a broad range of risks for data breaches. Law firms should have control over every BYOD device, including all applications contained therein, as well as the ability to remotely wipe all data from devices. Law firms should also put into operation robust mobile device management platforms that support containerization of business and personal data, enhanced security controls, encryption key escrow and tracking and management of laptops, tablets, mobile phones and other mobile devices.

Password Policies. Law firms should have written and technologically enforced policies mandating that passwords are changed at certain intervals throughout the year with specified configurations and characteristics. The use of administrative passwords and administrative rights should also be tightly controlled, monitored and documented. Cyber-attackers prey in particular on administrative passwords, especially those rarely used, which can fly under the radar. Inadvertently keeping old administrative passwords or assigning too many administrative passwords can lead to massive data breaches and is an easily avoidable vulnerability. Passwords should be regularly audited for compliance with the password policy. Passwords are the first line of defense in any firm. Weak or predictable passwords make it very easy for an attacker to access external email portals or VPNs.

Law firms should have a rigorous password complexity policy. Passwords should be long (greater than ten characters), complex, random, and contain numeric, upper/lower alpha, and special characters. Easily guessed credentials, default passwords, shared passwords, and cyclical passwords (e.g. Winter2016, Spring2016), coupled with a single factor VPN, web portal, or Internet reachable email portal, can spell disaster for a law firm. Attackers will find external portals, enumerate users, and guess passwords and then start

accessing private data. Once the attacker is on the network and impersonating a valid user, detection will be more difficult, costly and time consuming.

Wireless Precautions. Law firm partners and associates spend large amounts of time on the road and are often tempted to use unknown and unsafe wireless access. Wireless access points are not much different than untrusted devices and software. Exploitation of mobile devices, including laptops, utilizing public wireless access, such as in airports, train stations and hotels is a common cyber-attacker skill. Law firm executive committees should deploy technological barriers to enforce strict policies along these lines and provide safe and secure mobile hot-spots for traveling attorneys and legal staff.

Endpoint Detection and Response. Law firm executive committees should consider the most recent wave of dedicated incident response solutions known as "endpoint detection and response" or "EDR" tools have come into being. Typically installed within a swath of IT equipment including domain controllers, database servers, and workstations, the real-time "intelligence feeding" of EDR tools will likely become a corporate cyber-security standard.

For instance, most internal data breach investigations kick off with manual data acquisition, user system forensics, and log file analysis on data aggregated and collected after the suspected cyber attack. By providing continuous monitoring and recording of activity on endpoints and servers, EDR tools reduce the need for such after-the-fact data collections. EDR tools decrease the cost, complexity, and time of internal investigations and regulatory response, while simultaneously accelerating the identification of root causes and attack vectors of data breaches.

EDR technologies also provide a richer depth of behavior-based anomaly recognition and better visibility into threats of all varieties, not just malware. For example, by providing instant aggregate threat information and decreasing the "dwell time" of targeted attacks, EDR solutions enhance enterprise visibility and help counter internal threats and malfeasance.

Flexible IT Budgeting. Most budgeting at law firms is conducted annually and planned carefully and thoughtfully before execution – yet cybersecurity budgetary priorities can shift very quickly. Thus, a one-year budgetary cycle might not be swift or agile enough to manage rapidly emerging cyber-threats. Moreover, the average cost of a data breach continues to increase. Law firm executive management should understand how cybersecurity budgeting works; how emergency items are identified and funded; and whether the budget appropriately provides for contingencies in the event of a cyber-attack or sudden cybersecurity need.

Incident Response Firm on Speed-dial. When a law firm experiences a cyber-attack, the law firm will likely need to hire an expert and experienced digital forensics/data breach response firm to investigate for several reasons. First, very few law firms employ the kind of personnel who have the technological expertise to understand and remediate today's cyber-attacks. Second, like any company in a crisis, engaging an independent and objective investigator not only insures integrity in the response but also creates a

defensible record if challenged later on (e.g. by regulators, class action lawyers, partners, customers, etc.). Finally, if the digital forensics/data breach response firm is engaged by outside counsel, a law firm can (arguably) maintain and secure the attorney-client privilege for the reports and other investigative documents pertaining to the attack.

Given the scarce number of firms who can truly investigate a cyber-attack, especially those with oft needed malware reverse engineering expertise, it makes sense to search for a firm before experiencing a cyber-attack and negotiate some sort of master service agreement.

Malware. Law firm leaders should realize the term "malware" is often misunderstood. The term "malware" is often defined as software designed to interfere with a computer's normal functioning, such as *viruses* (which can wreak havoc on a system by deleting files or directory information); *spyware* (which can gather data from a user's system without the user knowing it.); *worms* (which can replicate themselves in order to spread to other computers -- unlike a computer virus, a worm does not need to attach itself to an existing program); or *Trojan horses* (which are non-self-replicating programs containing malicious code that, when executed, can carry out an attacker's actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm).

However, the definition of malware is actually far broader. In the context of a cyber-attack, malware means any sort of program or file that is used by attackers to infiltrate a computer system. Like the screwdriver a burglar uses to gain unlawful entry into a law firm's headquarters, legitimate software can actually be malware.

For example, in a so-called *Advanced Persistent Threat* or APT attack, malware can be tricky to identify. APT attacks are typically stealthy, sophisticated, targeted and relentless state-sponsored attacks that employ a carefully crafted and evolving reconnaissance, low-and-slow approach, that is difficult to detect, and are not flagged by antivirus technologies and other traditional cybersecurity tools. In fact, most malware used by APT attackers is undetectable by off-the-shelf antivirus products.

During an APT attack, attackers will often use "RAR" files as containers for transporting exfiltrated information, yet RAR files have a broad range of legitimate uses and can be used in the context of general corporate activities. (Specifically, RAR is the native format of WinRAR archiver. Like other archives, RAR files are data containers, they store one or several files in the compressed form. After you downloaded RAR file from the Internet, you need to unpack its contents in order to use it.)

Thus, reverse engineering malware, which can be hiding in plain sight, is both an art and a science. Forensic investigators, incident responders, security engineers, and IT administrators employ a broad range of practical skills to examine malicious programs that target, access and infect corporate computer systems. Understanding the capabilities of malware is not only critical for responding to information security incidents, but it is also critical to an organization's ability to derive threat intelligence and to fortify defenses.

Yet, malware reverse engineering is costly, with hourly rates more akin to a law firm partner's rather than information technology specialists. Even finding a specialist with reverse malware engineering skills can quickly become a challenge -- educational institutions are only just beginning to graduate individuals with malware skills and most malware specialists are self-taught or are "home-grown" within digital forensic firms. Thus, law firms should bear in mind that without a competent digital forensics firm, staffed with digital forensic examiners who are skilled at malware reverse-engineering, its executives may end up feeling like a homeowner with a rapidly flooding basement -- yet no plumber to help find the leak and plug it up.

Physical Security. Contrary to many popular notions of cyber-attacks, cyber-attacks can sometimes begin with a physical breach. For instance, a cyber attack can start when an outsider surreptitiously gathers fodder for a social engineering scheme (such as a spear-phishing campaign) or when an insider (such as a so-called "bad leaver") gains access to a law firm's network and wreak havoc, without initially using malware or other clandestine technological means. Hence, a law firm's cybersecurity efforts should also involve a review of physical security of facilities, including management's plans for reception and entry checkpoints; ID scanner and other access records; video or still footage; physical logs; and even elevator and garage records.

Training Programs. The most significant cybersecurity vulnerability at any law firm will always be its employees. If law firm employees do not adhere to cybersecurity rules and requirements, an attacker's exploit becomes all the more effective and capable of doing damage. Law firm executive management should understand how often and how effective are the firms' cyber-safety training programs; who participates in the training and how does the law firm handle policy violations, especially violations by partners, who studies have shown are typically the least compliant with cybersecurity policies.

Personnel Continuity: Recruitment, Hiring and Retention. Competition for talent in the information security space is intense, while the pressure on IT security senior executives is infinite and exhausting. Moreover, despite their rapidly rising salaries, IT turnover remains constant and there is a serious shortage of experienced and capable IT senior executives, especially CISOs. Law firm management committees should understand how their respective law firms are recruiting and retaining IT security talent. Relatedly, when a law firm loses key senior IT security personnel, it is not only a red flag but also an opportunity for a law firm executive committee to examine succession plans and to obtain an unbiased, albeit possibly disgruntled, view of any cybersecurity flaws.

The art and the benefit of the exit interview is lost on so many law firms today – too often because departing employees are dismissed as resentful and unreliable. In the case of a resigning IT executive, a proper exit interview may reveal critical cybersecurity weaknesses. Upon every important IT employee departure, law firm executive management should determine if there are threats or known risks that contributed to the decision to leave; if the departure is a potential "red flag" about weak cybersecurity; and who is best placed to assume (even on an interim basis) the day-to-day IT security responsibilities. Law firm senior management should also be sure that there exists a

succession plan in their IT departments and fully understand the HR approach (if any) to reduce turnover, recruit fresh talent and retain valued employees.

Business Continuity Plan. The critical importance of a business continuity plan in the event of a natural disaster is widely recognized and accepted. Yet, too often, such plans are not evaluated in the context of assessing cybersecurity risks. Law firm executive management should determine if the law firm has properly evaluated the effectiveness of its business continuity plan in the context of a cyber-attack, and if the business continuity plan should be reconsidered and refreshed with these additional considerations in mind.

Pre-Breach Law Enforcement Liaison. Keeping up with the latest developments in cybersecurity and the latest tools and techniques being utilized by cyber-attackers is a career within itself – and requires building relationships with law enforcement, including the FBI, U.S. Air Force, Department of Homeland Security, the U.S. Secret Service and others.

For example, the FBI has created a document called the *FBI Liaison Alert System* message, or *FLASH*. Through the system, the FBI releases high confidence data to the private sector with indicators and alerts related to computer intrusions and DDoS attacks. From April 2013 to July 2014, the FBI disseminated 34 FLASH messages, about 20 of which dealt with threats against the financial sector. The FBI disseminated, among other information, indicators for approximately 115,000 compromised systems in these FLASH messages. These declassified, technical indicators, associated with intrusions, are meant to enable industry partners to be on the lookout for and defend their infrastructure from nefarious traffic on their networks.

When the FBI receives credible information regarding a threat to U.S. critical infrastructure, FBI coordinates with DHS to discuss and determine victim notification and mitigation strategies, at times involving other agencies, such as the Department of Treasury, as well. To become a part of this network, all a law firm need do is reach out.

For instance, the U.S. Department of Justice (DOJ) has made cybersecurity a primary focus of its attention. Two common scenarios in which companies such as law firms can interact with the DOJ on cyber issues are: (1) ongoing investigations into data breaches or other security incidents, some of which involve an investigative agency affirmatively notifying a law firm that it is a cybercrime victim; and (2) general public-private party outreach efforts including sharing of potential threats and vulnerabilities.

In each of these scenarios, law firms might interact with one or more of the following three principal DOJ components involved in cybercrime prosecutions: the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS), the National Security Division (NSD) and any one of the 93 individual U.S. Attorney's Offices (USAOs). CCIPS is the DOJ's cybercrime subject- matter expert. NSD is the DOJ's national security subject-matter expert and combats cyber-based threats to national security. USAOs are the DOJ's front lines in prosecuting cybercrime, and frequently interface with cybercrime victims. These three groups combined form a network of over 300 DOJ cyber prosecutors.

Law firm executive management should also understand how the law firm will address the competing constituencies that arise during a data breach. On one hand, there are the FBI, Secret Service, and other law enforcement agencies who want to help find the intruders, and on the other hand, there are the myriad attorneys general and other state regulatory agencies who will be issuing requests and demanding answers about the safety of the PII of their respective citizenries. Law firm senior management should make sure some member of the data breach response team understands the rules, practices and procedures that govern the sharing of intelligence with government agencies. That same attorney should also make overtures to law enforcement agencies to build bridges and establish communication lines before any data breach occurs.

Staying Current. Not all law firms face the same cybersecurity risks. There is no "one size fits all" approach. Law firms that house and maintain large amounts of critical information and data need to tailor any defense, mitigation and response plans accordingly. By taking steps to insure that information flow about data breaches within the industry and the latest intelligence about rising threats are considered by IT management on an ongoing basis, law firms can stay current on the latest threats and prepare accordingly. Preparedness is the key.

Law firm executive committees should determine what steps their law firms have undertaken in the realm of security science to stay current about the latest cybersecurity intrusion modus operandi, data breach trends, etc.

Conclusion. Rather than being treated like *criminal victims*, law firms experiencing data breaches should expect to be treated like *criminals,* becoming defendants in federal and state enforcement actions, class actions and other proceedings. And given in particular the 47 or so separate state privacy regimes, together with a growing range of federal agency jurisdiction, instead of accepting a helping hand, law firms (especially law firm leaders) may find themselves accepting service of process of multiple subpoenas.

These harsh realities together with the spate of large scale and recent headline grabbing cyber-attacks experienced by law firms (and that most experts believe that this is just the beginning of a new era of cybersecurity defense), mean that members of law firm executive committees will become much more actively involved in ensuring the law firms they oversee are adequately addressing cybersecurity.

Formerly looked upon as the problem of a law firm IT director, cybersecurity has quickly evolved into an issue and responsibility which the law firm management committee should understand and oversee. Law firm partners and other employees expect as much -- and *law firm clients demand it*.

Sloane Perris, Chief Legal Officer of the Atlanta-based Krystal company, summed up her expectations of law firms as follows, which provides useful insight into the evolution of client's emphasis on the cybersecurity at their engaged law firms:

> "As a client, when searching for a reputable data protection firm, I look for a few key attributes, including deep knowledge of the latest industry best practices, full

transparency as a partner, and a comprehensive crisis management protocol. First, the firm must comply with not only our own industry standard in the hospitality field, but they must follow the highest standards within the data protection and regulatory fields. Next, they need to be transparent with us, which means going above and beyond to be open about actual and potential risks and any associated exposure. Lastly, any firm I look to hire for data protection must have a clear crisis management protocol in place. If a data breach occurs, we need them to respond appropriately and urgently to protect our data. In short, we're looking for a partner who can help us navigate through an incident that could easily cripple our brand."

In the aftermath of a corporate cyber-attack, law firms and their clients are subjected to immediate public scrutiny and, in many cases, unwarranted criticism. This new cyber-reality has essentially removed the distinction between law firm executive and IT executive.

But cybersecurity engagement for law firm executive committee members does not mean that they should obtain computer science degrees or personally supervise firewall implementation and intrusion detection system rollouts. Law firm leaders can accomplish oversight of cybersecurity in two ways. First, by using the concerns outlined in this guide to become actively involved in ensuring the law firms they oversee are adequately addressing cybersecurity. Second, and most importantly, by approaching the subject in much the same way as they would probe a law firm's internal financial statements and reports: with a vigorous, skeptical, intelligent and methodical inquiry.