Journal of Technology Law & Policy

Volume XIV – Spring 2014

ISSN 2164-800X (online)

DOI 10.5195/tlp.2014.145

http://tlp.law.pitt.edu

What Does It Take to Survive a Breach in Today's High-Risk World? *When Your Prevention Fails (and It's Going to Fail), What Do You Do?*

Scott M. Angelo

What Does It Take to Survive a Breach in Today's High-Risk World? *When Your Prevention Fails (and It's Going to Fail), What Do You Do?*

Scott M. Angelo*

INTRODUCTION

It's Monday morning, and while sipping on what will be your first of many cups of coffee, you receive an unannounced and unexpected visit by two agents representing the Federal Bureau of Investigation's Cyber Division. Not your typical visitors. They provide you with detailed information, suggesting that your firm has been targeted and subsequently breached by an international hacking organization. They proceed to tell you that this unauthorized access has most likely been going on for close to a year, and that it deals with theft of pharmaceutical research and development information. You immediately recall a matter that the firm is actively engaged in with one of its most-influential clients regarding advanced research pertaining to a breakthrough cure for cancer. According to the *Verizon 2013 Data Breach Investigations Report*, "it might not be your data they're after at all. If your organization does business with others that fall within the espionage crosshairs, you might make a great pivot point into their environment."[1]

The future of your firm's brand now relies on the maturity of your current security program, and how well it has been managed over the past year. More importantly, the type of conversation that you are going to have with your client is going to be based on your security program. Do you have the right security protocols in place to address the threat? This story is not an episode of *CSI*, but rather, a real-life depiction of what happens to any organization, particularly one that does not take steps to drastically enhance its cybersecurity initiatives. Unfortunately, stories like the above have become all too common in today's business environment.

The goal of this article is to address the real cybersecurity concerns that face the legal industry today and furthermore, to demonstrate how a firm can effectively

* Global Chief Information Officer, K&L Gates.

[1] *2013 Data Breach Investigations Report*, VERIZON, 16 (2013), *available at* http://www.verizonenterprise.com/DBIR/.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

mitigate the risks that exist by taking a proactive approach to cybersecurity. Part I provides some sobering statistics surrounding the reality of cyber-terrorism. Part II explores the components necessary to build a robust security program capable of protecting a firm against Advanced Persistent Threats. Part III highlights what critical factors must be considered when building a world-class security program. And last, but certainly not least, Part IV reflects on what can be done to strengthen the legal industry as a whole in the war on cybersecurity.

I. WHAT DO THE STATISTICS SAY, AND WHAT DOES THIS MEAN FOR US?

The statistics that support the opening of this article are unfortunately more fact than fiction. Approximately 70% of breaches are discovered by external parties.[2] News of scenarios like the one above could come from our own clients, calling to tell us that their information has been compromised. What is even more frightening is that many of these breaches, roughly 66% of them, go undiscovered for more than a month,[3] leaving the potential for an even greater breadth of exposed information. In 2013, there were 2,164 reported security incidents, involving the exposure of more than 822 million records.[4] In 2012, federal agents notified more than 3,000 U.S. companies that their computer systems had been hacked.[5] Those are scary, but very real, statistics.

Law firms are not immune; no one is. However, law firms can take active measures to counteract groups and individuals trying to cause them harm. According to House Intelligence Committee Chairman Mike Rogers, "there are two kinds of companies: those that have been hacked and those that don't know it yet."[6] In 2012, Mandiant, a security consulting firm, estimated that 80% of the 100 largest American law firms had some malicious computer breach in 2011.[7] This is why it

[2] *Id.* at 53.

[3] *Id.* at 52.

[4] *An Executive's Guide to 2013 Data Breach Trends*, RISK BASED SECURITY, 1 (2013), https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf.

[5] Corey Nachreiner, *Profiling Modern Hackers: Hacktivists, Criminals, and Cyber Spies. Oh My!*, WATCHGUARD SECURITY CENTER (May 30, 2013), http://watchguardsecuritycenter.com/2013/05/30/hacker-profiles/.

[6] Brian Fung, *When Corporations Are Hacked, Who Should Know?*, NATIONAL JOURNAL (Apr. 4, 2013), http://www.nationaljournal.com/magazine/when-corporations-are-hacked-who-should-know-20130404.

[7] *Mandiant Trends: An evolving threat*, MANDIANT (2012), https://dl.mandiant.com/EE/assets/PDF_MTrends_2012.pdf.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

is critically important to take necessary measures to reduce our risk by safeguarding our data and the data of our clients.

Let's revisit the hypothetical scenario above. After the fear, uncertainty, and doubt subside, and your preliminary investigation is over, you determine that the breach originated from a state-sponsored actor, and presents a real advanced persistent threat ("APT"). Not all threats are created equal, and understanding the level of threat you are trying to protect against is critical. APTs are defined as:

> A set of stealthy and continuous hacking processes often orchestrated by humans targeting a specific entity. APT usually targets organizations and/or nations for business or political motives. APT processes require high degree of covertness over a long period of time. . . . The threat process indicates human involvement in orchestrating the attack.[8]

APTs aim to attack the very heart of a business, and are often discovered months after an initial infiltration, leaving organizations at extreme risk. If you are a global law firm representing companies on complex matters, it is crucial to develop a program which directly focuses on APT-level countermeasures.

II. WHAT SECURITY PROGRAM IS "BEST" FOR ME?

What are the requirements for building a security program within the legal industry capable of protecting against an APT? There is no detailed roadmap that outlines all the steps a law firm should take to protect its data, but there are numerous frameworks, standards, and industry-related requirements available. Other industries have safeguards in place. For example, health care has the Health Insurance Portability and Accountability Act ("HIPAA");[9] financial services have a variety of requirements, such as those outlined in the Federal Financial Institutions Examination Council handbook;[10] and retailers have the Payment Card Industry Data Security Standards.[11] This is by no means a comprehensive list of industries

[8] *Advanced Persistent Threat (APT)*, SEARCHSECURITY, http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT (last updated Nov. 2010).

[9] Health Insurance Portability and Accountability Act of 1996, Pub. L No. 104-191, 110 Stat. 1936.

[10] *What is the InfoBase*, FFIEC IT EXAMINATION HANDBOOK INFOBASE, http://ithandbook.ffiec.gov/ (last visited Mar. 2014). *See also FFIEC Council*, FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, https://www.ffiec.gov/ (last visited Mar. 2014) (describing FFIEC's mission).

[11] *PCI SSC Data Security Standards Overview*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/security_standards/ (last visited Mar. 2014).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

or requirements; however, these industries have at least prescriptive guidance on what kind of controls are required for the protection of their respective information. Law firms have no prescribed requirements, and are often left to their own devices. Updated ethics rules require lawyers to make "reasonable efforts" to ensure client data is secure;[12] new rules also require lawyers to be "competent" with technology.[13] What is reasonable and what level of competence is going to be enough?

Regardless of industry requirements, there are several key components that are critical to the effectiveness of any security program and it is imperative that these components are tailored to the individual firm based on its own unique operating characteristics.[14] Too many organizations make the mistake of treating security as a one-size-fits-all initiative. Fifty percent of organizations believe that their current employed security controls are adequate in protecting their data from advanced attacks.[15] This false sense of security is reason for concern.

III. COMPONENTS THAT ARE CRITICAL SUCCESS FACTORS IN A FIRM'S SECURITY PROGRAM

The intent of this article is not to address in detail all of the requirements necessary to ensure a program's effectiveness, but to provide an overview of how the components risk, people, process, and technology are critical success factors in a firm's security program.

A. Defining Risk, Vulnerabilities, and Threats

To provide applicable cybersecurity solutions in today's virtually connected world, it is critical to understand the risks, threats, and vulnerabilities that exist. The first area I will focus on is risk: I have used the following basic risk equation for close to twenty years now to teach new security practitioners about risk

[12] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2013) (stating: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.").

[13] *See* MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (2013) ("To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.").

[14] Including, but not limited to, practice areas, geographic footprint, client base, and information types.

[15] Helena Brito, *Five Reasons You're a Prime Target of Cybercriminals*, FIREEYE (Mar. 25, 2014), http://www.fireeye.com/blog/corporate/2014/03/five-reasons-youre-a-prime-target-of-cybercriminals.html.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

management and how to design highly effective security programs. Furthermore, a well-defined risk management approach to building and maintaining a security program ensures a tailored and pragmatic set of controls based on your business's operating model.

1. RISK = (Vulnerability + Threat) – Countermeasures

The basic premise of this equation is that you cannot have a risk unless you have both vulnerability and a corresponding threat with the capability of exploitation, or in other words, a lack of countermeasures.

i. Vulnerability

Let's discuss the first piece of the risk equation, which is often the single biggest failure companies and practitioners make, specifically, remaining vulnerable to attacks. Vulnerability is "a weakness which allows an attacker to reduce a system's information assurance."[16] They are often mechanical in nature, and are usually well documented and quick to be identified, categorized, and sometimes even glorified. Vulnerabilities are passive in nature, meaning that in the history of vulnerabilities, no one has ever been compromised via vulnerability alone. Vulnerabilities cannot exploit themselves, but rather, require a catalyst to act on the opportunity vulnerabilities present to a firm. Analogous to an explosive device, which requires an ignition (threat) and an igniter (exploitation), vulnerabilities require someone or something (an attacker) to take advantage of the identified weakness and infiltrate the system.

These vulnerabilities are documented in what is called the "CVE," which is a "dictionary of publicly known information security vulnerabilities and exposures."[17] Since 1997, there have been over 60,000 vulnerabilities identified and documented; there have been over 12,000 new vulnerabilities in the last 27 months alone (January 2012–March 2014).[18] Fortunately, because these vulnerabilities can be well defined, vendors have developed vulnerability scanning tools and services to help organizations identify, detect, and remediate them.

The primary role of a vulnerability scanner is to detect weaknesses within a system. Let it be noted that these scanners detect only basic vulnerabilities which have previously been discovered and should only be considered a basic form of

---

[16] *Vulnerability (Computing)*, WIKIPEDIA, http://en.wikipedia.org/wiki/Vulnerability_(computing) (last modified Apr. 24, 2014).

[17] *Common Vulnerabilities and Exposures*, CVE, http://cve.mitre.org/ (last updated Mar. 17, 2014).

[18] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

detection. Vulnerability assessments of an organization performed either internally or by third-party companies, often result in large numbers of verified "high" vulnerabilities. These vulnerabilities often create fear, uncertainty, and doubt within a leadership team. The key item to remember is that the vulnerabilities identified require an accompanying threat, and the severity of that threat is dependent on its exposure; for example, is this system externally accessible?

A common example of vulnerability is referred to as a "zero-day vulnerability," or a hole in software that is not known to the vendor.[19] This gap is capitalized on by hackers, and typically developers rush to fix these holes in their software; these fixes are called "patches," which you have probably seen applied to various applications and tools that you use every day. These patches help resolve identified issues; ideally, before the hackers can cause any major problems. However, zero-day vulnerabilities render the majority of organizations defenseless, as their defenses are based on known vulnerabilities. A targeted, dynamic APT is almost impossible to defend against. These are the type of exploits used in high-profile attacks, such as Google Aurora, which was an "ultra-sophisticated" hack.[20]

Now that we have an understanding of what vulnerabilities are, we can begin to talk about the threats, or the igniters.

ii. Threats

Threats come in many different forms, making them even more challenging to identify and mitigate. To even begin to address potential threats, you must understand your business. For example, in a law firm, it is critical to not only grasp the service that is being provided, but it is also important to know the types of matters that are being handled, and whether or not any of the information is potentially valuable to someone else. Given the nature of a law firm, it is highly likely that this type of information is exchanged. Information, such as trade secrets, intellectual property, pre-initial public offering information, or corporate strategies, is just some of the type of data that is highly desired by outside parties.

A simple way to understand the threats is to know how they are categorized. Most often, they are broken down into three main types:

---

[19] *What is a Zero-Day Vulnerability?*, Posting under *Security News*, PC TOOLS, http://www.pctools.com/security-news/zero-day-vulnerability/ (last visited Mar. 21, 2014).

[20] Matthew J. Schwartz, *Google Aurora Hack Was Chinese Counterespionage Operation*, Comment to *Attacks/Breaches*, INFORMATION WEEK DARK READING (May 21, 2013, 12:58 PM), http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

- **Hacktivists:** The act of hacking or breaking into a computer system, usually for politically or socially motivated purposes. One well-known "hacktivist" group is the Syrian Electronic Army ("SEA"). These individuals are strong supporters of the Syrian government, and they mainly target western websites and humanitarian groups.[21] The SEA has attacked major organizations such as the *New York Times* and *Forbes*, and is capable of not only defacing websites, but potentially exposing individuals to other malicious websites and code.[22]

- **Criminals:** This is the most-common type of threat, usually performed either by a group or an individual driven to make a profit from information. In May 2013, thieves stole $45 million dollars from banks without ever setting foot in one. The unnamed hackers infiltrated a credit card system and obtained access to customer's personal information, allowing the criminals to withdraw millions of dollars from thousands of accounts.[23]

- **Nation states (or state-sponsored organizations):** This type of threat is relatively new and quite concerning, because these types of organizations are backed by governments. Due to the financial resources available to these groups, they are able to utilize the most-advanced technologies, systems, and talent, creating some of the most stealthy and impactful threats.[24]

These threats are omnipresent, and cause serious concern in today's business environment for a variety of reasons. Not only do they aim to compromise valuable information, but they also seek to infiltrate and destroy systems, and gain access to proprietary and very sensitive documentation.

Knowing these threats are imminent, and understanding the potential implications of these threats when coupled with vulnerabilities, how can we best protect ourselves from those who wish to cause us harm in such nefarious ways? What can you do to safeguard yourself and your industry from such advanced and capable attackers, and has your firm made the right investments? I will examine

---

[21] Laura Smith-Spark, *What is the Syrian Electronic Army?*, CNN (Aug. 28, 2013, 5:19 PM), http://www.cnn.com/2013/08/28/tech/syrian-electronic-army/.

[22] *Id.*

[23] Marc Santora, *In Hours, Thieves Took $45 Million in A.T.M Scheme*, N.Y. TIMES, May 9, 2013, http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?_r=0 Security News.

[24] Nachreiner, *supra* note 5.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

these questions more closely while reviewing the three key components that should drive any advanced cybersecurity program: people, processes, and technology.

B. People

As the old adage goes, "knowledge is power," and this could not be more applicable to how valuable knowledgeable cybersecurity professionals are to any effective defense system. Cybersecurity is a globally recognized profession and many universities now offer anywhere from bachelor degrees to PhDs in this field of study. In addition to education available in this area, the Certified Information Systems Security Professional ("CISSP") is a highly sought-after certification, governed by International Systems Security Certification Consortium, a non-profit group committed to Information Security education and certification.[25] In addition to the CISSP, another well-respected certification is the Offensive Security Certified Professional designation. This is governed by Offensive Security, and requires individuals to demonstrate their ability to "research the network (information gathering), identify any vulnerabilities, and execute tools, including modifying exploit code, all with the goal to compromise the systems and gain administrative access."[26] This test demonstrates an individual's ability to efficiently identify holes within security programs and effectively exploit them, simulating what a penetration testing scenario or an attack would really be like.[27]

Simply relying on other information technology ("IT") professionals to perform the work of an IT security professional is a mistake many organizations make. While those individuals might understand the basic tenets of security, they lack the in-depth knowledge to provide a more-advanced and robust system. Hiring and properly maintaining a team highly skilled in cybersecurity is the first indicator that an organization takes cybersecurity seriously. Without the proper knowledge and skills in place, the processes and technologies necessary to defend against threats cannot be as effectively implemented. Knowing how advanced hackers are, how can you even begin to address the protection of your information without your own highly skilled cybersecurity professionals?

---

[25] *CISSP—Certified Information Systems Security Professional*, (ISC), https://www.isc2.org/CISSP/Default.aspx (last visited Mar. 2014).

[26] *Offensive Security Certified Professional*, OFFENSIVE SECURITY, http://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/ (last visited Mar. 2014).

[27] *See id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

C. Process

You have the right people in place. Now it is time to look closely at your processes, specifically the policies and procedures that drive network access and usage. Cybersecurity policies and protocols are a necessity, and should serve as the basis for any comprehensive security education and awareness program. An "Information Technology Acceptable Use Policy" should clearly define usage parameters and expectations, and should be maintained and reviewed regularly. Training and annual acknowledgment of these policies should be required to ensure individuals have the proper education and awareness regarding the use of systems, software, and devices.

Proper policies allow an organization to hold individuals accountable, and enable them to share in the goal of protecting a firm's most-valuable information. This information should be audited for compliance on a regular basis, and should be driven from the top of an organization down. Even those at the most-senior levels of an organization should be required to demonstrate that they take the protection of client data seriously, and adhere to the standards set forth within the policies.

Some of the most-significant threats to any security program are social-engineering and phishing, which are designed to bypass even the best technology-based controls. Social engineering is when a hacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.[28] Phishing is a form of social engineering where the attackers use e-mail or malicious websites to solicit personal information by posing as a trustworthy organization.[29] The most effective, and often only, defense is end-user awareness.

D. Technology

The final critical component is technology. Unfortunately, this is where I most often see organizations make significant mistakes in the establishment of an effective security program. There are many technical security controls available that can adequately address many of the risks that firms face on a daily basis; however, the tool I would refer to as a "technical control" is only as good as it is configured. For example, you can purchase anti-virus software, but if it is not configured properly, it might not be protecting you as well as you think. Many of the security tools required for an effective security program are complex and

---

[28] Mindi McDowell, *Security Tip (ST04-014) Avoiding Social Engineering and Phishing Attacks*, UNITED STATES COMPUTER EMERGENCY READINESS TEAM (US-CERT) (Oct. 22, 2009), http://www.us-cert.gov/ncas/tips/ST04-014 (last revised Feb. 6, 2013).

[29] *Id.*

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

require daily management, configuration, and modification. This relates directly back to the people aspect, as well; specifically, how critical it is to have professional security practitioners there to administer and maintain these tools.[30]

More often than not, a tool is implemented by a third-party vendor based on a "cookie cutter" model, and is left unaltered for long periods. This structure provides a business nothing more than a false sense of security. Typical anti-virus and anti-malware software is not enough; tools that monitor system activity and scan for vulnerabilities are also important to a robust defense, and all should be used simultaneously to monitor systems and activity. Anti-virus software is less than 5% effective against new viruses.[31]

The expected outcomes of an effective security program are to prevent as many risks as possible, detect the risks that successfully bypass your prevention strategy, and finally monitor "all" activity on your firm's technology platform. There is no program that exists today that is capable of ensuring 100% prevention and/or detection of risks. However, firms are capable of monitoring as much of their network as their risk model would allow. My professional opinion is that monitoring capability, such as Security Information and Event Monitoring ("SIEM"), will serve a firm with the most value in the case of a breach (and we know that a breach is going to happen eventually).

SIEM technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources.[32] It also supports compliance reporting and incident investigation through analysis of historical data from these sources.

A comprehensive SIEM allows a swift response to an incident. This system should include the collection of data from as many devices as possible (e.g., authentication devices, network traffic, web browsing, databases, and security logs). These resources are critical to an effective incident-response capability and allow an organization to replay the hacker's movements and subsequent actions. Only this level of knowledge can provide a firm with an understanding of the source of the problem, and begin to suggest solutions. The level of monitoring a

[30] *See* Part IV.B *supra*.

[31] Nicole Perlroth, *Outmaneuvered at Their Own Game, Antivirus Makers Struggle to Adapt*, N.Y. TIMES, Dec. 31, 2012, http://www.nytimes.com/2013/01/01/technology/antivirus-makers-work-on-software-to-catch-malware-more-effectively.html?pagewanted=all&_r=0.

[32] *Security Information and Event Management (SIEM)*, GARTNER, http://www.gartner.com/it-glossary/security-information-and-event-management-siem (last visited Mar. 31, 2014).

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

firm performs successfully will determine the level of compromise that the breach caused, and consequently, determine the appropriate level of disclosure. This is why monitoring can be the difference between a minor breach and a catastrophic compromise.

Monitoring via SIEM allows for an alternative ending to our hypothetical scenario.[33] Let's say that the company had a very robust monitoring and incident response capability. After performing an extensive post-breach investigation, the firm determined and validated through monitoring data exactly how the criminal circumvented the firm's prevention and bypassed its detection controls. Consequently, based on this new threat data, the firm understands what adjustments to its program are required to prevent future incidents based on the same threat vector. Furthermore, and probably most importantly, the firm was able to verify via monitoring logs that, although the breach did happen, no unauthorized access was granted to client data due to other internal controls based on the firm's in-depth defense strategy. In this alternative ending, both the trust in and brand of the firm were preserved. Consider SIEM one of the most-fundamental and critical components of your security program. Monitoring and detection are the only ways you will ever discover crafty attacks when other countermeasures fail.

IV. How Can We Strengthen the Legal Industry?

In addition to the aforementioned, there are two major initiatives that would not only make a difference from a cybersecurity perspective, but would make a very clear statement that the legal industry places a major emphasis on the protection of data. The first initiative would be driven from the legal side of the industry in the area of minimum continuing legal education ("MCLE") requirements. Establish cybersecurity education and awareness as an approved continuing legal education requirement for all attorneys. Emphasizing cybersecurity as a minimum requirement would make a profound statement by the legal industry that it takes the protection of client information seriously. Several states have already warmed to the concept of providing MCLE credit for technology training that enhances a lawyer's proficiency and competency as it relates to client service. However, this topic reaches far beyond traditional "technology training." Instruction in cybersecurity and the protection of client data is not only a technology issue, but a risk-management and client-protection issue, as well. Even if state MCLE boards do not recognize cybersecurity training as a mandatory component of the MCLE requirement, similar to ethics, elimination of bias, or substantive legal curricula, at a minimum, they should accredit these types

[33] *See* Introduction *supra*.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

of programs to ensure that all lawyers are made aware of the significant risks associated with the use of technology, cybersecurity, and data protection in the practice of law. In a recent report to the Board of Governors of the American Bar Association by the ABA's Cybersecurity Legal Task Force, Principle 5 states that: "Training, education, and workforce development of government and corporate senior leadership, technical operators, and lawyers require adequate investment and resourcing in cybersecurity to be successful."[34] To this end, it is essential that all state MCLE organizations recognize this type of accredited training and continuing education.

The second shift that would increase cybersecurity prevention in the legal field would be establishing an information sharing and analysis center ("ISAC") focused on the legal profession. This ISAC would provide more legal-specific services, such as intelligence and information sharing, incident response, risk management, threat research, leading practices, and general knowledge transfer. The financial and retail industries, which are targets of cyber-crime, have created ISACs in the management of their respective cyber risks. If the legal industry also had such a group, additional and necessary information-sharing would take place, helping prevent future attacks.

CONCLUSION

The threat of cyber attacks is real, and immediate steps must be taken to achieve safer and more-secure environments in today's legal industry. When there is a knock on the door by an external entity (law enforcement, client, etc.) regarding some type of suspicious hacker activity, it is too late to start thinking about what to do. It is critical to start now, enhancing our controls by eliminating what I believe are the four most-prominent mistakes that organizations make:

Mistake #1: Most organizations, regardless of industry, focus heavily on prevention versus detection and monitoring. The criminals will continue to enhance and perfect their craft, and consequently, your prevention-based program is going to fail. Detection and monitoring via SIEM is critical to a meaningful security program.

Mistake #2: Focus on vulnerabilities versus threats. In order to tailor a security program's effectiveness to your firm, you must focus more on the threat of exploitation, rather than vulnerabilities alone. The availability of vulnerability

[34] Cybersecurity Legal Task Force, *Report to the Board of Governors*, AMERICAN BAR ASSOCIATION (Nov. 2012), *available at* http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cybersecurity_res_and_report.authcheckdam.pdf.

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu

information has made the risk equation asymmetrical and tends to be a focus trap. The more you can factor threat into your program, the more accurate it will be to manage your risk.

Mistake #3: Lack of effective security education and awareness programs. The criminals know this and will continue to target your end-users' lack of awareness. If you want a fighting chance, you will need to focus efforts on this part of your program and modify it often to meet the risks associated with your firm. Security is a team effort, but individual responsibility is most effectively addressed through training.

Mistake #4: Assuming that any IT professional can second as a cybersecurity professional. Cybersecurity is a profession, and the sooner you realize it, the better off you will be. Furthermore, you can only outsource so much regarding an effective security program. If you are serious about cybersecurity, show it by hiring professionals. Invest in cybersecurity professionals and get them focused on staying sharp and proactively defending your organization.

Firms must continue to strengthen their security programs through a well-balanced defense-in-depth strategy to meet the ever-changing environment that is cybersecurity. We know that attackers are continuing to evolve, and it has been said that the act of hacking is what cyber criminals think about first thing in the morning and is the last thing they think about before they go to sleep at night. I would add that they probably dream about their next big exploit. As their obsession for exploitation continues, we must realize that we are not unique as an industry. Every organization has the potential to be affected by attacks. So, the question remains, what are you going to do about it? It is never the risk that causes damage or creates opportunities; it is how we respond . . . before, during, and after. Are you prepared to effectively respond?

Volume XIV – Spring 2014 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2014.145 ● http://tlp.law.pitt.edu