bsi.

...making excellence a habit.™

Cybersecurity in the Legal Community

Background and overview

A Whitepaper

Executive Summary

It's never been more important to protect the information in your law firm. Cybersecurity attacks have become more prevalent and sophisticated, supply chains are more complex and the volume of personal data and business information (such as financial services, health care, and other regulated industries) handled by law firms continues to increase. Cybersecurity attacks show no signs of slowing down in 2017.

If you don't make sure your client information is secure, you could risk financial penalties or fines as well as damage to your law firm's reputation. Implementation of strong cyber controls, however, result in law firm survival, retention of clients, and preservation of trust.

Here are three ways cyber underinvestment and negligence can cause real harm to your law firm, even if your law firm hasn't had a data breach.[1]

- Your law firm can't survive an initial third party vetting using a standardized cyber risk assessment
- Your existing clients are forced to change firms because some haven't complied with heightened cybersecurity standards
- Your competitors offer more security and your clients opt to entrust their data to firms with strong, documented cybersecurity practices

You simply cannot afford not to have an information security management system (ISMS) in place to protect the client information in your law firm's data systems. Fortunately, the controls of ISO/IEC 27001, the international standard for an ISMS, offer a framework to address those areas most frequently attacked. [2] The increasing acceptance of ISO/IEC 27001 by the legal community is meeting the ever-increasing demand that law firms have evidence of a formal ISMS for protecting client data. [3] Law firms and clients are considering ISO/IEC 27001 certification to validate their data security and establish a competitive advantage. This paper describes the value of ISO/IEC 27001 risk-based security controls for protecting client information in law firms from cybersecurity attacks, and the benefits and challenges of aligning your law firm's ISMS with ISO/IEC 27001.

With the extensive use of electronic data and communications, protecting the transmissions and storage of privileged client information from inadvertent and unauthorized release, as well as deliberate interception and diversion, has become one of the most important concerns for the legal community, including law firms of all types and sizes.

---

[1] "Three Ways Cybersecurity Can Put Your Firm Out of Business (Perspective)," Bloomberg Law, November 2016, See https://bol.bna.com/three-ways-cybersecurity-can-put-your-firm-out-of-business-perspective/.

[2] ISO/IEC 27001: 2013 Information technology – Security techniques – Information security management systems – Requirements.

[3] "Law firms must manage cybersecurity risks," ABA Journal, March 1, 2017. http://www.abajournal.com/magazine/article/managing_cybersecurity_risk.

ISO/IEC 27001, the International Standard for Information Security Management

There are a number of accepted frameworks and standards that can serve as references for developing, implementing, and maintaining an appropriately-tailored cybersecurity program. [4] A cybersecurity program is comprised of a series of activities. These activities include, for example: governance by boards of directors and/or senior management; development of security strategies, plans, policies and procedures; creation of inventories of digital assets; selection of security controls; determination of technical configuration settings; performance of annual audits; and delivery of training. [5]

A successful implementation of an ISMS in a law firm requires leadership, management commitment, competence, and sufficient resources.

Evidence shows that law firms are obtaining ISO/IEC 27001 certification as a means to validate their security profiles. There are benefits to selecting ISO/IEC 27001 for setting up your law firm's ISMS. ISO/IEC 27001 is the only internationally-recognized standard that provides a roadmap to develop an ISMS and provides a set of controls that are scalable and applicable to organizations of all types and sizes. ISO/IEC 27001 specifies the "requirements for establishing, implementing, maintaining and continually improving an ISMS." [6] The management systems standard was developed by consensus over a period of years by subject matter experts from scores of nations, so it's safe to say that ISO/IEC 27001 is the global standard for information security. ISO/IEC 27001 is one of the few security frameworks to which an organization can be formally audited and certified by an independent third party.

ISO/IEC 27001 provides requirements for an information security management system (ISMS) that "preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed."

ISO/IEC 27001: 2013 Information technology – Security techniques
Information security management systems – Requirements, Introduction, p. v.

[4] American Bar Association, Revised Resolution 109, August 2014, Report, p. 6. See,http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity/aba-policy-initiatives.html>.

[5] Id. <http://www.americanbar.org/groups/leadership/office_of_the_president/cybersecurity/aba-policy-initiatives.html>.

[6] Introduction, ISO/IEC 27001 – Security techniques – Information security management systems – Requirements, p. v.

ISO/IEC 27001 helps you manage, protect, and store information whether internally or externally with third party vendors. Client information remains safe and secure, helping you build a responsive and resilient law practice. A growing number of professionals are maintaining business continuity, protecting client data, and fulfilling their ethical and professional responsibilities, using modern management systems standards.[7] While the implementation of and certification to global best practices standards can be challenging for most organizations given the resources required, a number of law firms are aligning themselves with ISO/IEC 27001, and ISO 22301, the international standard for business continuity management programs. [8]

Lawyers' Professional Responsibilities to Clients

The American Bar Association's (ABA) ethics rules require lawyer confidentiality, competence, and supervision that necessitate adopting safeguards and controls for the protection of data systems.[9] The rationale for ethical legal conduct stretches back through the centuries. A profession's most valuable asset is its collective reputation and the confidence which that reputation inspires. The legal profession especially must have the confidence of the community. With the extensive use of electronic data and communications, protecting the transmissions and storage of privileged client information from inadvertent and unauthorized release, as well as deliberate interception and diversion, has become one of the most important concerns for the legal community, including law firms of all types and sizes.

"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."

ABA Model Rules of Professional Conduct, Rule 1.6

Lawyers' Duty to Maintain Reasonable Knowledge about Technology

The ABA has determined that lawyers need to maintain reasonable knowledge about technology or have someone on staff that does. This ethical obligation is rooted in providing 'competent representation' to the client. The obligation has not gone unnoticed by lawyers charged with safeguarding the standards of the profession of law.

[7] For example, 63% of organizations report using ISO 22301 in guiding their business continuity management programs. Business Continuity Institute, Horizon Scan Report 2017.

[8] ISO 22301: 2012 Societal security - Business continuity management systems – Requirements.

[9] Jill D. Rhodes and Vincent I. Polley, The ABA Cybersecurity Handbook, A Resource for Attorneys, Law Firms, and Business Professionals, American Bar Association, 2013, pp. 62-67.

[10] "ABA begins offering cyber liability insurance to lawyers, law firms of all sizes," ABA News Release, February 28, 2017. http://www.americanbar.org/news/abanews/aba-news-archives/2017/02/aba_begins_offering.html.

"As the number of cyber breaches increases everywhere and throughout all industries, it is critical that lawyers and law firms that rely on vast amounts of electronic data are protected," ABA President Linda A. Klein said. [10]

Lawyers should keep abreast of changes in the law and its practice, "including the benefits and risks associated with relevant technology," to ensure that clients receive competent and efficient legal services. [11] Attorneys have an obligation to safeguard data relating to clients. This obligation may be achieved by approaching information security as a process, including competence, available assistance, security awareness and training, technology, and security options and controls over time.

This ethical obligation is complemented by the ABA Model Rules of Professional Conduct, such as Rule 1.6 Confidentiality of Information. [12]

"We live in a world where our national security is threatened by cyberterrorists, and where private enterprise is forced to respond to cybertheft of intellectual property on a daily basis. The ABA Cybersecurity Legal Task Force is examining risks posed by criminals, terrorists and nations that seek to steal personal and financial information, disrupt official infrastructure, and wage cyberwar. When our national security and economy is threatened, lawyers will not stand on the sidelines."

- Laura Bellows, Past President, American Bar Association

The Legal Community Prepares for Cyberattacks

How is the legal community responding to the constant threat of cyberattacks, and how are American lawyers maintaining their professional obligations to their clients of competence, confidentiality, and supervision in response to this global threat?

First and foremost, the American Bar Association (ABA) formed the Cybersecurity Legal Task Force as part of the Standing Committee on Law and National Security to develop guidance for its members. The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals (2013) provides threat information, practical guidance and strategies to lawyers and law firms of all sizes, and explores the relationship and legal obligations between lawyers and clients when a cyber-attack occurs. Amendments to the ABA Model Rules of Professional Conduct (Model Rules) adopted in 2012 provide that a lawyer's duty of competence includes keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology (Comment [8] to Model Rule 1.1).

---

[11] Client-Lawyer Relationship, ABA Model Rule 1.1: Competence. ABA Model Rules of Professional Conduct.

[12] ABA Model Rules of Professional Conduct. See, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html

Further, to enhance the protection of client confidential information, Model Rule 1.6 (Confidentiality of Information) provides that a lawyer shall make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." The touchstone regarding lawyers' obligations under Model Rules 1.1 and 1.6 is reasonableness. What is reasonable depends on the circumstances. With regard to data security, the Comments to Model Rule 1.6 provide lawyers with a nonexclusive list of factors designed to help them assess the reasonableness of their actions.

In 2013, the Task Force concluded, "Information security represents an increasingly important issue for the legal profession. Sophisticated hacking activities on private computer systems and networks, including on those utilized by lawyers and law firms, have increased dramatically over the last decade. These information security breaches expose clients, their lawyers, and society at large to significant economic losses. Further, these breaches undermine the legal profession as a whole by threatening client confidentiality, the attorney-client privilege, and the broader confidential lawyer-client relationship." [13]

The Task Force followed up a year later with a report on cybersecurity, concluding with Resolution 109, "Resolved, That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected." [14] This year, 2017, the Standing Committee's Task Force joined the Standing Committee on Disaster Response and Preparedness in support of Resolution 108 and Report on Community Resilience by adding paragraphs on cybersecurity preparedness that emphasize the importance of cyber-specific incident plans, education and training, and routine cyber exercises. [15]

---

[13] American Bar Association, Resolution 118, August 2013, Report.

[14] American Bar Association, Revised Resolution 109, 2014. This resolution was followed in 2015 by Resolution 118 focused on necessary funding for cybersecurity programs for courts. See, http://www.americanbar.org/content/dam/aba/images/law_national_security/Aug-2015-Cyber-Res.pdf

[15] American Bar Association, Resolution 108, February 2017. See, http://www.americanbar.org/content/dam/aba/images/disaster/Resolution%20108%20FINAL.pdf

Law Firms Prepare for Cyberattacks

As with any successful corporate strategy, effective information security programs begin with upper management making a visible commitment, including the provision of adequate resources, creating the necessary policies and procedures for the organization and hiring or training employees as appropriate. Leadership of the organization must be actively engaged to ensure information security is an important element of the firm's operations. This is demonstrated by designating an individual or establishing a steering committee dedicated to information security, including identifying a person or persons to conduct internal audits. Because the ISMS should address business activities and other disciplines of the firm, the steering committee should be represented by departments across the firm.

A recent symposium reported on the increased acceptance of ISO/IEC 27001 in the legal industry to meet the ever-increasing pressure for law firms to prove they have a formal, documented system for protecting confidential data.[16] "Information is the most valuable asset within a law firm and keeping this information secure is paramount to client and firm leadership."[17]

ISO/IEC 27001 provides a management systems approach to the ISMS by requiring the law firm to address each of the components of the management system within the Plan-Do-Check-Act cycle. Administrative, technical, organizational and physical controls help ensure the confidentiality, availability, and integrity of digital assets. Such controls should be carefully determined, implemented, and enforced. Figure 1, below, depicts the Leadership component of the cycle, Clause 5, and the actions that the law firm must take to demonstrate leadership and commitment. The initial areas of focus will be on leadership and the risks as shown in these graphics.

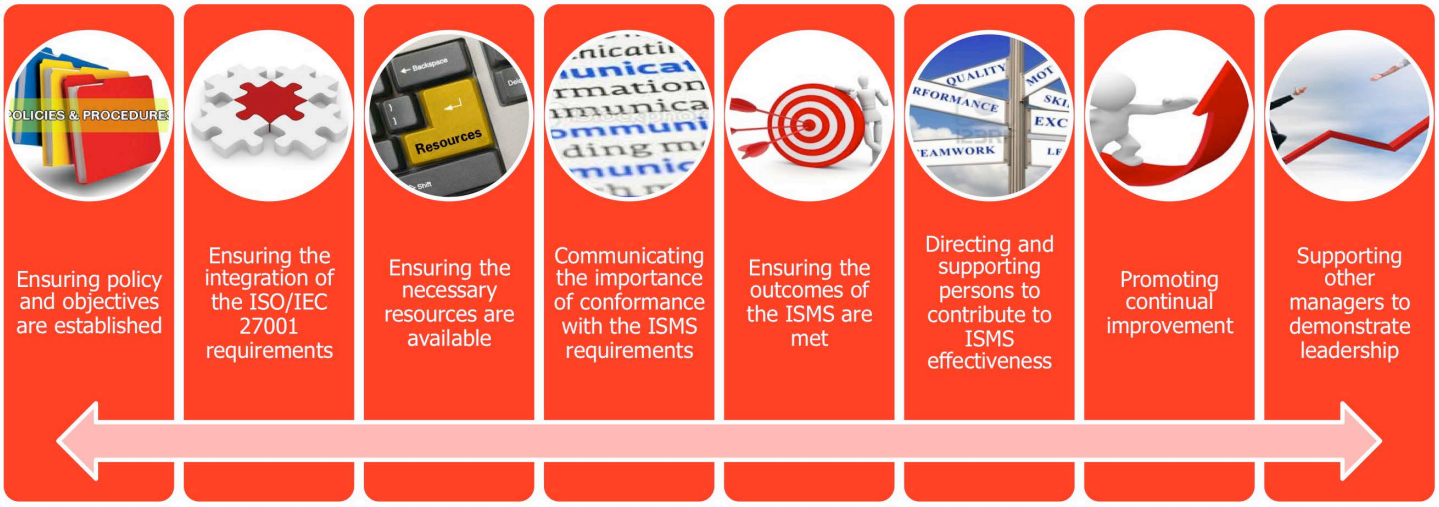

Figure 1. Clause 5.1, Leadership and commitment

[16] Leveraging Information Security Standards in Law Firms: The Increasing Popularity of ISO 27001 in the Legal Industry," Iron Mountain, 2016 Law Firm Information Governance Symposium. http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/L/Leveraging-information-security-standards-in-law-firms.aspx.

[17] Id.

Risk assessments inform decision-makers and support the risk management process by identifying: (i) relevant threats to the organization or threats directed through third party entities; (ii) vulnerabilities both internal and external to the organization; (iii) the impact (i.e., harm) to the organization and individuals that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a categorization of risk according to the degree of risk and magnitude of harm to the organization flowing from the threat or vulnerability if it occurred. [18]

ISO/IEC 27001, at Clause 6, requires the law firm to define and apply an information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for [in-scope] information. An effective ISMS must establish and maintain risk criteria that will be used to perform the risk assessments and identify specific risks and the risk owners, as well as potential consequences. A law firm will evaluate and prioritize risks as to the levels and likelihood of occurrence. Finally the ISMS requires the law firm to retain documented evidence showing that the risk assessments themselves will produce "consistent, valid and comparable results."

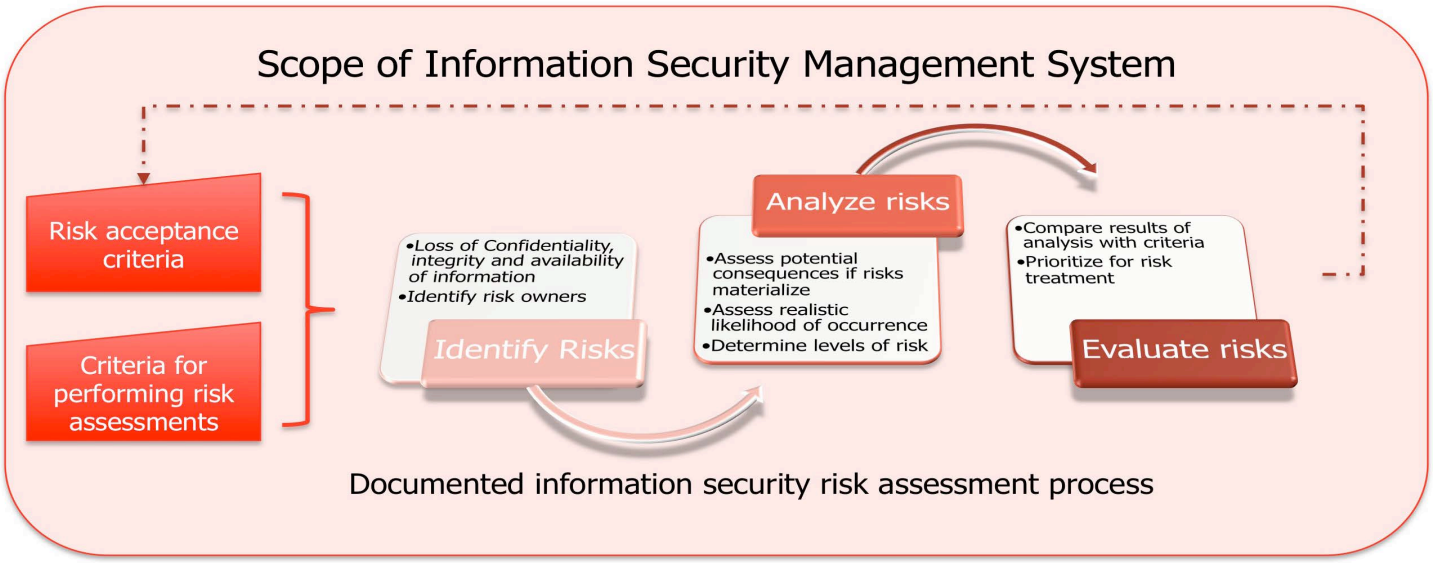

Figure 2. Clause 6.1.2, Risk Assessment in the ISMS

The outputs of the law firm's risk assessment process provide the inputs to the law firm's determination and selection of the right controls to implement the law firm's risk treatments and what they are meant to protect. Law firms will identify and close the gaps between current and desired state, monitor program, and improve the ISMS with a repeatable process. By preparing a Statement of Applicability during risk treatment, the law firm documents the necessary controls and justifies the exclusions. Thus the firm also uses the standard as a baseline to determine risks that are beyond the level of acceptability, and probability of occurrence. In the balance of this paper, we refer to the risk-based security controls of ISO/IEC 27001 that the law firm would chose to protect client information and limit the likelihood of cyberattacks.

[18] "American Bar Association, Revised Resolution 107, August 2014, p. 7.

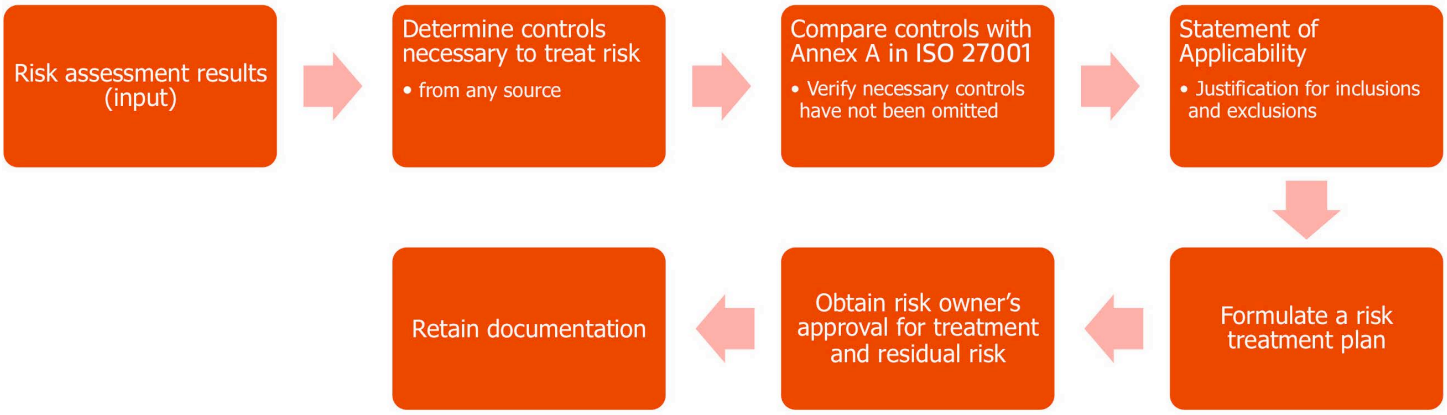

Figure 3. Clause 6.1.3, Information security risk treatment

"Law firms now recognize that cybercriminals are constantly looking for easy targets and sources of potentially valuable data that can be used to steal identities. Since law firms act as warehouses of extremely sensitive client and employee data, they are prime targets for cyberattacks."

National Law Review

The Nature of Cyber Attacks

Law firms collect and store large amounts of non-public information that is desirable for insider-trading schemes. In March 2016, the FBI's Cyber Division issued a warning that hackers are specifically targeting international law firms to seek confidential data.[19] A phishing attack is a fraudulent email, disguised as an authentic message that requests information or advises the recipient to take certain actions.

A highly publicized example of this intrusion reportedly occurred when Clinton campaign chairman, John Podesta, clicked on an email urging him to change his Gmail password.[20] A similar example of phishing occurs when a middle to lower level employee receives an email purportedly from their CEO or CFO requesting certain company confidential information or transfer of funds. Known as Whaling or Spear-phishing, this tactic is more difficult to detect as the email address initially appears to be legitimate, but upon closer scrutiny has been changed ever so slightly – an "m" is changed to an "rn" or "oo" is changed to "00".

With ISO/IEC 27001, the law firm puts controls place that can help lawyers protect their clients and the privileged information they hold. These include policies and processes regarding information transfer internally

[19] "FBI Alert Warns of Criminals Seeking Access to Law Firm Networks," Bloomberg Law, Big Law Business, March 11, 2016. https://bol.bna.com/fbi-alert-warns-of-criminals-seeking-access-to-law-firm-networks/

[20] http://www.cbsnews.com/news/the-phishing-email-that-hacked-the-account-of-john-podesta/

and externally, especially electronic messaging which can so easily be intercepted. These controls or safeguards provide the framework against which policies can be written to cover access levels, authentications and management, all of which will foster a controlled environment where only those with the "need to know" will be able to retrieve only that information that is appropriate. Controls guard against these types of attacks. For example, A.6.1.2. Segregation of duties, spreads the responsibilities within an organization, making it harder for phishing to succeed with one point of entry.

A.6.1.2 - Segregation of duties*

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

By segregating the responsibilities within an organization, the Whaling example above would have been more difficult to achieve.

Additional controls that are keys to promoting information security across the law firm include requiring a defined set of approved policies, which are published and communicated across the firm (including contractors) and robust training on information security awareness.

A.5.1.1 Policies for information security*

A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.

A.7.2.2 Information security awareness, education and training*

All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

Once a cyberattack is successful, access to information is often maintained through embedding malicious software or malware. Malware can take many forms – viruses, Trojan horses, worms – and each can impact an organization's network differently.

Viruses and worms can spread through the computer network. Viruses occur when an executable piece of code, usually embedded in a seemingly legitimate or innocuous image or link, is activated. Viruses have been known to wipe out a hard drive, corrupt applications or generally alter the manner in which a computer operates.

Computer viruses cannot infect computers without the computer-owner clicking on something to initiate its activation. The virus' evil twin, the worm, can independently self-replicate and take down a network by blocking/ encrypting files or create a backdoor to be used as access after the initial attack.

The third most prevalent type of malware is an application that appears to be a useful application, but actually contains malicious code. Known as a Trojan horse, this malware can delete or corrupt files, but is most prevalently used by cybercriminals to install a backdoor that can be used at a later date.

ISO/IEC 27001 provides controls to help prevent unauthorized and untested software from being downloaded or installed, either on an independent computer or on the network. These controls involve defining and allocating roles and responsibilities, segregating duties as mentioned above, preventing the introduction of malware, and restrictions on software installation or other downloads.

A.6.1.1 - Roles and responsibilities*

All information security responsibilities shall be defined and allocated.

A.12.2.1 – Controls against malware*

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

A.12.6.2 - Restrictions on software installation*

Rules governing the installation of software by users shall be established and implemented.

It is important to be prepared; it is not a case of "if" a cyberattack happens, but "when". According to the National Law Review, "Law firms now recognize that cybercriminals are constantly looking for easy targets and sources of potentially valuable data that can be used to steal identities. Since law firms act as warehouses of extremely sensitive client and employee data, they are prime targets for cyberattacks. In the new, highly connected reality we operate in, law firms must consider the risks these cyberthreats pose and take the data protection steps necessary to reduce those risks.

Otherwise, the oversight may prove costly." [21]

[21] Carlos Arcos, "Why You Need a Law Firm Data Breach Response Plan," National Law Review, August 8 2016. http://www.natlawreview.com/article/why-you-need-law- firm-data-breach-response-plan, Accessed January 29, 2017.

Mergers and Acquisitions at Risk

For the legal community, one of the more chilling results of a cyberattack occurred when three foreign nationals made millions of dollars from insider trading by using information they gleaned from hacking the computer networks of two major New York law firms.[22] This is a growing problem within the legal community. According to Department of Justice press release on December 27, 2016, the law firms' network and servers were penetrated, malware installed and the firms' Merger and Acquisitions' partners' emails exfiltrated.[23]

Manhattan U.S. Attorney Preet Bharara said: "As alleged, the defendants – including Iat Hong, who was arrested in Hong Kong on Christmas Day – targeted several major New York law firms, specifically looking for inside information about pending mergers and acquisitions. They allegedly hacked into two prominent law firms, stole the emails of their M&A partners, and made over $4 million in illegal profits.

"This case of cyber meets securities fraud should serve as a wake-up call for law firms around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals." [24]

Manhattan U.S. Attorney Preet Bharara

The international standard requires that the entire lifecycle of the information is considered in developing policies, and that when new technology or systems are put in place, these policies are updated to reflect changes. Means to detect fraud or unauthorized disclosures such as "incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay" must also be established. As examples:

---

[22] Joseph Facciponti, "SDNY Indicts Three Foreign Nationals for Insider Trading on Hacked Data," Mondaq, January 17, 2017 http://www.mondaq.com/unitedstates/x/562502/Securities/SDNY+Indicts+Three+Foreign+Nationals+for+Insider+Trading+on+Hacked+Data,

[23] U.S. Department of Justice, https://www.justice.gov/opa/pr/manhattan-us-attorney-announces-arrest-macau-resident-and-unsealing-charges-against-three, December 27, 2016. Accessed January 31, 2017.

[24] Ibid.

A.13.2 - Information transfer*

Objective: To maintain the security of information transferred within an organization and with any external entity.

A.13.2.1 - Policies and procedures*

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

A.13.2.2 - Agreements on information transfer*

Agreements shall address the secure transfer of business information between the organization and external parties.

A.13.2.3 - Electronic messaging*

Information involved in electronic messaging shall be appropriately protected.

Mossack Fonesca – Lessons Learned

Last year, records and documents from the fourth largest offshore law firm, Mossack Fonseca, were spread across the globe. With over 2.6 terabytes stolen from the internal database of the Panamanian firm, an estimated 11.5 million documents found their way to various news media, foreign governments and law enforcement agencies, exposing the secrets of clients ranging from "A-lister" celebrities and politicians, drug lords, and foreign despots. What *The Guardian* dubbed the "Biggest Leak in History", the so-called Panama Papers is an extreme case of the impact of a data breach. [25]

The International Consortium of Investigative Journalists' (ICIJ), the group originally provided with the leaked information, describes the range of the data, "The leaked data covers nearly 40 years, from 1977 through the end of 2015. It allows a never-before-seen view inside the offshore world — providing a day-to-day, decade-by-decade look at how dark money flows through the global financial system, breeding crime and stripping national treasuries of tax revenues. [26]"

In a July 2016 article, Deloitte outlines the impact of the breach to banks and financial institution, boiled down into two major areas, Regulatory Risk and Reputational Risk. "Banks, financial institutions and other intermediaries run the risk of becoming associated with the matter and may find themselves on the receiving end of allegations of having provided assistance to launder the proceeds of illicit activity, or of having taken part

[25] "Panama Papers: a special investigation" The Guardian, April 6, 2016 https://www.theguardian.com/news/2016/apr/08/mossack-fonseca-law-firm-hide-money- panama-papers, Accessed January 31, 2017.

[26] International Consortium of Investigative Journalists, https://panamapapers.icij.org/20160403-panama-papers-global-overview.html Accessed January 31, 2017.

in tax evasion, thus affecting their reputation." On the regulatory side, the report lists a number of authorities and watchdog groups that have launched inquiries and/or are pursuing tighter regulations.[27]

The ICIJ lists the continuing impact of these leaks:

- "At least 150 inquiries, audits or investigations into Panama Papers revelations have been announced in 79 countries around the world
- An estimated $135 billion was wiped off the value of nearly 400 companies after the Panama Papers
- Governments are investigating more than 6,500 taxpayers and companies, and have recouped at least $110 million so far in unpaid taxes or asset seizures
- Nine Mossack Fonseca offices have shuttered around the world, and the law firm has been fined close to half a million dollars" [28]

The exact nature of the breach has yet to be determined, but it is clear it was either hacked by an outside entity or was leaked by a disgruntled employee.

In either case, ISO/IEC 27001's requirement of a risk assessment process, control 6.1.2, could prevent a similar event. The information security management system requires a law firm to conduct a risk assessment to plan for any eventuality of client information becoming public. An effective Information Security program aligned with ISO/IEC 27001 must establish and maintain risk criteria that will be used to perform the risk assessment, identify specific risks, the risk owners, as well as the potential consequences. A law firm will evaluate and prioritize risks as to the level and likelihood of occurrence. Finally, the system requires documented evidence showing that the risk assessments themselves will produce "consistent, valid and comparable" results.

Understanding who has access to information, the methods used to transmit that information as well as how it is stored is paramount to protecting that information. When aligned to ISO/IEC 27001, the law firm will address access control, including user registration and de-registration, control of levels of access, changes to level of access, authentication, established review intervals, secure log-on and password management, and administrative rights.

[27] The impact of Panama Papers" Forensic Foresight, July 2016, Deloitte, https://www2.deloitte.com/tl/en/pages/risk/articles/impact-of-panama-papers.html, Accessed January 31, 2017.

[28] Journalists, https://panamapapers.icij.org/20161201-global-impact.html, Accessed January 31,2017.

Summary

Attacks on law firms are rampant as criminals now see the value of the information they can gather and how easy it is to access. The legal industry is being called "the latest gold mine for hackers".[29]

Almost half of attorneys say their firms have no data breach response plan in place, even though an American Bar Association survey has found that one in four law firms with at least 100 attorneys have experienced a breach due to a hacker, website attack, break-in, or lost or stolen computer or smartphone[30]. Forty-seven percent of respondents said their firms had no response plan in place to address a security breach.[31] Firms are reporting a significant increase in clients doing due diligence and questioning them about their information security posture.

"ISO/IEC 27001 provides a framework to better protect information from an increasing variety of threats including fraud, cyber-attacks, inappropriate access and data leakage."[32] Legal experts agree law firms should consider certification to the Information Security Management System framework as structured by ISO/IEC 27001. "Certification also strengthens security as it requires firms to focus on continuous improvement and periodic assessment of compliance against policies, procedures and good security practices.

Compliance with this standard provides law firms with a widely-recognized approach to information security that encompasses people, processes and technology." [33]

Information security must be an overarching concern and responsibility of any law firm. It affects each functional area, not just the IT department. Those in the organization responsible for documentation management, human resources, procurement, and general counsel as well as senior partners responsible for the firm's direction all must be included in a robust information security management system. The very existence of the firm or its clients depends on it.

About the Contributing Author:

George B. Huff Jr., Esquire, MBCI, ISO 22301 Lead Auditor, is the Director of Consulting of The Continuity Project, LLC. He is Special Advisor to the American Bar Association's Standing Committee on Disaster Response and Preparedness, and an ANSI-U.S. Delegate to the U.S. Technical Advisory Group to ISO Technical Committee 292, Security and Resilience.

[29] "Brief History of Law Firm Cyberattacks," Law 360, https://www.law360.com/articles/800579/a-brief-history-of-law-firm-cyberattacks, Accessed January 20, 2017.

[30] Ibid

[31] 1 in 4 Law Firms are Victims of a Data Breach," Law 360, https://www.law360.com/articles/705657/1-in-4-law-firms-are-victims-of-a-data-breach, Accessed January 20, 2017.

[32] "Iron Mountain, "Leveraging Information Security Standards In Law Firms: The Increasing Popularity Of ISO 27001 In The Legal Industry", page 20.

[33] Ibid.

Why BSI?

BSI has been at the forefront of ISO/IEC 27001 since the start. Originally based on BS 7799, developed by BSI in 1995, we've been involved in its development and the ISO technical committee ever since. That's why we're best placed to help you understand the standard.

At BSI, we create excellence by driving the success of our clients through standards. We help organizations to embed resilience, helping them to grow sustainably, adapt to change and prosper for the long term. We make excellence a habit.

For over a century our experts have been challenging mediocrity and complacency to help embed excellence into the way people and products work. With 80,000 clients in 182 countries, BSI is an organization whose standards inspire excellence across the globe.

Our products and services

We provide a unique combination of complementary products and services, managed through our three business streams: Knowledge, Assurance and Compliance.

Knowledge

The core of our business centers on the knowledge that we create and impart to our clients. In the standards arena, we continue to build our reputation as an expert body, bringing together experts from industry to shape standards at local, regional and international levels. In fact, BSI originally created eight of the world's top 10 management system standards.

Assurance

Independent assessment of the conformity of a process or product to a particular standard ensures that our clients perform to a high level of excellence. We train our clients in world-class implementation and auditing techniques to ensure they maximize the benefits of our standards.

Compliance

To experience real, long-term benefits, our clients need to ensure ongoing compliance to a regulation, market need or standard, so that it becomes an embedded habit. We provide consultancy services and differentiated management tools to facilitate this process.

bsi.

Call us today to learn more

Call: **1300 730 134**
Email: **info.aus@bsigroup.com** or visit:
bsigroup.com/en-au