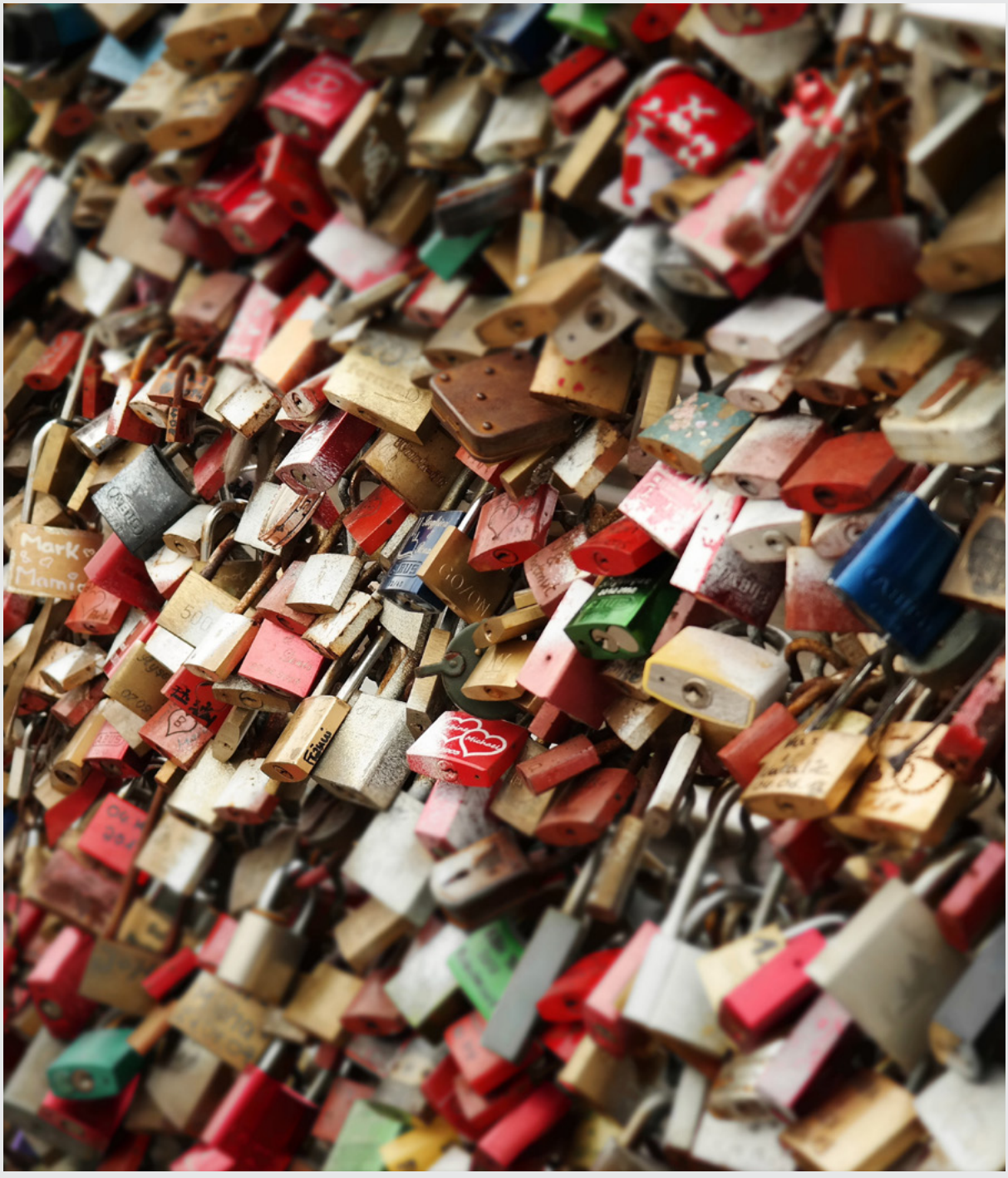
SIMPLE CYBERSECURITY AND REGULATORY COMPLIANCE STRATEGIES TO KEEP SMALL OR MID-SIZED LAW FIRMS IN THE BLACK WHILE AVOIDING A BLACK EYE

This white paper from Partners in Regulatory Compliance highlights how a law firm can materially mitigate its liability by conducting a comprehensive risk assessment, enlisting internal or external expertise, offering productive employee training, promoting cybersecurity awareness, investing in IT security, and focusing on reputation management.

PARTNERS
IN REGULATORY COMPLIANCE

INTRODUCTION

Law firms have historically been privy to the deepest, darkest secrets of the individuals and organizations they represent. Those records are now becoming a significant ethical, regulatory, and reputational liability for most lawyers given the increased focus on data governance, privacy protection, and brand management. Firms that proactively adapt will thrive. Those that remain complacent could suffer potential consequences ranging from short-term disruption or loss of business to long-term injury to their reputations or roles as trusted advisors.



I. LAW FIRM DATA BREACHES AND CYBER THREATS ARE ON THE RISE

In its highly-publicized October 2018 opinion, the American Bar Association emphasized that "Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession."[1] It warned that "As custodians of highly sensitive information, law firms are inviting targets for hackers."

In fact, the ABA's 2018 Legal Technology Survey Report supports this warning as 23% of the respondents advised that their law firms had experienced a security breach (including a lost or stolen computer or smartphone, hack, break-in, or adverse website issue), which reflects an 8% increase over a five-year period.[2]

Given the accepted inevitability that a cyberattack will occur, law firms must:

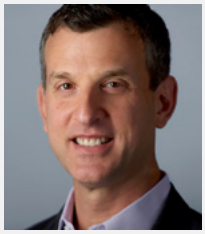
- Protect their perimeter.
- Evaluate the protocols of their vendors.
- Focus on a response and post-attack communications plan.[3]

[1] ABA Formal Opinion 483, Lawyers' Obligations After an Electronic Data Breach or Cyberattack, October 17, 2018, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf; see also, ABA Issues New Guidance on Lawyer Obligations After a Cyber Breach or Attack, November 2, 2018, https://www.americanbar.org/news/abanews/aba-news-archives/2018/10/aba-issues-new-guidance-on-lawyer-obligations-after-a-cyber-brea/.

[2] David G. Ries, 2018 Cybersecurity, American Bar Association 2018 Legal Technology Survey Report, January 28, 2019, https://www.americanbar.org/groups/law_practice/publications/techreport/ABATECHREPORT2018/2018Cybersecurity/

[3] Cyber Experts: Attacks Inevitable, Preparation for

Sidebar



Many law firms often assume they need not implement advanced security protocols, and instead, rely too heavily on the attorney-client privilege to protect their clients' information. These same law firms will mistakenly view a comprehensive data privacy and security effort as a costly insurance policy they believe they will never need. On the other hand, hackers and other malicious actors have come to realize that law firms may have better treasure troves of useful secret or proprietary information than any individual company they represent because these law firms may have information of numerous businesses. These bad actors also know that beyond the larger and more sophisticated law firms, most legal practices operate without thorough data privacy and security policies and procedures, and basic security awareness training. After all, clients rarely ask about their attorneys' policies, and few have the ability to conduct a simple audit or even know what to ask. Ultimately, law firms that have sophisticated and standardized data privacy and security protocols, as well as train their professionals and staff members accordingly, are much less likely to become a victim of a potentially costly and damaging data breach. Proceeding in such a manner with appropriate procedures and protocols not only provides a substantial level of protection against the bad actor, but also minimizes the most common source of data breaches – the malicious or careless insider.

Michael Feldman, Esq., Partner,
OlenderFeldman LLP
Certified Information Privacy Professional (CIPP)

OLENDER FELDMAN
ATTORNEYS AT LAW

A. Mid-Sized and Larger Firms Are at an Increased Risk for Security Threats

One of the most alarming conclusions in the ABA's 2018 Legal Technology Survey was that as firms grow and hire additional employees, their risk of experiencing a breach rises steeply. In fact, the data shows that many mid-sized firms face the greatest threat:

- 42% of firms with 50-99 lawyers reported a breach.
- 31% of firms with 100+ employees reported a breach.
- 14% of solo practices reported a breach.

In addition, the number of survey participants who were unaware of whether their firms were breached rose with the organization's size:

- 61% of respondents at firms with more than 500 attorneys had no knowledge of a breach.
- 57% of respondents at firms with 100-499 attorneys had no knowledge of a breach.

While it is unreasonable to expect every professional within a law firm to know whether the firm had been breached, it is imperative for firms to involve every single employee in its data protection practices. For example, anyone with access to the network should complete various levels of training that addresses phishing, mobile access, password protection, and proper information transfers, among other topics. Strong cybersecurity hygiene is critical since 40% of law firms that responded to the ABA's survey reported an infection from a virus, spyware, or malware with firms of 10-49 attorneys experiencing the greatest incidence of this contamination at 57%.

Each employee should also know how and when to report a potential problem, as well as the protocols for addressing client directives in email correspondence. After all, the consequences of a mistake could include material financial losses and undesirable media coverage. For respondents to the ABA's survey who experienced a breach:

- 41% reported some downtime or loss of billable hours.
- 40% were forced to pay consulting fees to make repairs.
- 27% had to replace hardware or software.
- 11% experienced file destruction or loss.

For firms of almost any size beyond a few lawyers, several hours of saved billable time could easily pay for the cost of a proactive cybersecurity assessment identifying areas in a firm's security posture in which to reduce risk.

Only 9% of the 23% of firms that experienced a breach actually notified their clients. This is a sobering statistic, but the number of firms who reached out to their clients rose to 17% for firms with 50-99 lawyers and 19% for firms with more than 500 lawyers. Interestingly, more breached firms gave notice to law enforcement (14%) than to their clients, with 25% of firms at 50-99 lawyers doing so (as compared to the 17% who advised their clients). Depending on the data that was lost, this could represent both a significant compliance concern, as all 50 states have mandatory breach notification laws requiring companies to advise individuals when their personal information is exposed,[4] and an ethical issue since an alert to law enforcement should likely include a corresponding report to clients who are impacted as well.

Law Firms Essential, American Bar Association, August 04, 2018, https://www.americanbar.org/news/abanews/aba-news-archives/2018/08/cyber_experts_attac/.

[4]Security Breach Notification Law, National Conference of State Legislatures, September 29, 2008, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

B. A Minor Law Firm Breach Could Have Major Consequences

Law firms are already on notice of their obligations because a few years ago, the FBI issued a warning to large law firms that hackers were targeting their confidential client information.[5] Still, it was not until a very public ransomware attack on one of the world's largest a year later, however, that the entire community reacted.[6]

The breach at DLA Piper, with lawyers in over 40 countries, forced the firm's leadership to shut down its entire U.S. IT infrastructure for days costing the firm 15,000 hours of overtime pay and countless other undisclosed expenses in addition to a significant loss of productivity.

Beyond the quantifiable repercussions is a pervasive loss of credibility that is difficult to regain. In an increasingly competitive environment where clients view law firms of a similar caliber as fungible, a preventable security lapse can inflict long-term damage.

---

[5]Linn Foster Freedman, FBI Issues Warning to Law Firms, Data Privacy + Security Insider, March 24, 2016, https://www.dataprivacyandsecurityinsider.com/2016/03/fbi-issues-warning-to-law-firms/.

[6]Jeff John Roberts, Law Firm DLA Piper Reels Under Cyber Attack, Fate of Files Unclear, Fortune, June 29, 2017, http://fortune.com/2017/06/29/dla-piper-cyber-attack/.

II. THE ETHICS OF PROACTIVELY PROMOTING SECURITY

The practical importance of properly valuing data security is as much of an ethical concern for individual lawyers as it is a business priority for their firms. ABA Model Rule 1.6(c) governing the confidentiality of information specifically states: "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."[7]

And, in an August 2014 opinion, the New York State Bar Association Committee on Professional Ethics urged the legal community to proactively address cybersecurity, warning:

> *Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks.*[8]

While advanced security may have exceeded the scope of a lawyer's professional responsibility a generation ago, the standard of reasonableness has evolved with the popularity of technology and its familiarity within the legal profession. As such, lawyers are now required to consider the likelihood of disclosure of client information and the cost of employing safeguards to prevent it, among other factors.[9] Since they have received ample warning from many different sources about the potential for a data breach and the costs associated with common security measures are now relatively low, their liability outweighs any perceived value in ignoring these obligations.

A. Lawyers are Practically and Professionally Required to Consider Security

Lawyers have been formally aware of the importance of understanding the perils and promise of technology since the ABA approved a change to the Model Rules of Professional Conduct over six years ago. It updated the traditional duty to be competent in the practice of law with an understanding of the benefits and risks associated with technology.[10] Although 14 states have still not formally adopted this obligation, it is well-recognized nationwide.[11] In fact, two states – Florida and North Carolina – also require

---

[7]ABA Model Rule 1.6: Confidentiality of Information, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/.

[8]New York State Bar Association Committee on Professional Ethics Opinion 1019, Confidentiality; Remote Access to Firm's Electronic Files, August 6, 2014, http://www.nysba.org/CustomTemplates/Content.aspx?id=51308.

[9]See, Comment 18 to ABA Model Rule 1.6: "The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)." https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6/

[10]Comment 8 to Model Rule 1.1 states: "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." https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1/

[11]Robert Ambrogi, Lawsites.com, https://www.lawsitesblog.com/tech-competence/.

technology-focused continuing legal education.[12] Mid-sized firms in particular must focus on this trend because smaller IT services support teams may not be as familiar with the full array of unique obligations they face. To fuel this effort, they must assign knowledgeable employees with adequate accountability to monitor the firm's data and privacy issues, with support from external resources for incident response, cybersecurity policy development, and procedure creation, such as the increasingly popular CISO-as-a-Service model. This is especially important because the rules do not mandate that security be a dedicated internal function only that it is reasonably addressed.

B. Hackers Are Specifically Targeting Law Firms and Their Client Data

Applying a combination of internal and external expertise is particularly important given that the ABA's May 2017 opinion focused on securing the communication of client information and emphasized that law firms are targets because they have highly sensitive material with weaker safeguards to protect it. The valuable records are, therefore, more identifiable because clients generally send their law firms only the critical data that relates to a pending matter and simpler to steal because they have traditionally had fewer protections than their original source.[13]

To fight this dangerous combination, all law firms should conduct a vulnerability assessment to establish a baseline of their threat landscape. It will expose any actual weaknesses that an experienced attacker could leverage to penetrate the system.

A CISO-as-a-Service resource may also be able to enhance your risk and cybersecurity assessment efforts, especially since it allows firms to split their investment between leadership and IT infrastructure. It independently monitors any attacks or breaches that impact your network, as well as your overall approach to information governance.

---

[12]Doug Austin, A Second State Now Has Approved a Technology CLE Requirement for its Lawyers, eDiscovery Daily Blog, December 7, 2018, https://ediscovery.co/ediscoverydaily/electronic-discovery/a-second-state-now-has-approved-a-technology-cle-requirement-for-its-lawyers-ediscovery-trends/.

[13]ABA Formal Opinion 477, Securing Communication of Protected Client Information, May 11, 2017, https://www.americanbar.org/content/dam/aba/administrative/law_national_security/ABA%20Formal%20Opinion%20477.authcheckdam.pdf; see also, Kathryn T. Allen, Law Firm Data Breaches: Big Law, Big Data, Big Problem, Nat'l L. Rev., Jan. 11, 2017, https://www.natlawreview.com/article/law-firm-data-breaches-big-law-big-data-big-problem.

III. STATE AND FEDERAL RULES DICTATE THAT LAW FIRMS MUST MANAGE DATA LIKE THEIR CLIENTS

Regardless of the industry, law firms must treat data from their clients with the same level of protection as if they were the original owner. For example, law firms representing "Covered Entities" under the New York Department of Financial Services Cybersecurity Regulation (23 NYCRR 500), which places cybersecurity requirements on all businesses licensed under the insurance, banking, and financial services laws in New York State, must meet their clients' obligations even though they are not themselves financial institutions. Similarly, firms working with data from healthcare clients are typically considered "Business Associates" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and must ensure compliance with that law.

A. Failure to Reasonably Protect Data and Prevent Cyber Attacks Could Result in Malpractice

In addition to potential penalties for regulatory non-compliance, law firms that provide insufficient data protection could face malpractice claims associated with failing to protect client confidentiality. Even a lack of proper employee supervision could be characterized as negligent and rise to the level of fraud and misrepresentation if caused by a malicious insider.[14] For instance, a 2016 class action suit was filed against a Chicago law firm for inadequate security and a hacked New York attorney was sued for erroneously wiring almost $2 million.[15]

Ultimately, if a firm's data ends up on the "dark web" and a client's information was sold or released as a result, the liability could be substantial. In addition, the reputation of the law firm would be negatively impacted and potentially suffer permanent damage.[16] Even firms that have cybersecurity insurance cannot afford to lose the lifetime value of an institutional client or the potential to gain another due to a loss of standing in the legal community.

B. Robust Policy and Reporting Framework Can Enhance Cybersecurity

While simple to draft, agreements governing data protection, IT security, insider threats, privacy, and related concerns are challenging to implement because they require universal commitment. Once firms achieve that objective, they will materially reduce their risk, as well as safeguard their professionals from embarrassing, yet preventable mistakes.

For example, despite obvious red flags, a lack of effective protocols allowed a large law firm associate in Vancouver to be fooled into wiring $2.5 million in client funds to a fraudulent

---

[14]Rudolf v. Shayne, Dachs, Stanisci, Corker & Sauer, 867 N.E.2d 385, 387 (N.Y. 2007).

[15]Shore v. Johnson & Bell, Case No. 16-cv-4363 (N.D. Ill. 2016); Millard v. Doran, Index No. 153262/2016 (Sup. Ct. N.Y. Cty. 2016).

[16]See, e.g., Ethan S. Burger, "Cyber Attacks and Legal Malpractice," U.S. Cybersecurity Mag., July 15, 2016, https://www.slideshare.net/EthanSBurger/2016-us-cybersecurity-magazine-july-cyber-attacks-and-legal-malpractice.

account through a combination of familiar, though creatively deceptive, tactics that should have been more obvious in 2019.[17]

Even if an employee succumbs to a criminal's clever ruse, there should be a reporting structure in place that requires several levels of approval before an action can cause any damage. It is also imperative for proactive organizations to eliminate unnecessarily dangerous practices, such as exchanging unencrypted hard drives through the mail or a courier. They must provide a mechanism for employees to report lost data, both for follow-up and any regulatory concerns, e.g., requirements associated with loss of healthcare data, and to alert security teams about suspected phishing scams or associated, inadvertent security errors. Organizations with proper policies and adequate reporting structures are often able to address security concerns more quickly and effectively.

[17]Scott Flaherty, Dentons Lawyer Wired $2.5 Million to Scam Bank Account in Elaborate Con, American Lawyer, January 22, 2019, https://www.law.com/americanlawyer/2019/01/22/dentons-lawyer-wired-2-5-million-to-scam-bank-account-in-elaborate-con/.

IV. EMPLOYING CERTAIN BEST PRACTICES COULD BOOST CLIENT CONFIDENCE

Law firms are not required to have flawless security practices. Rather, they need industry standard protocols maintained by a minimal level of expertise and infrastructure while supplemented with outside support. That formula will often meet client expectations and generally prevent obvious breaches. Additional best practices will strengthen the firm's approach and reinforce its security arrangement.

A. Re-Evaluate Your Outsourced IT Infrastructure and Management

While basic support teams focus on straightforward perimeter protection technology, generic anti-virus software, updated security tools, prompt patching and operating system upgrades, and routine backups, they are often not acutely aware of the responsibilities and laws to which your firm is subject. Law firms, therefore, should collaborate with organizations that understand the nuances of working with personal health information or restricted financial details and the heightened regulatory requirements associated with each. Declining to do so at the outset could cause problems if (and when) a breach ultimately occurs and prompts an array of disclosures, with which a generic vendor may be unfamiliar.

B. Hire Specialized Employees and Support Teams

Those who have specific responsibility for storing and protecting data, and ensuring that all mobile and personal devices that access your network are fully protected or prohibited from accessing your system, will create the safest environment and highest level of protection for the firm's client data. Information security and information technology are very different disciplines. They are often treated the same and may share budgets or personnel, but it is essential for law firms to apply an appropriate level of expertise to each specific problem.

C. Establish an Educational Awareness Program

Providing guidance to employees through regular training programs, newsletters, phishing campaigns, and cybersecurity awareness initiatives can materially lower a firm's risk profile. Beyond basic presentations, educate your staff about the value of adhering to physical security standards and all related policies, the need for using a virtual private network in public, e.g., coffee shops and airports, and the importance of taking specific steps to protect firm hardware and data when traveling overseas, particularly to China or Russia. Given that most security breaches are the result of employee mistakes, focusing on education is an absolute imperative.

Conclusion

Until recently, hackers viewed law firms as the unprotected back door to a treasure trove of highly-valuable corporate data. The heightened regulatory environment, an increase in embarrassing breaches, and elevated expectations from clients has created a material shift in security awareness. Despite this renewed focus on data protection, many firms still need to supplement their capabilities with outside support. Those that do so are finding that their regulatory compliance, client service, and business continuity are all much stronger.

Partners in Regulatory Compliance provides an array of cybersecurity services including policy management, risk assessments, employee training, and regulatory compliance assistance to law firms in New York, New Jersey, and Connecticut. It is a cybersecurity consultancy that provides innovative answers to the growing, complex need for cybersecurity in law firms representing clients facing strict regulatory compliance controls. By addressing the full range of digital and human threats to create a compliant, secure environment, Partners in Regulatory Compliance helps attorneys meet their professional, ethical, and legal commitments to protect the sensitive data they work with and store on behalf of their clients.

Learn more at piregcompliance.com and please feel free to contact us at **(646) 863-9050** or **info@piregcompliance.com.**