knowcyber™

Client-Centered Cybersecurity (C^3) for Law Firms

Cybersecurity: a law-firm imperative

For any law firm, the risk of being the target of cyber attack runs high, and the stakes are high as well. Nearly every aspect of a law firm's work involves the exchange, sharing, and storage of information in electronic form, via a rapidly proliferating array of devices, platforms, applications, and services. The firm handles, holds, and generates vast volumes and varieties of confidential information—from valuable client IP to strategic case- or litigation-specific communications and work products to personally identifiable information (PII). Failure to uphold ethical and professional obligations to protect such confidential information can have serious repercussions, including the loss of attorney-client privilege. Further, the financial, reputational, legal, and other business consequences of compromise can be severe—not only for the firm but also for its clients, individual attorneys, and third-party vendors.

Addressing cybersecurity-related risks

In recent years, most law firms have become more cognizant of the cybersecurity-related risks they face. But few have addressed them adequately. Implementing technologies to detect and thwart attacks is essential but not enough. Tasking an individual or department with cybersecurity responsibility is helpful but not enough. Appropriate, effective steps for safeguarding confidential information must be baked into each facet of the entire client-relationship life cycle. Everyone who handles or has access to confidential information—partners, associates, support staff, and vendors—must not only be knowledgeable of why and how it may be compromised, but also prepared and motivated to act on that knowledge consistently.

Our unique, flexible C^3 approach

KnowCyber's unique approach to cybersecurity education and practice equips law firms of all types and sizes to meet the steep cybersecurity challenges they face. Created by learning professionals in tandem with experienced attorneys, legal professionals, and cybersecurity experts, our Client-Centered Cybersecurity (C^3) offerings address the legal profession's cybersecurity needs comprehensively and conveniently.

- **Our C^3 curriculum segments** address, from an operational perspective, all critical facets of protecting confidential information through every phase of the client relationship life cycle.

- **Modularization and customization options** give each firm the flexibility to tailor the curriculum to address the issues and challenges unique to its industry, specialization, size, and current level of cybersecurity preparedness.

- **Role-based and third-party versions** of the curriculum segments ensure across-the-board consistency of content and terminology while focusing on the specific knowledge and competencies each type of cybersecurity contributor, in-house and vendor, must master.

- **Multiple delivery options**—including live classroom and virtual instructional sessions, facilitated discussions, webinars, and self-study e-learning modules—offer additional flexibility.

A full range of business benefits

KnowCyber's C^3 approach enables any law firm not only to minimize its exposure to cybersecurity risk effectively but also to demonstrate its cybersecurity competence, and that of its third-party vendors, convincingly. It provides a common framework, process, and vocabulary that enables firm and client to work together to assure the protection of confidential information throughout an engagement. The active, structured collaboration that ensues builds mutual trust and respect, thereby strengthening each client relationship and creating multiple opportunities to deepen and expand it.

~Continued on reverse side

C³ CURRICULUM SEGMENTS

knowcyber™
Cybersecurity through learning.

Client Relationship Framework

Collaboration on cybersecurity and information management must begin with the firm's initial exchange of information with the client and extend throughout the relationship. This segment explains the sources and implications of the firm's obligations to protect confidential information. It surveys the essential steps needed to ensure that the parties agree on the level of cybersecurity expected and how it will be achieved, reflect their agreement in sound contractual terms, and embed cybersecurity processes in every phase of the work.

Securing Communications

Lawyers sell their know-how, imparting knowledge and advice both orally and in writing—almost exclusively through communications that are transmitted and stored electronically. This segment stresses the criticality of securing communications in order to protect confidentiality, safeguard information assets, and preserve attorney-client privilege. It provides sound, practical, specific advice on how to secure communications via the vast range of communication devices, channels, and systems in use today.

Cyber Insurance

While the cyber insurance market has exploded in recent years, a lack of actuarial data means that the sophistication of the market remains low; misconceptions about how much to rely on insurance abound. This segment clarifies the role of cyber insurance and explains what policies actually cover vs. exclude. It provides a structure for decision making, and pointers on how to obtain coverage at the best price.

Managing Third-Party Vendor Risk

As law firms outsource more of their work to third parties with whom they interact electronically, and those third parties do the same, cyber risk mounts exponentially. This segment focuses on how to reap the tremendous benefits of outsourcing while understanding the associated ethical challenges and addressing the risks. It recommends sound processes for anticipating and containing risk throughout the vendor life cycle.

Full-Lifecycle Data Protection

Clients have come to expect that a law firm has in place sophisticated information governance processes to ensure that data is safe. This segment prepares a firm to demonstrate effectively that it has the necessary people and processes, standards and policies, tools and technologies to protect client data through every phase and aspect of the delivery of legal services.

Anatomy of a Breach

Given the ubiquitousness of the cyber threat environment and the sophistication of cyber attackers—and the potentially staggering ramifications of a serious compromise of protected data—every law firm must collaborate with its clients and third-party vendors to prepare for a possible occurrence. This segment delves into best practices for each step that must be taken, from detection/discovery, through triage and containment, through response and remediation—including how to handle required notifications and disclosures.

571.210.4710
info@knowcyber.com
www.knowcyber.com

Incident Response

Law firms, their clients, and third-party vendors must anticipate and agree upon how they will cooperate in the event of a data security incident that does not rise to the level of a breach but must be communicated and resolved. In addition to covering top means of incident prevention, this segment prepares the parties to develop and implement a sound incident response plan with appropriate communication protocols.

Best Practices in Client-Centered Cybersecurity

This segment integrates the guidance provided throughout the other C³ modules to provide a practical compendium of essentials for implementing effective cybersecurity in a client-centric manner. It prepares people — the firm's, and its clients' and third-party vendors'—to recognize how confidential information can be compromised, as it motivates and equips them to play an active, effective role in prevention and mitigation. ■