HBR
CONSULTING

Five Reasons to Build Your Law Firm's IT Security Framework on NIST Standards

hbrconsulting.com | info@hbrconsulting.com | 312.201.8400

advisory | managed services | software solutions | insights

Introduction

Law firms are daily targets for cybercrime and targeted data breaches. Criminals are keenly aware that law firms can be a “back door” to valuable confidential data, such as trade secrets, intellectual property and financial information related to potential business deals. In fact, 23 percent of law firms reported that they have been the victim of a data breach at some point, according to the ABA’s *2018 Legal Technology Survey Report*.[1]

Meanwhile, corporate clients are ramping up due diligence efforts to ensure their outside law firms are protecting their information with comprehensive information security controls. They also want to be assured their firms can quickly and easily respond to all possible compliance items or requests. Roughly one-half of law firms were subjected to a cybersecurity audit last year, according to a presentation from the Association of Legal Administrators.[2]

This two-pronged challenge — the need to protect the firm’s IT systems from cybercriminals and the need to respond to client demands for information security — is a daily battle for any law firm CIO or CISO.

There are a number of compliance standards and data security certifications available to help law firm CIOs develop their IT security posture. These standards, such as ISO 27001 or COBIT, provide important frameworks for guiding your firm’s IT workflow and instilling confidence in your IT systems — but they are not as robust or granular regarding overall sound information security. And since each law firm has its own culture, size, personnel, scope of work and organizational complexity, most firms typically want to modify their IT processes to meet their unique needs, rather than forcing themselves into “one size fits all” workflows.

This whitepaper discusses several reasons why law firms should consider building their IT security program on the framework laid out in the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[3]

> **This two-pronged challenge — the need to protect the firm’s IT systems from cybercriminals and the need to respond to client demands for information security — is a daily battle for any law firm CIO or CISO.**

What Is NIST's Cybersecurity Framework?

NIST is a division of the U.S. Commerce Department that promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. NIST is a non-regulatory agency of the U.S. Department of Commerce.

One of NIST's key strategic initiatives has been the development of a framework of "standards, guidelines and best practices" to help organizations manage cybersecurity-related risk. The most recent version of this framework — the "Framework for Improving Critical Infrastructure Cybersecurity" — was released in April 2018.[4]

The NIST Cybersecurity Framework provides an approach for managing data security today, as well as a roadmap for improving data security in the future with ongoing development, alignment and collaboration between industry and government. The structure laid out in the NIST framework establishes five core functions for organizations to implement in their IT systems and processes:

- Identify known cybersecurity risks to your infrastructure
- Protect the delivery and maintenance of infrastructure services
- Detect the occurrence of a potential cybersecurity event
- Respond to a detected data security incident with specific methods
- Recover and restore your organization's capabilities that were impaired

The NIST framework provides law firms with a valuable paradigm for building their IT systems and developing their unique approach to information security.

"While there is no one legal standard to apply (to cybersecurity defense systems) in the U.S. yet, the NIST Cybersecurity Framework comes close," writes F. Paul Greene, an information security lawyer.[5] "The framework was the result of a long and interactive collaboration with the private sector, giving it the cache of significant private-sector input. Partially because of this, the NIST framework has steadily gained traction in the private sector, becoming a de facto national cybersecurity standard in some areas."

The NIST framework provides law firms with a valuable paradigm for building their IT systems and developing their unique approach to information security. It is a process more akin to an ongoing feedback loop than to a set of systems controls or technical standards. For this reason, the NIST framework can save time and money by sparing law firms from the onerous mission of attempting to chase down the technical requirements for every new third-party certification that emerges, while avoiding the complexity of trying to customize their IT systems to every client's security solutions.

Why Should Law Firms Use the NIST Framework?

Here are five reasons to consider building your law firm's IT program on the NIST framework:

1. **The NIST Framework Is Comprehensive**

   The NIST framework is a representation of a complete information security program. It includes sections ("families") ranging from physical security to business continuity to access controls. A mature information security program accounts for all aspects of security commensurate with the environment it is instituted in and data it is subject to protect. Since a program is only as good as its weakest link, the NIST framework ensures all potential areas for information security concern are at least considered when developing the program, diving deep to cover all possible information risks and process issues. After all, would it make any sense to lock all of the doors to your house, put up a fence around your property . . . and then leave your garage door open? The NIST framework is comprehensive and granular enough to make sure your data security program has locked up all of the entry points.

2. **The NIST Framework Is Used by the U.S. Federal Government and Major Financial Institutions**

   U.S. federal agencies have adopted the NIST framework for purposes of securing their systems and their third-party contractors' systems as well. Federal agencies are diligent in their efforts to protect information maintained on third party-contracted systems.

   Leading financial institutions, such as Goldman Sachs[6] and Bank of America,[7] among others, have adopted the NIST framework to ensure all information security controls are addressed in their heavily regulated businesses. Additionally, they strongly suggest their third-party relationships adopt the framework to help assist in protecting their confidential information.

   These are similar to the law firm-client relationship, where law firms maintain client data on their systems. Clients will find assurance that a robust security framework is being leveraged to secure systems and assist with structured compliance requirements. Law firms would be wise to consider these crucial endorsements.

3. **The NIST Framework Serves as a Gap Analysis**

   The NIST framework functions as a valuable guide to help law firms identify potential weaknesses in their systems and help determine the future state they seek to create. This gap analysis guides IT/IS planning by serving as a tool for directing where the firm's security framework should evolve in response to changing conditions, threats and needs. In this sense, it functions as a quasi risk assessment, helping law firms go through the process of documenting which controls they have in place and which ones are not as mature, so they can identify areas within their security program that need additional attention. Firms can easily parse the results to help triage efforts and determine where budget is best allocated to mitigate the most risk.

4. **The NIST Framework Provides a Security Playbook**

   The "System Security Plan" created via the NIST framework can be used to generate constant feedback that helps law firms operationalize their IT security program for day-to-day implementation. This security playbook creates a continuous cycle for security: design, implement, review; update and then resume the cycle again. Risk mitigation activities are constantly evolving and therefore your processes and documentation should evolve as well. Firms should evaluate their control set, triage activities and align budget, implement controls, update documentation and review for gaps at least annually.

5. **The NIST Framework Simplifies Audit Responses**

   The NIST framework provides a structure to use in organizing important descriptions, data maps and information security processes that are commonly requested in security and compliance questionnaires sent by clients. The System Security Plans, for example, will hold a vast amount of data that can easily be lifted, copied and pasted into answers responding to most audit queries. Maintaining documented structure for your security program assists in providing structured and consistent responses regarding client compliance. This reporting format can provide comfort and assurance around security concerns relating to your most important asset, your client data.

> **The NIST framework functions as a valuable guide to help law firms identify potential weaknesses in their systems and help determine the future state they seek to create.**

Conclusion

HBR Consulting partners with our law firm clients to build and maintain a secure structure for their data and systems. We understand that effective information security takes into account all facets of a law firm's physical and logical technical presence. We are committed to a holistic approach to structuring systems and consulting on a firm's information security program.

The NIST Cybersecurity Framework provides a comprehensive information security method that covers all of the technical bases for clients, meets the expectations of federal government agencies and delivers law firms an operational playbook for the protection of their IT systems and client data. This framework is a management tool for firms to ensure that every area of IT information security is reviewed, documented and assigned responsibility.

By relying on the NIST Cybersecurity Framework as your law firm's information security framework, you can go a long way toward resolving the two-pronged challenge of protecting your firm's IT systems from cybercriminals and responding to your clients' information security compliance requests.

Connect With Our Expert

For more information about law firm use of the NIST framework or how HBR Consulting can help with your firm's other IT needs, please contact:

Ken Kulawiak
Vice President, Information Security & Technology

O 312.964.4243
E KKulawiak@hbrconsulting.com

Sources

[1] Riles, David G., “2018 Cybersecurity,” American Bar Association, January 28, 2019. https://www.americanbar.org/groups/law_practice/publications/techreport/ABATECHREPORT2018/2018Cybersecurity/

[2] Harrison, James. “Responding to Client Cybersecurity Questionnaires,” ALA Annual Conference & Expo, May 5, 2018. http://my.alanet.org/events/annual/handouts/ac18/OM30_Responding_to_Client_Cybersecurity_Questionnaires.pdf

[3] “NIST Cybersecurity Framework” website (last visited July 8, 2019). https://www.nist.gov/cyberframework

[4] “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.1, National Institute of Standards and Technology, April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[5] Greene, F. Paul. “De-mystifying NIST - A Practical Introduction to the NIST Cybersecurity Framework,” Harter Secrest & Emery LLP, March 8, 2016. https://www.hselaw.com/blog/privacy-and-data-security/entry/de-mystifying-nist-a-practical-introduction-to-the-nist-cybersecurity-framework

[6] “Client Security Statement,” Version 7.0, Goldman Sachs, April 2019. https://www.goldmansachs.com/disclosures/client-security-statement.pdf

[7] “Our Business Practices Governance,” Bank of America website (last visited July 8, 2019). https://about.bankofamerica.com/en-us/what-guides-us/governance.html#fbid=9VoFHx41qJS

HBR
CONSULTING

HBR Consulting (HBR) delivers advisory, managed services and software solutions that increase productivity and profitability, while mitigating risk for law firms, law departments and corporations. As trusted advisors with deep industry experience, clients partner with HBR to achieve significant, sustainable results.

hbrconsulting.com | info@hbrconsulting.com | 312.201.8400

advisory | managed services | software solutions | insights