Keys to Establishing a Cybersecurity Program

ABA Cybersecurity Legal Task Force

1/18/2023

Maureen Kelly, Co-Chair, ABA Cybersecurity Legal Task Force

Claudia Rast, Co-Chair, ABA Cybersecurity Legal Task Force

Alex Thierer, Staff Attorney, ABA Cybersecurity Legal Task Force

Bar associations and state bars are not immune from cyber threats as evidenced by the State Bar of Georgia cybersecurity incident in April 2022, in which malicious actors gained unauthorized access to its computing infrastructure. Protect your bar by reading this series of three articles by the ABA Cybersecurity Legal Task Force which will outline key components of cybersecurity principles and best practices. This first article will focus on establishing an effective governance program. The second article will discuss preparing a response to a cyber incident. The third and final article will detail how to assess third-party and other vendors for cybersecurity risks.

Large-scale cyber incidents are often front-page news but are only the tip of the iceberg when it comes to the number of incidents organizations face each day. All types of organizations, including educational institutions, government entities, large and small businesses, and healthcare organizations have been victims of cyber incidents. According to CheckPoint, the Insurance and Legal industry faced an average of 976 cyber incidents per week in the third quarter of 2022. This represents an increase of 35% according to year-over-year data. Both large firms like Cleary Gottlieb, and small firms as well as Federal courts and other federal entities suffered cybersecurity incidents. Notably, state bars not immune from cyber threats as evidenced by the State Bar of Georgia cybersecurity incident in April 2022, in which malicious actors gained unauthorized access to its computing infrastructure.

Given the cyber risks faced by all entities, including bar associations, this is the first of a series of three articles discussing three key components of cybersecurity principles and best practices. This first article will focus on the need to have and maintain an appropriate, risk-based cyber governance structure. The second article will focus on the need to be prepared in advance for responding to a cyber incident. The third and final article will focus on how to effectively address potential cyber risks associated with your organization's vendors or other third parties.

Keys to Establishing and Maintaining an Effective Cybersecurity Program

An effective cybersecurity governance program relies on the establishment and maintenance of a risk-based set of cyber policies, practices, and controls tailored to the needs and vulnerabilities of your organization. To develop such a program, your organization must (i) identify the sensitive data and information collected or controlled by the organization and how and where it is processed; (ii) learn about any industry specific cyber risks attendant to your industry or handling of this type of data; and (iii) understand any legal, ethical or contractual requirements that govern your entity's obligations to protect the sensitive data entrusted to your organization and the computing systems that house such data. Once you understand your organization's cyber risks, you can then start to develop a program designed to implement the needed technical controls, practices and policies and procedures, including establishing an implementing an organizational culture that prioritizes training.

1. Identifying sensitive data and information collected or controlled by the organization.

The first step that must be taken to establish and maintain an effective cyber governance program is to identify the types of sensitive data that the organization processes. For example, many organizations maintain sensitive personal information, such as social security numbers of employees, medical information, or credit card and other financial information about customers or members, that could lead to identity theft or financial losses. Other types of sensitive information that may need to be protected include your entities or third parties' proprietary information. An entity also is likely to generate other internal data not intended for public release.

State bars and bar associations likewise collect, use, and maintain sensitive data and information about their employees, applicants, members, and others. These records may include employee and member information such as social security numbers, addresses, and other personally identifiable information (PII). These organizations may also maintain disciplinary records, PII, or financial information of their members.

2. Applicable security requirements

The duty to provide reasonable data security is imposed on entities through a variety of different means, including statutory and regulatory law, contractual commitments, representations made by parties whose data is processed, and for lawyers, ethical obligations. While we have no federal law imposing a uniform standard, many states' data breach laws impose a requirement to implement reasonable security requirements when processing certain categories of sensitive personal information of its residents. Importantly, courts have found that a common law duty to safeguard sensitive data may exist when an entity collects sensitive data, irrespective of the applicability of any specific law or regulation.

Some industries are subject to particular cyber legal requirements such as the health care and financial industries. For example, medical providers must be knowledgeable of the requirements of the federal Health Insurance Portability and Accountability Act (HIPPA) and numerous state requirements for protecting health-related data. Similarly, financial entities and publicly traded companies should be knowledgeable of the relevant Securities and Exchange Commission (SEC) guidance and New York state requirements. In addition, many contracts may include affirmative obligations to provide reasonable safeguards and an entity's public representations (e-privacy notices) as to its cybersecurity protections are likewise a source of potential enforceable commitments.

Of particular interest, lawyers are increasingly subject to ethical obligations and standards of conduct with regards to data security. Because lawyers collect, use, and safeguard sensitive client information. The American Bar Association's Formal Opinion 477R, which establishes at least a base duty of technological competence and awareness of the sensitive nature of their clients information. The Formal Opinion builds upon the ABA Model Rules of Professional Conduct Rule1.1 and 1.6 which require that lawyers provide competent representation to clients and that lawyers keep client information confidential respectively.

State bars and associations must endeavor to identify and understand its data security obligations, both with respect to the level of protection that must be provided and when it must disclose a breach. In processing sensitive membership data, a state bar will likely be subject to the privacy laws of the states in which its members reside (and the laws of other countries if the members live outside of the United

States). Other laws or regulations such as federal or state unfair business practice laws may also apply. The conduct of background checks conducted as part of the bar admittance process could possibly also trigger obligations. As part of this process, Bar associations should also identify potential additional commitments under its contracts or other documentation. Chapter 4, Understanding Legal Obligations to Provide Data Security, of the recently published third edition of the ABA Cybersecurity Handbook, as well as the books appendices identify various potential legal requirements, and could serve as a valuable aid in conducting this analysis.

3. Implementing appropriate cyber security policies, practices and technical controls

Once an organization identifies their sensitive data, and determines the legal, ethical, or other obligations that pertain to the protection of that data, an organization must next develop a comprehensive cybersecurity plan tailored to its organizational needs and risk tolerances. The plan should cover the management of all aspects of its infrastructure, including technical, operational and management controls, policies, and practices. To develop the plan, an entity will need to review existing measures and determine where technical or policy updates or upgrades are appropriate to guard against current cyber risks. As part of this process, an entity may decide to make technical improvements (e.g., enhancing its firewall rules or approaches, requiring multi-factor authentication rather than relying solely on passwords, increasing visibility to its network activity) or potentially to shift some data to different internal or external computing environments. Similarly, a review of current policies and procedures may result in adoption of a wide array of changes (e.g., reducing the number of user accounts with administrative rights, more stringent password requirements, denoting emails with a special marking indicating an email is externally received). Entities often rely on external expertise to help identify what potential changes make the most sense given the entity's cyber risks, risk tolerances and budget. Many organizations, including the federal Cybersecurity and Infrastructure Security Agency (CISA), the Federal Trade Commission, and other agencies maintain and update numerous resources to help companies enhance their cybersecurity postures. For example, CISA released a *Security Tip* focused on the importance of security patches and software updates, with a list of best practices, including enabling automatic software updates, ensuring such updates originate from trusted networks, and verifying trusted vendor sites.

Once a plan is adopted, it must be regularly reassessed and enhanced; it cannot simply be a check-the-box exercise that sits in someone's desk drawer. An entity must ensure it assigns responsibility for its implementation and updates the plan regularly given the rapid evolution of both cyber risks and technology. Malicious cyber actors are continually adapting new methods to gain unauthorized access to information, systems, and networks. The increase in ransomware incidents in recent years is an excellent example of an important change to the cyber threat environment. An entity's ability to adapt by adopting new administrative, technical, and operational controls by updating their plan will be a key factor in ensuring its continued cyber readiness.

4. Culture and training

According to a study by IBM, human error from inside the organization is a major contributing factor in 95 percent of all cybersecurity breaches. Ensuring all parties involved have strong training on cybersecurity, can dramatically decrease the likelihood of a successful breach. To maximize an organization's chances of avoiding a cyber incident. This can be best achieved by creating a culture of responsibility around data security and cyber incident response. Adoption of a training plan tailored to employees' responsibilities is key to reducing your entity's cyber risk. Training on cybersecurity issues should be regular and accessible. A culture of responsibility around cybersecurity ensures that each member of your organization is aware of their cyber-related duties to prevent a successful cyber incident.

As Ruth Hill Bro, a former chair of the Task Force, and Jill Rhodes, an editor of the third edition of the Cybersecurity Handbook, wrote, organizations should "Get SMART on Data Protection Training." SMART training consists of five steps: (1) **S**tart training on hiring, (2) **M**easure what you do, (3) **A**lways train, (4) **R**aise awareness and provide updates continually, and (5) **T**ailor training by role. Following these guidelines can help organizations and individuals plan ahead and ensure that everyone has the cybersecurity training and education they need to safely respond to an incident. By framing training and education as an ongoing responsibility, organizations can drastically improve their incident response to a cyber threat.

Conclusion

Even those entities that have effective cyber programs may experience a hostile cyber incident. The question is no longer whether a cyber incident or data breach will occur, but rather when one will. The response to a cyber incident can have long-term implications for state bars, bar associations, lawyers, and their clients, and it is never too late to develop, revisit, or improve an incident response plan.

Many of the tools and strategies referenced in this article are explored in the third edition of the *ABA Cybersecurity Handbook.* The *Handbook* brings together experts and professionals from government, private practice, and the private sector to provide a data-driven comprehensive resource for the legal community. The *Handbook* can be found here, save 20% with the code ABACYBER20 through February 28, 2023.

In the next article in this series, we will discuss the cyber incident response, and how an organization can prepare for such an incident.