Cybersecurity Vendor Management

ABA Cybersecurity Legal Task Force

4/15/2023

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

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

This article, which is the final article in a special three-part cybersecurity series presented by the ABA Cybersecurity Legal Task Force, focuses on the need for bar organizations and other organizations to undertake affirmative steps to assess whether the service providers and third-party products on which your organization relies provide adequate cyber security protections. We provide both provide an overview of the cyber risks associated with third party vendors and products and recommend steps your organization can take to both identify and mitigate the risk consistent with your organization's cyber risk assessment. Even more importantly, we also introduce you to a valuable resource to facilitate addressing cybersecurity in vendor relationships: the "ABA Cybersecurity Legal Task Force's Vendor Contracting Project: Cybersecurity Checklist." This Checklist is available for download for free by ABA members.

Third-Party Cybersecurity Risks

In today's work environment, all organizations rely on third party services and/products in their digital environments. Some organizations, especially those that are small or medium-sized, may rely entirely on out-sourced computing resources (e.g., third-party IT service providers, the cloud). Thus, it can be said that the security of your bar organization (or law firm) could only be as strong as its weakest business partners.

Management of vendor relationships is critical to effective cybersecurity because many breaches happen through vendors. Take for example the December 2020 news of the SolarWinds breach. SolarWinds is an IT monitoring and management company that provides software tools for network systems operators. Though little-known before the breach, SolarWinds counted 425 of the Fortune 500 among its customers and multiple federal government agencies. Also revealed in December 2020, but with less media coverage was the breach of Accellion's file transfer tool, FTA, which impacted law firms Jones Day and Goodwin Proctor, among others. Unfortunately, many entities may not even realize how many vendor relationships they have, or what access their vendors will have to systems and data.

Effective Cybersecurity Vendor Management

Identifying and mitigating potential cyber risks should be a key component of your vendor management program. Proper cybersecurity vendor management must go beyond merely including a provision that the vendor will follow best practices and indemnify the organization (subject to any liability cap). Rather, an organization must conduct due diligence and ensure that adequate contractual terms are in place. You should use the procurement process as an opportunity to identify and specify specific risks and ensure that sufficient mitigations are in place.

1. Conducting Due Diligence

Before entering a vendor relationship, the current best practice is to conduct a due diligence risk assessment to identify and address any risks presented by the proposed transaction. Customers want to ensure that what they obtain from vendors at least maintain the level of cybersecurity required by applicable law, relevant security frameworks, and their own internal policies and procedures. Given today's cyber risks, it is critical that your organization conduct a thorough review of vendor's security controls as part of that due diligence, especially if the vendor will have access to your systems or sensitive data. From a cyber perspective, the due diligence should include a thorough review of the vendor's security controls and their security, incident response, and continuity/crisis management plans.

Cybersecurity due diligence activities start with conducting a security assessment of the vendor, evaluating the vendor's ability to manages its internal infrastructure consistent with cybersecurity objectives, and identifying past breaches and vulnerabilities in the vendor's systems. Qualified information security personnel and cyber lawyers should assist the customer to identify relevant areas of assessment and to evaluate the information provided by prospective vendors. Entities without such internal resources should retain outside technical and/or legal personnel to support the process.

Due diligence should typically not be limited solely to a documentation review, but rather should also include discussion to ensure the vendor's efforts will mitigate any risks in accordance with the purchaser's cybersecurity risk tolerance. As part of this process, it is also important to learn how the prospective vendor manages its own suppliers from a cybersecurity perspective especially if the scope of work will involve, or be dependent upon, the performance of those suppliers.

While the cybersecurity questions may vary depending on the anticipated scope of work and the risk tolerances of the parties, common key topics covered during due diligence typically include:

- written information security program
- third-party security certification or assessment (e.g., ISO 27001 or a SOC2 certification)
- back-up strategy and recovery plan and associated testing
- cyber insurance
- employee cybersecurity training program
- process that ensures systems are up-to-date and any patches promptly implemented
- process to conduct regular internal and external vulnerability scans and penetration testing and resolve identified issues

Entities often require vendors to complete cybersecurity questionnaires to facilitate the due diligence process. Some larger vendors may offer to provide customers with their own set of answers to their own standard security questions or risk assessments rather than respond to individualized questionnaires. The Checklist identifies various resources and tools for assembling due diligence questionnaires.

To the extent that security weaknesses are identified (e.g., weak passwords or password reset management, lack of multi-factor authentication, the purchasing entity needs to weigh these risks against the transaction's benefits and consider appropriate mitigation. The initial assessment and the planned remediation should inform the parties' agreement.

2. Cybersecurity Contract Provisions

The Checklist provides sample cybersecurity-related provisions and other resources that can be used in drafting appropriate contractual language for procurement contracts. Remember cybersecurity provisions must be tailored to reflect the specific transaction and specific risks and cover the whole lifecycle of the transaction. t is not enough to require a representation and warranty of "compliance with applicable and relevant laws or industry standards." The dynamic and evolving nature of cybersecurity vulnerabilities defies being tied simply to current law or a particular generic guidance document.

In addition to identifying the cybersecurity and privacy controls that must be implemented as part of the security program, the agreement's cybersecurity provisions should address an array of other issues, such issues as data ownership and access and use rights, confidentiality obligations, post-contract audit rights, cyber incident reporting obligations, remedies, data and transition obligations upon termination and/or expiration of the contract, cyber insurance obligations, and business continuity and resiliency obligations in the event of disruption of the vendor's operations.

Conclusion

Adequately addressing vendor-related cybersecurity risks has never been more important. It is increasingly important in our current increasingly interconnected environment of evolving cyber threats, increasing cyber incidents, new emerging technologies, and changing cyber laws, standards, and guidance. We hope that this article and our Cybersecurity Checklist helps you identify and better manage your entities' vendor-related cybersecurity risks.