CORPORATE COUNSEL
The Business Magazine for In-House Counsel
corpcounsel.com | January 4, 2021

How Legal Depts Can Implement a Law Firm Cybersecurity Assessment Program That Benefits All Players

Given the criticality of knowing and addressing our outside counsels' cyber risk, we set our sights on developing an assessment program that would provide ongoing digital evaluations of our law firms.

By Connie Brenton

Businesses face new cybersecurity threats from new bad actors daily, and high-profile cyber failures have taken major companies to their knees—and their executives along with them. As such, cybersecurity and risk management are top-of-mind for boards of directors and their leadership teams, including NetApp.

In January of 2020, the Office of Compliance Inspections and Examinations of the Securities and Exchange Commission (OCIE) published its **OCIE Cybersecurity and Resiliency Observations** report. The report identifies practices for managing and combating cybersecurity risks based on thousands of reviews. The cybersecurity management practices addressed include:

- Governance and risk management
- Access rights and controls
- Data loss prevention
- Mobile security
- Incident response and resiliency
- Training and awareness
- Vendor management

shutterstock

While all of these practice areas merit due consideration, vendor risk management is one area that has everyone's attention. Gartner research found that 75% of Fortune Global 500 companies treat vendor risk management as a board-level initiative to mitigate brand and reputational risk. While vendor risk management is a moving target, and staying one step ahead of the bad guys is extremely challenging, it is a "bet the company" issue, and it must be addressed comprehensively.

Flying Under the Radar No More

As important as vendor management is as a cybersecurity practice, historically, professional services providers like law, accounting and consulting firms generally have avoided being deemed a "vendor," as the term is used by virtually all corporations. In doing so, law firms have flown

under the cybersecurity radar because only "vendors" typically undergo cybersecurity reviews as a part of corporations' procurement teams' onboarding process. NetApp Legal Ops' informal survey of corporations showed this to be a common failing across virtually all industries with fewer than 15% of companies completing security assessments of their law firms. Unfortunately, recent history provides many cautionary tales demonstrating that law firms are just as vulnerable to cyber incidents as any other business. And the consequences of those vulnerabilities being exploited can be as bad or worse than failings associated with virtually all other vendors.

Given the criticality of knowing and addressing our outside counsels' cyber risk, our Legal Ops team, already focused on digital transformation, set our sights on improving our cybersecurity processes and developing an assessment program that would provide ongoing digital evaluations of our law firms in a way that would meet NetApp's constantly evolving cybersecurity needs. Our assessment process needed to evaluate our firms' security capabilities in key areas and create a benchmark risk score for each firm with an eye to mitigating risks to NetApp.

Scoping the Problem

NetApp Legal has been aware of the need to scrutinize law firm cybersecurity for some time, and we have undertaken efforts to secure information and assurances from our outside counsel. However, given that we entrust our law firms with very sensitive company data, we need to confirm that our firms continually demonstrate the same, if not greater, rigorous and ever-evolving security protections and assurances defined by NetApp's cybersecurity team.

Globally, NetApp regularly uses 38 outside law firms that handle a variety of matters including litigation, intellectual property and human resources. That's a relatively small number of firms for a Fortune 500 company. However, it's still enough to turn a non-automated review process into a major undertaking. So, full automation had to be a focus for any revamped process.

Reviewing Industry Practices

As a first step to updating our practices, we spoke with peers in other legal departments with advanced cybersecurity practices to understand what they were doing, what they were asking of their firms, and what actions they were taking after learning their firms' approaches to various issues. In addition, we reached out to our own firms and some industry leading firms to understand what they were doing for their customers. The NetApp team engaged in candid conversations with over 20 of the largest law firm CIOs to assess the state of the industry, and to discuss standards and best practices before updating our own Cyber assessment program.

Among the many things we discovered was that most law firms' information security (InfoSec) resources were overwhelmed with security assessment questionnaires. Although more than 80% of the content in the questionnaires law firms received from their clients was similar from assessment to assessment, the formats and sequence of questions differed radically. The questions, when aligned by topic, issue, etc., almost never asked anything different, but the wording was sufficiently different such that the firms had to spend an inexorably long amount of time to make sure they were responding accurately. These differences left law firms over-burdened—and often scrambling—to complete "unique" assessments in a timely fashion. Worst of all, the volume and length of the assessments cascading down on law firms was consuming critical law firm resources that should have been used to address security gaps.

In the end, it was abundantly clear that one of the most important things NetApp could do to improve our own security was to help law firms reduce the burden they carried in responding to client questionnaires. We concluded that we could help in two ways. First, we could streamline and optimize our own questionnaire and automate it. Second, we could begin working with other corporations to have them agree to a standardized process and questionnaire. This latter task would not be easy. Yet, it would be in everyone's great self-interest to even move a moderate fraction of companies. That could probably

free up enough law firm resources to improve overall cybersecurity in the law firm "vendor" space to make everyone more secure.

Defining a Scalable Digital Law Firm Cybersecurity Assessment

As a first step to revamping NetApp's assessment process, we reviewed the questions we were asking firms in our questionnaire with a full "acid test." Second, we defined what we needed to automate. The risks to be avoided and rewards to be had here were too great—we chose to leverage outside experts. So, we brought in two external partners to help create the framework for law firms to respond to using a standard, industry recognized questionnaire. We wanted something that, once complete, would allow law firms to give the same answers to many clients. The framework also needed to be able to morph as industry standards evolved. The two partners we selected were Keesal Propulsion Laboratories ("KP Labs") and Privva Inc. We selected these partners to perform the initial assessment and to establish an initial cybersecurity risk rating that we would then use to benchmark progress and activities year over year.

Questionnaires from Hell

To determine what questions were truly necessary for our questionnaire, we turned to NetApp's own cybersecurity experts, law firms' CIO's, KP Labs and Privva. The law firm CIOs we met with all described a similar situation: questionnaires that were all maddeningly long—from 1200 to as many as 1600 questions or more. However, the majority of the questions did not raise any issues, practices, etc., that would result in more or better information. It was simply a belt-and-suspenders approach. After very careful review with our own experts, KP Labs and Privva, we agreed fully with the law firms' analysis and recommendations.

Our first goal in streamlining and driving efficiency and addressing risk was to identify a robust but minimal set of questions to have a thorough assessment, but not overwhelm the firm answering it. Similarly, the questions selected needed to address most of the cybersecurity issues that any corporation (except for relatively extreme corner cases) typically asked.

From our analysis, we determined that the law firm cybersecurity questionnaire by the Standardized Information Gathering Questionnaire from Shared Assessments (the "SIG") covered the bases fully and was also a relatively common questionnaire already used by many corporations in assessing firms. The 2020 SIG came in three sizes (the Lite has 325 questions, the Core has 950 questions, and the Full Content Library of questions has 1,515 questions). The SIG includes security and privacy and covers 18 major risk controls and has been around for about 10 years.

After a final set of conversations and meeting with peers, security experts, law firms, NetApp chose the SIG Lite which was readily available on Privva's security assessment platform. That would allow us to automate our process—a key goal from the outset.

The SIG Lite is updated annually, so we can update our process continuously and run the assessment year over year to reflect new and updated changes as the industry continuously improves. Our goal was not to reinvent the wheel but instead use an industry standard framework, making the process easier for the law firms as well.

Leveraging Technology and SIG Lite

One of the key components of NetApp's Cyber assessment solution was implementation of the Privva "Vendor and Client Risk Management" technology. Privva's technology allowed NetApp's Legal team to generate a baseline cybersecurity evaluation of all NetApp's outside counsel law firms as part of our overarching digital transformation program.

Once implemented, the Cyber assessment process was seamless, and our law firms had their questionnaires in-hand within 14 days. The entire assessment process of all our firms was completed within 90 days.

Most firms agreed to complete the questionnaire without hesitation. A firm's willingness to complete the questionnaire became a leading indicator that they would continue to partner with NetApp on security going forward.

The firms completed and submitted answers to the questionnaires directly in Privva. The Privva database then stored the law

firms' answers to the questions and the system easily generated assessment responses for their subsequent review and revision.

Law Firm Ranking and Report Card

Once the questionnaires were completed, Privva presented the risk scores in a "report card" dashboard which visually represented how our firms ranked in different areas and how they compared to one another. The high-level summary included several findings and corresponding unintended consequences. The preliminary score range was 65-100%, and many firms follow up with questions and clarification before submitting.

Surprises and Lessons Learned

Despite acknowledging the importance of vendor risk assessments, as well as the acceptability of the SIG framework, some firms were resistant to filling out NetApp's assessment sent via the Privva platform. This included some of the largest firms. And while the majority of the firms to which we sent our questionnaire responded, many firms did not know how to answer the questions despite that fact that we used the SIG, which is a widely accepted industry standard questionnaire. On the bright side, some firms requested clarification throughout the response process, and they used the process as an opportunity to learn about certain security controls which will have long-term benefits for both parties. Had we not used an industry standard like SIG, we can only imagine how problematic the process would have been with a form replete with non-standard questions and language. Still there is a need for an education process, especially as it relates to smaller/medium sized law firms.

Surprisingly, a good number of the firms that responded made little or no effort to communicate with us despite being confused by any number of questions in the assessment. They made no attempt to clarify any of the questions *before* submitting answers. That resulted in a waste of everyone's time. Going forward, we will take the opportunity to meet with firms first before sending them our questionnaire. And, where appropriate, we will educate law firms in real time and encourage communication from the beginning. We can ensure they understand this process is not to get them in trouble, etc. We will think about offering to do a pre-assessment webinar session.

Many smaller firms, such as solo practitioners, answered N/A to many of the questions. After speaking with them, we determined that small firms need some extra guidance in best practices, and it is important to ask for compensating controls during the audit process. It is not fair to penalize smaller firms for not having an enterprise security program in place, but they may have other guidelines and practices that provide sufficient assurances to provide compliance with your cybersecurity needs. Ultimately, NetApp may need to create different assessments based on size/maturity of the firm at issue to get the information we need to evaluate the firm's cybersecurity practices and to determine if they are or can meet our requirements even with changes. In some rare cases, a firm may not be able to meet our requirements, and we will need to create a secure environment to provide access to data within NetApp's data environment if we want to use that firm.

Based on the report card results and analyzing the data, NetApp's team, in collaboration with KP Labs and Privva developed and communicated a customized remediation plan to each law firm, to mitigate or eliminate risks detected throughout the questionnaire process. NetApp's Cyber assessment showed us which firms were keeping current and staying vigilant regarding cybersecurity protections. The Cyber assessment allowed us to have frank, thoughtful conversations about needed changes and improvements and we collaboratively developed remediation plans and timelines. Without the report card from Privva, parsing the questionnaires and trying to make sense of the data across many firms with different risk profiles (based on the data they handled), would have been inordinately time consuming or impossible in some cases. Data visualization allowed us to understand our needs and the actions firms needed to take in a way that was efficient and led to effective short and long-term outcomes.

A New Collaborative Approach with Law Firms

NetApp planned for Year 1 of this program to be a collaborative win-win process with our law firms. The questionnaires clearly told our firms which subjective and objective criteria were important to us.

The baseline numbers showed that larger firms generally scored higher than solo practitioners. We realized that solo firms may not have the money, expertise or resources to build an internal cyber program, but there are certain foundations which scale well to even small firms and solo practitioners and are critical for securing sensitive information. For example, strong passwords, security awareness training, and automatic system and antivirus updates prevent the majority of breaches and are accessible to anyone with a computer.

Now when NetApp hires a new law firm, they are immediately included in the assessment process. We have created a workflow in Mitratech's TAP Workflow Automation technology that automatically sends out the Privva cyber assessment questionnaire as a part of our onboarding process.

While Year 1 has been educational and collaborative, Year 2 will focus on enforcing our policies and requiring firms to meet expectations. Minimum requirements will need to be met, and firms with low scores that have not acted positively to improve their assessment performance will come under closer examination, or will be replaced by those that meet our requirements.

Surprising Results

The NetApp outside counsel assessment program yielded some unexpected results, all of which showed that education and due diligence about law firm cybersecurity is still needed.

- 37% of our law firms confirmed that fourth parties have access to NetApp data, showing their data risks and exposure went beyond their firm alone.
- 64% of questions had at least one N/A (not applicable) response, showing that some law firms either needed more clarification when answering standardized questions, or they were not even tracking that data sufficiently to provide a response.
- Most firms had already retained a third party to review their security controls, but even those firms had control gaps.
- Firms were still thinking about how privacy regulations affect them—they are not 100% clear on how to proceed.

Cyber Assessment Provided a Complete View of Law Firm Risk

The outside counsel cyber assessment project at NetApp has led to a rapid and successful process revamp. We have a clearer picture of the security risks associated with our use of outside counsel than ever before. And with Privva's Vendor and Client Risk Management technology, we are equipped with the tools to continue a vigilant, metric-based approach into the future. Our approach has reduced the strain on NetApp's own information security ("InfoSec") resources, as well as those of our law firms, too. Law firms' InfoSec resources can now focus on keeping our client data safe rather than filling out tedious questionnaires.

The cyber assessment program provided NetApp with a complete view of law firm risk. We gained a deep understanding of how our law firms, large and small, were securing their networks, data and systems. Each firm that participated in the process walked away with a remediation plan to mitigate potential risks. We track their resolution of issues and provide help when needed. At NetApp, vendor risk assessment is now an annual standardized hygiene process. The cyber assessment initiative has had made our risk management and data security protections even stronger.

NetApp will continue to collaborate within the industry to help create a more standardized cybersecurity assessment process.

Connie Brenton *is VP of Law, Technology and Operations at NetApp Inc. She leverages her legal and business experience to foster continuous improvement in the NetApp legal department, which has been recognized internationally for innovation. She can be reached at* ***Connie.Brenton@NetApp.com***