Protecting Your Data and Reputation in the Pandemic Age:

A Guide For Corporate Legal Officers

Empowering your team to effectively manage and mitigate third-party risks

Counself®

www.counself.com | 1-833-545-8324 | info@counself.com

Protecting Your Data and Reputation in the Pandemic Age:

A Guide For Corporate Legal Officers

For the past several years, corporate legal department management has been adjusting to a new world - one where data breaches and cyber attacks are growing in number and impact. Millions of dollars have been spent to rectify, justify and compensate for the colossal financial and reputational damage sustained as a result of seemingly harmless interactions with vendors. An infamous example is the unfortunate lesson Target had to learn back in 2013, when an inconspicuous security shortcut snowballed into a massive breach and an investigation that resulted in the firing of its CEO. Shortly after, other prominent companies followed: Sony, Home Depot … but these examples merely represent the tip of the iceberg.

The Landscape

The business world continues to recognize and adjust to the fact that company executives will be held personally responsible for data breaches. In the case of the Target breach, it turned out to be a vendor with access they didn't need, who unintentionally downloaded a phishing email. Supply chain security is fundamental, particularly because law firms and legal services firms, rich with confidential data and PII, have become prime targets for cybercriminals. Attacks are happening at a more rapid pace, and the breaches are more consequential.

Since most law firms are privately owned, they do not face the same compliance requirements publicly held companies do, or the rigorous regulatory reporting financial institutions do. This is alarming. Since law firms not only have access to their clients' most confidential and valuable information, smaller firms tend to employ fewer security measures, which makes them especially irresistible to hackers and cybercriminals looking for backdoor access.

42%
of the U.S. labor force now working from home

77%
of CLOs expect remote working going forward

Taking into account the additional challenges and changes due to COVID-19, it is clear how in an already exposed environment, the ramifications may take years to resolve and restabilize. According to Stanford economist Nicholas Bloom, the new "work-from-home economy" created by the virus is likely to continue long past the pandemic that spawned it. An incredible 42% of the U.S. labor force is now working from home full-time.[1]

The 2020 Altman Weil Survey points to the colossal and multi-faceted impact of the pandemic on corporate legal departments: decreased revenues, a surging workload, layoffs and downsizing, as well as a significant reduction in vendor budgets. Of the CLOs surveyed, 77% expect remote working will be a common practice going forward. The need for more security training, oversight, and efficient tools to adapt quickly to this environment is critical.[2]

The Numbers

The average cost of a data breach to a corporation globally is $3.86 million, according to IBM's 2020 Cost of a Data Breach Report. In the United States, the total is $8.86 million - more than double the global average. Even more concerning is the fact the average time to identify and contain a data breach is 280 days - nearly an entire year. Further, the damage and long-term costs are felt by corporations for several years after the incident. In fact, 39% of the total costs of a breach are incurred a year after the incident. The largest contributing factor to this cost is the loss of business, accounting for an average of $1.52 million – 40% of total loss.[3]

Companies that have deployed a security automation process have seen significant savings improvements over those that have no such systems in place; however, keep in mind, there is hardly ever a one-size-fits-all solution. For maximum protection, it is important to evaluate specific business and industry needs depending on the type of data your organization receives, stores, or transmits.

The Guidelines

In order to address new and emerging cyber dangers, The American Bar Association issued several rules that specifically cover data protection and cybersecurity. These Model Rules of Professional Conduct (1.1, 1.4 and 1.6 respectively) require lawyers to "keep abreast of… the benefits and risks associated with relevant technology" and "ensure that the tools used to communicate are secure;" and finally "prevent the inadvertent or unauthorized disclosure of… or access to, information relating to the representation of a client."

Legal departments are understandably demanding increased security from their firms. Third-Party Risk Management (TPRM) guidelines have been issued by a variety of vendors in the legal space. Despite these efforts to respond to the crisis, the ABA's 2020 Cybersecurity Survey reveals some glaring gaps in law firms' awareness, rules and response plans to data breaches, especially in larger firms. Overall, 29% of firms report having experienced a security breach, however, 21% do not know whether they have had one. Shockingly, the rate of unawareness in firms of 100+ attorneys totals 62% - meaning in a large firm, nearly two-thirds of practitioners have no idea if their data has been compromised.

More sobering is the fact that only a third, 34%, of firms have incident response plans in place. The ABA concludes that

> ***"professionals in firms of all sizes need to synthesize good cybersecurity practices into the everyday practice of law."***

The Road Map

How can legal departments best protect themselves? Here are some best steps to ensure the oversight and monitoring of sensitive data:

1. Define relevant performance and security criteria for outside counsel. These will serve as your first source of data for effectively monitoring vendor performance and risk against your priorities and expectations.
2. Categorize your vendors based on their risk level to you. Less sensitive information is exchanged with a firm handling a Class Action matter that took place in the past, while more risk is involved with matters concerning future actions such as M&A or IP transactions.
3. Once you have your criteria, put it into action, utilizing your team to monitor and assess vendors, establishing a regular dialog to collect feedback and improve processes.
4. Enforce vendor compliance. You are only as strong as your weakest link. If you suspect any lack of transparency or non-compliant activity, escalate it immediately.
5. Automate your manual processes. Use available tools that will help cut down human error, increase efficiency and resolve collaboration challenges.

Case In Point

You don't have to take our word for it.

In 2017, a major financial institution encountered a colossal challenge in cybersecurity. As the Federal Reserve Board conducted its scheduled audit, it demanded to examine the risk management program in place for each of the bank's third-party vendors, including over 150 law firms.

This new level of governance took the bank by surprise - especially since they had a robust risk management program in place for several years and had never experienced a breach. The regulators gave three months for the submission of an action plan of due diligence - a Material Request for Action (MRA).

The Challenge:

Using a standard corporate procurement process, vendors generally require several months to onboard. Repeating this process for each of the 150+ law firms posed a seemingly insurmountable problem for the legal department. This is where Counself was chosen to reduce law firm onboarding time and to streamline legal vendor due diligence.

The Solution:

Recognizing that crucial communications with law firms were stored in several different places, such as emails, Excel and other documents in shared folders, we worked to centralize and organize all points of contact and made this information easily searchable and accessible in one place. Once an RFI or questionnaire is created, it can be saved and used again, sent to numerous firms with one click. The client users were able to use Counself to communicate directly and effectively with different firms, all in one place.

Counself also provided them with a dashboard of all requests, responses, tasks, and deadlines, placing the entire process at their fingertips, as well as giving regulators the ability to quickly and easily monitor all activities for compliance.

The Results:

After having only used Counself for six months, the legal compliance team shared feedback raving about the ease of reference across questionnaire responses, and continues to use Counself as a daily vendor management and compliance tool.

23 Corporate Plaza Dr.
Suite 280
Newport Beach, CA 92660

1-833-LGL-TECH

Counself is a highly secure and ISO certified tool designed specifically to enable Legal Ops teams to manage their legal vendors and mitigate risk. We provide a convenient, secure, compliant and customized solution for law firm and vendor due diligence, onboarding and continued monitoring.

We work with our clients to facilitate collaboration with vendors and increase efficiency, cut costs, and maximize the potential of data they already possess.

Contact us to see how our solutions will save you time, money and safeguard your data and your reputation.

Article Sources:

1. Stanford Report, "Stanford research provides a snapshot of a new working-from-home economy" June 29, 2020
2. Altman Weil, "Law Firms in Transition 2020: An Altman Weil Flash Survey"
3. IBM Security, "Cost of a Data Breach Report 2020"
4. American Bar Association, "ABA TechReport 2020"