BAKER TILLY

Accountants and Advisors

"Attorneys' and hackers' eyes only": cybersecurity risk management program for law firms

By David Gola, Senior manager

Since the American Institute of Certified Professional Accountants (AICPA) issued guidance relating to a cybersecurity risk management reporting framework, many service industries have considered adopting this new framework as a key component to their risk management program. More specifically, law firms and other professional services organizations have considered implementing this framework as they look to improve their cybersecurity safeguards and other key controls to combat the increasing threat of data breaches that have plagued society in today's technological age.

The new System and Organization Controls (SOC) for Cybersecurity guidance provides a common language for organizations to use in describing their cybersecurity risk management program effectiveness. Put simply, it establishes baseline standards for auditors to confirm independently that an organization's cybersecurity preparedness meets acceptable guidelines. Such attestation represents a new opportunity for gaining assurance about cybersecurity and it is not without cost. So why is it important, and to whom?

Many senior leaders and board members worry about the effectiveness of their law firm's cybersecurity measures and desire verification to obtain assurance. The potential of significant financial and reputational risks outweighs the effort and cost of achieving greater confidence.

However, external stakeholders will likely drive the majority of initial interest in cybersecurity risk management reporting via the new SOC for Cybersecurity guidance. Those seeking to minimize risk – clients, prospective clients, lenders, investors and analysts, M&A attorneys and advisors, insurance providers and regulators – may see an immediate benefit by obtaining a SOC for Cybersecurity report as part of their due diligence.

With clients now requesting additional assurances related to the overall security of their data, law firms are now in a position of having to respond to these additional requests on a more frequent basis. As a result, this puts an additional burden on IT and other supporting departments needed to fulfill these requests. Large firms may be able to absorb the added resources and costs associated with each client request; however, it's the small and midsize firms that will suffer the most as they may not have the capacity or time to fulfill these requests completely without allowing other areas and responsibilities to suffer.

The SOC for Cybersecurity report is designed in such a way that allows law firms the ability to distribute an objective and independent report over their firm's cybersecurity controls and

safeguards, while also reducing the cost of compliance and the additional burden on their supporting team members.

Breaches pose a significant risk at small, midsize and large firms

Organizations that fail to prepare adequately for cybersecurity breaches expose themselves to substantial risks. Most cybersecurity experts agree that a breach is not a matter of "if," but a matter of "when." According to the American Bar Association's 2017 Legal Technology Survey Report, 35 percent of firms with 10-49 attorneys reported experiencing a security-related breach, and 23 percent of large firms with more than 500 attorneys also reported they had experienced a breach. On the other hand, another figure indicated that 56 percent of overall respondents reported that their firm had not experienced a security-related breach.[1] One could argue – quite reasonably, given the months and years it can take to recognize a breach – that the 56 percent simply don't know it yet.

Broadly speaking, the risk posed by cybersecurity breaches takes on three key forms:

- **Financial:** Irrespective of industry, organization size or type of attack, data breaches present substantial costs. These costs include everything from technology investments, legal fees, notification costs and lost sales. A 2018 study of 65 organizations that had experienced a data breach noted an average total cost per breach of $7.91 million.[2]
- **Reputational:** Cyberattacks can be public relations disasters and create intense fallout from a consumer standpoint. One survey found that 70 percent of consumers stated that they would stop doing business with an organization if it experienced a data breach.[3] For example, the law firm Mossack Fonseca announced in March 2018 that it was shutting operations due to "reputational deterioration" since its widely publicized data breach was announced less than two years ago.[4]
- **Compliance/legal:** The labyrinth of complex cybersecurity laws varies based on a variety of factors, including location, industry, type of data and type of breach. Failure to comply exposes an organization to lawsuits, regulatory scrutiny and punitive action. Numerous federal agencies – from the Federal Trade Commission and Department of Defense to Health and Human Services, to name a few – can take action for failure to safeguard information adequately. Likewise, private sector suits brought by consumers and employees are becoming commonplace.

AICPA guidance adoption elevates confidence in an organization's preparedness

The AICPA's SOC for Cybersecurity guidance provides an important tool for defining the increasingly valuable role of providing controls assurance for effective cybersecurity. Practically speaking, the guidance helps organizations understand what they should have in place to evaluate their cybersecurity controls.

The guidance lays out nine categories to describe and assess a firm's cybersecurity framework. These include:

1. Nature of the business and operations
2. Nature of information at risk
3. Cybersecurity risk management program objectives
4. Factors that have a significant effect on inherent risks related to the use of technology
5. Cybersecurity risk governance structure
6. Cybersecurity risk assessment process
7. Cybersecurity communications and quality of cybersecurity information
8. Monitoring of the cybersecurity risk management program
9. Cybersecurity control processes

Within each of the nine categories, the final guidance presents 26 related points of focus to help explain relevant aspects of an organization's cybersecurity risk management program.

Cybersecurity risk management reporting reduces specific risks to law firms

There are significant cybersecurity risks that can impact law firms of varying sizes, and the need for clients to be able to safeguard their sensitive and confidential information is paramount. What good is it to use disclosure restrictions on attorney-client documents if your firm experiences a breach? You might as well use the designation "attorneys' and hackers' eyes only" instead.

The Mossack Fonseca law firm breach taught us a number of lessons as it pertains to safeguarding your firm's environment and sensitive client information. The biggest failure made by Mossack Fonseca was due in part by an outdated version of Outlook Web Access (OWA) email and a client access portal that was supported by an obsolete and insecure security protocol (SSL v2 protocol).[5] Both OWA email systems and client portals are considered common methods to transmit client information and other sensitive data. It is these exact types of technologies that would be part of any SOC for Cybersecurity examination.

Cybersecurity risk management reporting adds to existing resources

For example, a SOC 2© report can enable firms to report on the security processes designed to protect their client's data. SOC 2© reports enable clients and other user entities to assess the security of their attorney's client-facing systems and their ability to mitigate technical risks. SOC for Cybersecurity reporting, on the other hand, addresses enterprise-wide security and its ability to mitigate business risk.

Cybersecurity risk management reporting also strengthens governance approaches as outlined in the Director's Handbook on Cyber-Risk Oversight by the National Association of Corporate

Directors (NACD). The handbook lays out five principles for board-level oversight. These include understanding the risks, recruiting board-level expertise, hiring the right people, investing in solutions and understanding how to mitigate risk. Cybersecurity risk management reporting builds on these NACD principles to give boards and organizational leadership the assurance that the organization delivers on the five principles at a practical level.

Cybersecurity risk management reporting improves preparedness

Cybersecurity risk management reporting does not provide a cure or panacea. It cannot guarantee that an organization won't be breached. Instead, it demonstrates that an organization is prepared to effectively and efficiently prevent or detect, respond to and recover from a breach.

The financial, reputational and legal risks outlined above intensify in the context of inadequate preparation. If a breach goes undetected for an extended period of time, involves significant amounts of sensitive data or involves improper, ill-timed or insufficient notifications to affected parties, the associated costs increase dramatically.

Yahoo did not detect its widely publicized 2014 breach for two years. The U.S. Office of Personnel Management left government employees' data exposed for a full year. In these cases, it wasn't the breaches that did the damage, it was the time it took to detect, respond and recover.

Cybersecurity risk management reporting gives law firms the objective assurance that the appropriate systems, processes and controls exist to manage a cyberattack.

Cybersecurity reporting enhances due diligence

There are many stakeholders whose interests and decision making depend on accurately assessing cybersecurity preparedness and risk. These parties will be well advised to integrate cybersecurity risk management reporting into their due diligence. They include:

- **Lenders:** Providers of financing have an interest in confirming the stability of their debtors' cybersecurity frameworks. In fact, some lenders already include third-party cybersecurity review as a condition of closing. Cybersecurity risk management reporting could fill such a need.
- **Investors and analysts:** Cybersecurity preparedness provides an indicator of an organization's overall health and certainly a predictor of any issues that could arise in the near term. As such, analysts are likely to take an interest in cybersecurity as part of overall efforts to assess vulnerabilities.
- **M&A attorneys and advisors:** With the value of data at a premium and a well-documented gap between the time of a breach and detection, those involved in M&A

transactions could see cybersecurity risk management reporting as an element of due diligence in understanding the value and risks associated with the transaction.

- **Insurance providers:** While important, insurance isn't the foolproof safety net some organizations think it is. Sony, Cottage Health and P.F. Chang's have all been involved in costly legal battles with their insurers over what losses their cyber insurance policies actually cover. As costly cyberattacks continue, insurance companies are likely to step up efforts to assess the risk of cyber policies. Cybersecurity risk management reporting could serve as a valuable tool in such efforts.
- **Regulators:** Cybersecurity risk management reporting can provide a layer of compliance documentation for government agencies responsible for protecting national security, consumer interests, infrastructure and trade practices.

Bottom line: SOC for Cybersecurity reporting framework can improve a law firm's cybersecurity risk profile

Law firms of all shapes and sizes face cyber risks. As with most things related to cybersecurity, it is not a matter of "if," but a matter of "when." Some will seek to transfer these risks to insurance carriers. Others will create ad hoc solutions or simply hope for the best. Those looking to ensure their own security controls and protect their firms' interests will stay ahead of the curve by making the necessary investments before a devastating breach occurs.

Whether or not a small, midsize or large firm chooses to undergo cybersecurity risk management reporting proactively, stakeholder pressure to prove its cybersecurity risk management capabilities will continue to grow. The universe of possible circumstances and vested third parties demonstrates a clear need for objective cybersecurity reporting. Cybersecurity reporting will strengthen a law firm's profile and demonstrate that it proactively manages risk.

1 - *ABA* 2017 Legal Technology Survey Report, American Bar Association, 2018. https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html

2 - 2018 Cost of Data Breach Study: United States, IBM and Ponemon Institute, 2018. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&

3 - "70% of consumers would stop doing business with a company if it experienced a data breach," Gemalto, 2017. https://www.gemalto.com/press/pages/majority-of-consumers-would-stop-doing-business-with-companies-following-a-data-breach-finds-gemalto.aspx

4 - "Mossack Fonseca law firm to shut down after Panama Papers tax scandal," The Guardian, 2018. https://www.theguardian.com/world/2018/mar/14/mossack-fonseca-shut-down-panama-papers

5 - "The security flaws at the heart of the Panama Papers," Wired, 2016. https://www.wired.co.uk/article/panama-papers-mossack-fonseca-website-security-problems

Accountants and Advisors