Data Security

Cybersecurity: Not Ours—Theirs

When it comes to cyber-risk oversight, boards should look beyond the four walls of the organization.

By Phyllis Deiso

Globally, many cybersecurity discussions are focused on a company's internal security protocols and on the security protocols of key vendors, such as those that process credit card transactions. However, professional services firms (audit, law, and valuation firms, and consultants, etc.) are not immune to data loss or theft, and while these key service providers are handling valuable corporate data, providers are not often subject to scrutiny.

According to NetDiligence, a cyber-risk assessment and data breach services company, the professional services and healthcare sectors experienced the highest percentage of cyber-claims of all industries in 2017 at 18 percent each. This is not surprising given that hackers have an abundance of data at their disposal should they be successful in infiltrating a professional services firm: the penetration of one consulting firm can yield the data of thousands of individuals and companies.

Data provided to professional services firms often is highly confidential, and not just because it might include personal identification information such as Social Security numbers. Consider, for example, information sent to a law firm regarding a possible merger or about improper behavior by an executive. On a personal level, do you think twice about information provided to your mortgage broker, tax preparer, or financial planner?

The reality is that no information is safe. Upon transfer of information to a service provider, the company transfers control of that data to the service provider and should require the appropriate safeguards to be in place.

In fulfilling its cyber-risk oversight duties, it seems reasonable that the board may wish to revisit cybersecurity from a different perspective: not ours—theirs. Has the company's third-party cybersecurity risk management program recently and holistically addressed the issue of which professional services firms have access to or retain sensitive company data?

After determining which professional services firms have access to the company's data, there are a plethora of routine follow-up questions the company could consider, including, but not limited to:

- Who is privy to sensitive data sent to the firm?
- What does the professional services firm do with such information after they obtain it? How is it stored? Is the data provided to any subcontractors (e.g., a law firm sharing information with an expert witness who is assisting with the defense of a lawsuit)?
- How is the data protected as it travels via email from one professional to another?
- How long does the firm retain the information?
- What is the firm's information technology security policy (e.g., are employees' computers encrypted)?
- What is the time frame in which the professional services firm will alert the company should there be a data breach?
- Who is responsible for the costs if data is lost? Your insurance or theirs?

Key questions for the board:

- Does the company think through who uses the data and then alter its cybersecurity inquiries accordingly?
- Are we asking people at the right level within the firm to obtain an appropriate response?
- How do we monitor the responses to the inquiries? Have we considered validating that information by receiving the firm's service and organization controls report?

Although a disciplined approach may exist for internal cyber-risk management, now may be the time to consider whether that approach is broad enough to take into account all of those third parties outside the company that receive, store, or process company data. Cyber-risk parameters and board oversight must expand well beyond company boundaries to consider the procedures of professional service firms with access to your data. In other words, not just ours but theirs.

Phyllis Deiso is a partner and the national SEC Practice Leader for RSM US LLP.