Securing Investor Confidence on Cyber Efforts

October 2020

When evaluating both current and potential investments, investors are increasingly looking at cyber responsibility as a criterion. But they aren't just looking at the investee's cyber risk profile, they are also analyzing steps taken by industry peers. This means that at any given time, risk may be measured for your peers' businesses based on what you are doing, and vice versa. It's called the "contagion" effect, according to a study conducted at North Carolina State University, which reveals that when one company experiences a cybersecurity breach, other companies in the same field can also become less attractive to investors. However, companies that are forthcoming about their cybersecurity risk management efforts fare significantly better than those that wait until it's required.

When a company falls victim to a cyber breach, the most common knee-jerk reaction is to develop an incident response plan that tackles the vulnerability at hand. A software patch, for instance, is a quick fix, but it fails to address the broader picture. It's critical to have a comprehensive cyber program in place that aligns with overall business strategies. The program should cover asset identification all the way through to reporting and remediation in the event of a breach.

In BDO's 2020 Digital Transformation Survey of 600 c-suite executives at middle market organizations, 39% cited cyber attacks as the biggest digital threat to their business—a figure that has likely only increased as COVID-19 brought an uptick in privacy breaches.

Despite being an entity-wide issue, cyber awareness still falls on IT most of the time. In fact, we often see board members with little to no insight into their companies' cyber programs. According to a BDO survey of board directors, a full 39% said they were only somewhat or not at all familiar with their organization's data breach response plan. Another 37% said they were moderately familiar. Meanwhile, when asked if their company had cyber risk requirements that third-party vendors must comply with, 27% answered that they were not sure.

When a board member tells an investor what their cyber risk looks like, they need to be able to answer the question, "how do you know?" Just as boards receive financial updates and are well-versed in how they're

Trout CPA®
Accounting | Tax | Advisory

tracking on sales, accounts receivable and where their business is falling short, they should have the same level of insight into their cybersecurity function.

While companies have historically faced challenges in communicating with investors and other stakeholders on their cyber risk management programs, the AICPA's voluntary reporting guidelines provide a reporting framework that's broadly accepted. Following these guidelines for your cyber reporting is a good first step. However, third party verification of compliance can lend additional credibility.

Some companies are hesitant to go down the path of auditing their cyber efforts out of fear that it will uncover weaknesses and shine a spotlight on non-compliance issues. But the fact is, transparency and proactivity can help offset negative publicity and regulatory scrutiny in the aftermath of a breach.

Whether your cyber risk is under examination due to a data breach within your organization or a peer's, presenting a SOC for Cyber assessment could assuage investor concerns. It proves you have met the AICPA's voluntary reporting guidelines and are proactive about protecting your business' and customers' critical data assets.

Trout CPA®
Accounting | Tax | Advisory

For questions or assistance, please contact one of our professionals at 717-569-2900.

LANCASTER
1705 Oregon Pike
Lancaster, PA 17601
717-569-2900

LANCASTER CITY
160 E King Street
Lancaster, PA 17602
717-569-2900

MECHANICSBURG
930 Century Drive, Suite 104
Mechanicsburg, PA 17055
717-697-2900

CARLISLE
62 W Pomfret Street
Carlisle, PA 17013
717-243-4822