

TECH INSIGHTS



weaver  IT advisory services
Assurance • Tax • Advisory

HOW TO GUARD AGAINST CYBER SECURITY RISKS

The Division of Corporation Finance, a part of the Securities and Exchange Commission, has issued guidance on disclosure obligations related to cyber security risks and incidents. And although public companies aren't yet required to disclose this information to shareholders, it's just a matter of time until it is required.

Right now, this is simply guidance in the best interest for your shareholders, but that will likely change. It could become a requirement, probably sooner rather than later.

When the Senate headed for its August recess, efforts were made to pass cyber legislation. Although the bill didn't pass, more regulation surrounding cyber risks and security are certainly coming.

Brittany Teare, IT advisory manager, answers a few key questions about what the current guidance entails and how businesses can measure and guard against cyber risks.

Have the SEC Reporting Requirements for Cyber Security Changed with this Guidance?

The new guidance takes the existing requirements that public companies follow and expands upon them. There's no mandatory piece yet that results in a direct impact on a company if it doesn't disclose information on cyber incidents.

Basically, the guidance states that if cyber security risks and cyber incidents have a material effect on your shareholders — if it could affect how financial information is reported — you have to report them to the SEC.

How Can You Tell When Cyber Security Risks Are Going to Materially Impact Your Company?

The guidance addresses some of the possible risks and whether they should be voluntarily reported to shareholders. For example, if a company doesn't have cyber security controls around its key financial systems or intellectual property, then the manner in which data is recorded or reported could be easily manipulated or altered. The SEC wants companies to report on these risks to first pressure public companies to resolve them, and second to assist investors in evaluating the risk associated with cyber security. Even if a cyber breach has not yet occurred, it is likely to occur in the future.

Cyber security itself is a gray area. Employers typically know that network and perimeter security, access and change controls should be in place, however executives may not consider disclosing vulnerabilities. CEOs and CFOs are used to looking at the balance sheet and seeing line items for hardware and other things they can touch. It can be challenging to consider the likelihood and risk that the organization could be breached and the ways it could happen. Addressing weaknesses is something that companies need to continue to do.

What are Your Thoughts About Quantifying Data and Seeing Vulnerabilities from a CEO's Perspective?

A starting point is to designate a person or group of people responsible for cyber security. These people should understand where the SEC is at in passing new regulations and where requirements are potentially heading with this guidance. In



Companies should use complex, strong passwords to help protect the network, systems and data, and regularly change them. The system should lock out users after a certain number of failed attempts.

In addition, they should identify risks to the specific organization.

There is a central entry point in any network, but key people need to know where the most sensitive data is located since this is where an attacker will target. If an attacker can access the most sensitive data in a network, this could lead to a huge loss. If the company does not store much of this type of information, then an attack could involve a company's reputation, which is much more difficult to value.

Another challenge is improving communication from the CIO or IT manager. Often, IT will say, 'We need X dollars for new equipment, applications and hardware that are going to help make our organization more secure.' It's usually a considerable amount of money and can be millions of dollars in larger organizations. Since IT infrastructure can be expensive over a short period of time, explaining the return on investment (ROI) can be a struggle. It's important for CIO and CFO groups to work together to effectively identify and communicate the ROI with IT expenditures.

A CIO needs to be able to tell other executives, 'If this firewall, application or system is not installed, a breach could cost us X dollars, or the company could lose X dollars per day,' for example. Not everything can be quantified, such as a company's reputation, but this gives CIOs a place to start.

Is Cyber Security a Big Factor for Investors?

Yes, and it is becoming more so as the public realizes the prevalence of cyber attacks. Shareholders and employers alike are justifiably concerned about this because some of the most secure companies in the world have been breached in the recent past. For example, RSA, which provides security management solutions such as strong two-factor authentication for many well-known organizations, was recently breached. If a large company that specializes in security can be breached, then small and mid-market companies are susceptible.

What are Some Steps Businesses Should Take to Protect Their Data and Reputation?

There are key, high-level steps that companies should consider:

- Take inventory of the data systems and gain an understanding of where critical data is located.
 - Then, work to ensure that there is an appropriate amount of security around those areas.
- Use complex, strong passwords to help protect the network, systems and data and regularly change them.
 - Set the system to lock out users after a certain number of failed attempts and log all such activity.
- Most importantly, heavily monitor the networks and all systems.
 - Check who is logging in and from where, who is successfully entering and who is failing.
 - Then set a baseline to understand any abnormalities.
- Use the principle of least privilege, especially for critical accounts and functions.
 - This ensures that no single employee has all access; instead, access is tailored to the job function.
 - If there is a breach, it prevents those accounts from being abused for something they shouldn't be used for in the first place.

These simple steps are often overlooked by many companies. There is much more that companies can do, but first take small steps to implement fundamental controls. Then, if a breach occurs, the company can more easily identify what and how it happened.

Disclaimer: This content is general in nature and is not intended to serve as accounting, legal or other professional services advice. Weaver assumes no responsibility for the reader's reliance on this information. Before implementing any of the ideas contained in this publication, readers should consult with a professional advisor to determine whether the ideas apply to their unique circumstances.

© Copyright 2013, Weaver and Tidwell, L.L.P.

Weaver has offices in Austin, Dallas, Fort Worth, Houston, Midland, Odessa and San Antonio, Texas and Stamford, Connecticut.

CONTACT US

BRITTANY TEARE

Manager, IT Advisory Services

Brittany.Teare@weaverllp.com, 942.448.9299

BRIAN THOMAS, CISA, CISSP

Partner, IT Advisory Services

Brian.Thomas@weaverllp.com, 713.800.1050

More at weaverllp.com