IT Insights

Cyber Security Risks

How to guard against cyber security risks

THE DIVISION OF CORPORATION FINANCE, a part of the Securities and Exchange Commission, issued guidance on disclosure obligations related to cyber security risks and incidents. This is simply guidance in the best interest for your shareholders. Public companies aren't required to disclose this information to shareholders, but it could become a requirement in the future.

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

What does the guidance outline as the SEC reporting requirements for cyber security?

THE GUIDANCE EXPANDED upon the existing requirements that public companies follow. There's no mandatory piece yet that results in a direct impact on a company if it doesn't disclose information on cyber incidents.

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.

weaver
Assurance • Tax • Advisory

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 the status of proposed and final SEC regulations. 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. If larger companies can be breached, then small and mid-market companies are susceptible.

What are some steps businesses should take to protect their data and reputation?

HERE 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.

CONTACT US

Brittany George, CISA
Sr. Manager, IT Advisory Services
brittany.george@weaver.com

Brian Thomas, CISA, CISSP
Partner, IT Advisory Services
brian.thomas@weaver.com

Weaver's IT advisory services group focuses on delivering performance-enhancing consultations that address your IT and business agendas. We work directly with CIOs and others to create a more risk-aware, effective IT organization that can drive process efficiencies throughout your company and better support and deliver transformational business change. Specific services we provide include:

- Application controls review
- Business continuity/disaster recovery
- Cloud computing assessment
- Data analytics
- Data privacy
- Information security and vulnerability assessment
- ISO27001 reviews
- IT audit
- IT governance and organizational effectiveness
- IT risk assessment
- Pre- and post-implementation application reviews
- System and Organization Controls (SOC) reporting

weaver
Assurance • Tax • Advisory