INSIGHTS

Cyber made simple.

SEC REQUIRES CYBER EXPERTISE

BY JAY BORDEN

An original proposal by the SEC mandated a named cybersecurity expert on the Board of Directors and one in the company.

They have since walked that back and don't require a named member of the board with cybersecurity expertise.

But they are still very focused on improving cybersecurity oversight on companies. The new requirement is for "registrants to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats."

The SEC understands that unless the most senior management and Board of Directors of a company understand the impact of cyber risks to the company, and the fundamental need for cybersecurity, companies will not give it the budget, staffing or priority required. Equally important is the ability to impact other department's decisions. For instance, Sales may want a new product or service to be introduced as soon as possible. But unless the new offering has proper cybersecurity it will pose a serious risk to the company. Implementing the necessary cybersecurity at the design stage may delay the final introduction or increase the budget. But the SEC is saying that cybersecurity and the reduction of risk is important enough not be pushed aside.

What does this mean in practical terms? How do you describe this expertise? How are companies to report cybersecurity expertise to the SEC?

Interestingly, the SEC did not specify the level of cybersecurity expertise needed and left it to each company to decide for themselves. This level of ambiguity is consistent with other expertise requirements issued by the SEC.

onebrightlycyber.com
(888) 773-1920
A global leader in cyber service, technology, insurance and innovation.

INSIGHTS

Cyber made simple.

SEC Requires Cyber Expertise

Continued

So how do you ensure compliance? We believe it is the company, their competitors, and the industry that make that decision.

How will that take place? If a company experiences a breach, what occurred will become known. The precautions and protections put in place by the company will be reviewed by regulators, cyber insurers, and the public. If what the company did is found to be lacking, then the SEC can impose sanctions in addition to those imposed by the other constituencies. Their cyber insurer may refuse to cover the loss. Customers may look to other suppliers.

Companies wishing to avoid that kind of negative publicity, financial and reputational damage may choose to be proactive here.

Take a look at the cyber expertise of your peers and other companies in your industry and income group. How does the level of your cyber expertise and protections measure up? If it is found lacking, then up your game. Hire more experienced cyber talent or train your inhouse talent. Or engage a third party experienced in cyber protection to handle this for you.

This applies at the technical level, company management level, and Board level. If any one of these three is deficient it will affect your overall level of cyber expertise, cyber protections, and company-wide risk.

The need for technical skill is obvious. Management experience is required to understand what your technical experts are saying and what the Board is saying. Then to understand the risks, provide proper direction, and take the necessary steps to mitigate the risks and improve protections.

At the upper management and Board levels, cyber experience and understanding will become table stakes for those positions.

Let One Brightly Cyber help you understand this in more detail and take the necessary actions.

Need help or guidance? Learn how we can help you in so many ways.

Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.