The threat is real

Governing your company through the age of cybersecurity attacks

TODD BAUMGARTNER
Partner
Corporate & Securities Group
Brouse McDowell
(216) 830-6812

PATRICIA GAJDA
Chair
Corporate & Securities Group
Brouse McDowell
(216) 830-6819

WEBSITE: To learn more about what your company can do to protect against a cybersecurity attack and identify the threats that exist, visit www.brouse.com.

Insights Legal Affairs is brought to you by **Brouse McDowell**

Experts are now saying it is not a matter of if your company will suffer a cybersecurity attack, but rather when it will occur. With customer and vendor information at risk, as well as internal hacks into your company's systems and sensitive information, the risk is relevant and very real.

Smart Business spoke with Todd Baumgartner, Patricia Gajda, Rachael Mauk and Kate Wexler, attorneys with the Corporate & Securities Group at Brouse McDowell, about how to manage the threat.

What types of cybersecurity threats are out there?

Cybersecurity is the state of being protected against the criminal or unauthorized use of electronic data. Given that electronic data has become an ever-increasing component of a company's asset portfolio, the importance of protecting these assets has increased as well. Cybersecurity threats come from internal and external sources.

Although the headlines center on criminal activity, your employees' actions present an even greater threat. And while this group does include the disgruntled employee, your data is probably most at risk of exposure from employees opening emails from unknown sources, which may open the door to a hacker's access to the company's information systems.

Whose responsibility is it in a company to manage cybersecurity risk?

Consumers, shareholders, and regulators are looking to the board of directors to oversee the management of cybersecurity risk. Depending on the size of a company, the actual management of the risk may lie with the board or be delegated to a committee of the board (i.e., the audit committee or cybersecurity committee). The board needs to ensure that management of the risk is addressed. This entails developing a plan to prevent cybersecurity attacks and a response plan to mitigate the damages of an attack. It is clear in recent case law that the board will not be able to avail itself of the business judgment rule – to be reasonably informed – in its duty of care to the company if it fails in the oversight of cybersecurity.

What should directors ask to identify cybersecurity risk to their organization?

The board or committee needs to pose questions that center around five critical areas:

- Risk Assessment — What are our mission-critical assets? Have we assessed the probability of a cyberattack on these assets?
- Resources — Are we devoting adequate resources to address the risk presented to our organization? Is the budget sufficient to address the level of risk presented? Do we have qualified personnel to address the cybersecurity risks presented? Are we spending time training our employees to prevent data breaches?
- Standards — What standard are we using to design our cybersecurity policies and procedures?
- Crisis Response — Does the company have a cyber incident response team? Does our response team include members of our legal team to help address the legal and regulatory issues related to a cyber incident? Has our response team developed a cyber incident response plan?
- Disclosure — For public companies, are we making adequate disclosure of the cybersecurity risks facing our company? Are we prepared to meet state and federal regulatory requirements for disclosure of a breach? Does the company have a form of consumer notice with language and means of delivery for that notice?

What other preparatory measures can be taken?

Control insider threats by training your employees on your cybersecurity policies and the dangers of 'phishing' scams. Review your current insurance policies to see if you are covered for data breaches, regulatory investigations, misappropriation of intellectual property, transmission of malicious code, data recovery, business interruption and extortion. Review contracts with vendors and subcontractors to ensure they contain provisions that impose security standards, restrictions on data storage and transfer, breach reporting, and provide you with a mechanism for auditing their compliance when handling your data. ●