CYBERRISKS+LIABILITIES

IN THIS ISSUE

5 Cyber Risk Questions Every Board Should Ask

When a data breach or other cyber event occurs, the damages can be significant, often resulting in lawsuits, fines and serious financial losses. In order for organizations to truly protect themselves from cyber risks, corporate boards must play an active role. Not only does involvement from leadership improve cyber security, it can also reduce liability for board members.

To help oversee their organization's cyber risk management, boards should ask the following questions:

1. **Does the organization utilize technology to prevent data breaches?** Boards should ensure that the management team reviews company technology at least annually, ensuring that cyber security tools are current and effective.
2. **Does the organization have a comprehensive cyber security program that includes specific policies and procedures?** Boards should ensure that cyber security programs align with industry standards and are audited on a regular basis to ensure effectiveness and internal compliance.
3. **Has the management team provided adequate employee training to ensure sensitive data is handled correctly?** Boards can help oversee the process of making training programs that foster cyber awareness.
4. **Has management taken appropriate steps to reduce cyber risks when working with third parties?** Boards should work with the company's management team to create a third-party agreement that identifies how the vendor will protect sensitive data, whether the vendor will subcontract services and how it will inform the organization of compromised data.
5. **Has the organization conducted a thorough risk assessment and considered purchasing cyber liability insurance?** Boards, alongside the company's management team, should conduct a cyber risk assessment and identify potential gaps. From there, organizations can work with their insurance broker to customize a policy that meets their specific needs.

Contact Tooher Ferraris Insurance Group to learn more about cyber risk mitigation strategies that you can start using today to keep your business secure.

Yahoo Says All Accounts Were Hacked in 2013

Yahoo recently announced that, in contrast to an earlier estimate, all 3 billion of its accounts were hacked in 2013. The news could not only increase the legal exposure for Yahoo's new owner Verizon Wireless, but also increase the number of class-action lawsuits expected in U.S. federal and state courts.

Recently obtained information shows that the stolen information did not include passwords in clear text, bank account information or card data. However, this information was protected with outdated encryption that experts said is easy to crack. It also included backup email addresses and security questions that could make it easier to break into other user accounts.

In late 2016, Yahoo made users change their passwords if they hadn't since the hack, and invalidated old security questions and answers.

Equifax Cyber Security Incident

Equifax Inc. announced in September that about 143 million U.S. consumers may have been affected by one of the largest breaches in history.

Names, Social Security numbers, birthdates, addresses and driver's license numbers were accessed by the intruders, according to a statement from Equifax. Credit card numbers for about 209,000 consumers were also accessed.

GDPR Compliance Deadline Approaching

The General Data Protection Regulation (GDPR) requires businesses to protect the personal data and privacy of European Union (EU) citizens for transactions that occur within EU member states. Noncompliance could be costly for businesses—amounting to up to €20 million or 4 percent of global annual turnover, whichever is higher.

Companies that do business with customers in the EU must be able to show compliance by May 25, 2018. For more information on whether the GDPR affects your business, and how to comply, visit the website of the European Commission here.

Key Considerations When Buying Cyber Insurance

Buying cyber insurance is not a one-size-fits-all process. To ensure your business has sufficient cyber coverage, it is critical to assess your needs and consider your specific risks. The following are some common elements of cyber insurance policies to consider when building optimal coverage for your business:

- **Limits and sublimits**—Tooher Ferraris Insurance Group can assist you in determining appropriate limits by utilizing industry benchmarking data and projected breach costs. From there, we can examine your sublimits, which don't provide extra coverage, but set a maximum to cover a specific loss.
- **Retroactive coverage**—Breaches can go undiscovered for years. For protection from unidentified cyber incidents, ask for a retroactive date that is earlier than the policy's inception date.
- **Exclusions**—Common cyber policy exclusions, such as outdated software, unencrypted mobile devices and penalties from credit issuers, can adversely impact coverage. Understand your policy exclusions before committing.
- **Panel provisions**—Many insurance companies require policyholders to use preapproved investigators, consultants and legal professionals in the event of a cyber breach. If you have a preferred team of experts, make sure your preferred policy allows you to work with them before signing.
- **Consent provisions**—Some cyber policies contain consent provisions that require obtaining the insurer's consent before incurring certain expenses related to cyber claims. If prior consent provisions are included in the policy and cannot be removed, policyholders can change them to ensure that the carrier's consent cannot be unreasonably withheld.
- **Vendor acts and omissions**—Most organizations use third-party vendors to process or store a portion of their data. While they make it easier to do business, they also represent a potential exposure. It is critical that your business's cyber liability policy covers claims that result from breaches caused by your vendors.

Cyber insurance is continually evolving alongside emerging cyber threats. Contact Tooher Ferraris Insurance Group to help proactively assess your risks and ensure that your insurance coverage is in line with your specific business practices and exposures.

Tooher Ferraris Insurance Group
43 Danbury Road
Wilton, CT 06897
203.834.5900
www.toofer.com