Third Quarter 2023

Cyber Risks & Liabilities

Provided by: Winters-Oliver Insurance Agency

The Role of Cybersecurity in Corporate Governance

As cyberattacks become more widespread and destructive, stakeholders are increasingly motivated to hold businesses accountable for poor digital security controls, response protocols and recovery measures. However, this poses increased litigation concerns and associated expenses.

The latest industry findings show that data breach class action lawsuits have jumped by 44% since 2020. With litigation issues on the rise, companies' senior leaders are pushed to have more conversations regarding digital threats in the boardroom, making cybersecurity a critical element in the arena of corporate governance.

Going forward, companies that fail to make sure their senior leaders have a solid grasp of cybersecurity and do not encourage these leaders to be actively involved in related initiatives could be more vulnerable to lawsuits and additional losses following cyber incidents. As such, businesses should ensure their senior leaders can answer these key questions:

- Does the company utilize software or other technology to prevent cyberattacks?
- Has the board designated certain senior leaders to be responsible for companywide cybersecurity awareness and compliance?
- Does the company have comprehensive cybersecurity procedures (including a cyber incident response plan) in place?
- Has the board set a cybersecurity budget (and does this budget include insurance)?
- Does the company have cybersecurity measures specifically aimed at minimizing data breaches and third-party exposures?
- Does the board conduct ongoing cyber risk management assessments and stay up to date on the latest digital threats?

Contact us for more cybersecurity solutions.

WINTERS-OLIVER
INSURANCE AGENCY, INC.

Cyber Insurance Market Demonstrates Signs of Growth

Even amid unfavorable market conditions (e.g., steep rate hikes, additional underwriting scrutiny and various policy restrictions), the cyber insurance space experienced record-setting growth over the last few years by nearly tripling in size and outpacing all other lines of commercial coverage, according to industry research. In fact, credit rating agency AM Best reported that direct premiums written in the segment surged by 50% to $7.2 billion during 2022, while standalone cyber coverage jumped by 62%.

Such growth is likely due to increasing cyberthreats and associated losses impacting businesses across industry lines, thus fueling demand for coverage. Furthermore, many businesses now have no choice but to purchase cyber insurance in light of numerous state laws and industry standards mandating such coverage.

However, as the market expands and premium pricing starts to moderate, it's important for businesses to note that most cyber insurers have remained cautious when it comes to taking on greater risk, sticking to strict underwriting measures and upholding certain coverage restrictions. With this in mind, businesses should continue to prioritize effective cyber risk management measures and clearly document related policies and procedures for their insurers.

Contact us today for further cyber insurance developments.

Tips for Protecting Against Weaponized AI Technology

The past few years have seen artificial intelligence (AI) surge in popularity among both businesses and individuals. While this technology can certainly offer benefits in the realm of cybersecurity, it also has the potential to be weaponized by cybercriminals. In particular, cybercriminals have begun leveraging AI technology to seek out their targets more easily, launch attacks at greater speeds and in larger volumes, and wreak further havoc amid these attacks. Some of the most common activities cybercriminals have conducted with this technology include creating and distributing malware, cracking credentials, deploying social engineering scams, identifying digital vulnerabilities and analyzing stolen data.

Considering these emerging weaponization concerns, businesses should implement the following measures to mitigate their risk of experiencing cyberattacks and associated losses from AI technology:

- **Uphold proper cyber hygiene**. Such hygiene refers to habitual practices that promote the safe handling of critical workplace information and connected devices. These practices can help keep networks and data protected from various AI-driven cyberthreats.
- **Engage in network monitoring.** This form of monitoring pertains to businesses utilizing automated technology to continuously scan their digital ecosystems for possible weaknesses or suspicious activities, allowing them to detect and respond to cyber incidents as quickly as possible. Since time is of the essence when handling AI-related threats, network monitoring is a vital practice.
- **Have a plan.** Creating cyber incident response plans can help businesses ensure they have necessary protocols in place when cyberattacks occur, thus keeping related damages at a minimum. These plans should be well documented and practiced regularly.
- **Purchase coverage.** It's imperative for businesses to secure adequate insurance and financially safeguard themselves from losses that may arise from AI technology. It's best for businesses to consult trusted insurance professionals to discuss specific coverage needs.

Contact us today for additional risk management and insurance guidance.