U.S. Risk, LLC

CISOs and D&O INSURANCE

Many companies don't consider the Chief Information Security Officer (CISO) a corporate officer as they would a CEO, CFO or COO. This means they're typically not covered under the organization's D&O policy.

When a CISO isn't covered, and a breach occurs, they can be personally liable under rules recently implemented by the SEC. Adding CISOs to the company's D&O policy is an important part of an organization's risk management strategy.

› Increasing Liability

Cybersecurity-related lawsuits are nothing new. But including security officers as named defendants is a fast-growing concern.

- Late last year, the SEC charged SolarWinds and its CISO for alleged securities violations stemming from accusations that both misled investors about the cybersecurity practices and known risks before, during, and after a major cyberattack four years earlier. This marks the first time the SEC has ever charged a CISO in this manner. While the majority of the charges were recently dismissed, the complaint shows CISO's are definitely vulnerable.
- In 2022, Uber's former chief security officer was convicted of covering up a ransomware attack while the company was under investigation by the FTC.

A cyber policy would typically not respond to these types of claims as they're intended to cover events such as loss or theft of data, not SEC enforcement actions. A company's D&O policy is what's most likely to respond on behalf of a CISO.

D&O insurance offers legal defense and indemnity coverage, allowing CISOs to focus on the responsibilities of their role without constantly worrying they'll be ruined financially. Additionally, having D&O coverage in place can provide a competitive advantage in recruiting top cybersecurity talent, as it demonstrates a company's dedication to protecting all its executives.

› Adding CISOs to D&O Policies

A recent survey reported that 38% of CISOs are not covered by their company's D&O policy. With increased frequency and sophistication of cyberattacks combined with rigid regulatory requirements, scrutiny of CISOs activities will continue to grow. An intensified focus on corporate governance and cybersecurity policies from a wide range of regulatory bodies makes it even more important for CISOs to be ready for legal challenges.

Steps to take include:

- Providing the CISO with a personal indemnification agreement. This can be done by an amendment to the by-laws or by a separate indemnification agreement.
- Making sure the CISO is covered by the company's D&O insurance This can be done through endorsement.
- Limiting exclusions for criminal or deliberately fraudulent activities in the D&O policy such as by "final adjudication" requirements.
- Looking for cyber-specific exclusions in the D&O policy. In fact, reviewing all of the company's insurance programs for cyber-related gaps can be beneficial as some policies may have broad exclusions for claims arising from cyber incidents.

Sample Endorsement to D&O Policy

It is understood and agreed that the first paragraph of definition P, Insured Person in Section II, Definitions is amended to also include any past, present, or future natural person executive or employee of the Company who oversees such Company's information technology, cyber security, data privacy and/or technology security, infrastructure, and storage, including but not limited to such individuals with the title of Chief Information Officer, Chief Information Security Officer, Chief Technology (or Technical) Officer, Data Protection Officer, Privacy Officer, or such functionally equivalent position.

THE BOTTOM LINE

Today's cyber threats continue to grow and evolve with insurers holding companies accountable for their cybersecurity programs and controls. A trusted expert highly experienced in cyber policy wording as well as D&O insurance and how to customize policy terms needs to be brought into the process as early as possible to help clients assess their exposure in this fast-changing arena and ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.