SECURITY EXECUTIVES

Safeguarding the CISO: Executive Liability Protections in an Era of Cyber Accountability

As CISOs face increasing scrutiny from regulators and stakeholders, understanding the legal, governance, and insurance protections available to them has never been more crucial. This guide explores the evolving fiduciary duties, indemnification rights, and D&O coverage that every CISO and organization should be aware of.

Sanjiv Tata

Nov. 7, 2025

Key Highlights

- **CISOs should understand their fiduciary duties of care and loyalty**, and document their actions to demonstrate good-faith efforts in protecting data assets.
- **Clarifying organizational protections, including indemnification and D&O insurance**, is crucial for CISOs to mitigate personal liability risks.
- **Effective governance structures and regular risk monitoring can help prevent liabilities** and demonstrate compliance with evolving cybersecurity expectations.
- **D&O insurance provides vital coverage for CISOs**, protecting personal assets and covering legal defense costs in case of litigation.

Promotion to the position of Chief Information Security Officer represents a career pinnacle for many cybersecurity professionals. That said, individuals who face such a promotion should carefully consider the increased responsibility that comes with this role, as becoming a CISO truly places one's decision-making under a microscope. The comments and decisions that a CISO makes while serving in their role can expose their organization and themselves to liability, particularly those that may result in injuries to the organization, shareholders, employees, customers, or other affected parties.

However, protections are available from both a governance and an insurance perspective, should the CISO's executive decision-making be called into question. Critically, individuals are not alone in protecting themselves and limiting their liability – indeed, well-governed organizations will institute protections for their executives as a matter of policy.

For an organization, protecting a CISO from personal liability risk is not limited to maintaining adequate indemnification and insurance policies, but also includes having effective governance structures in place to ensure that decisions are made and documented in a way that limits potential risk from occurring in the first place. Accordingly, both CISOs and the organizations they serve should carefully consider the liability concerns that a CISO role may present and examine methods to mitigate these concerns.

The Executive Nomenclature Conundrum

Oftentimes, executives do not know if they are afforded protection by their organization until they are enmeshed in a lawsuit. The CISO role has increasingly come under scrutiny from various regulatory authorities, including the SEC, for its responsibility in handling cybersecurity breaches, in some cases, even being named in litigation.

And yet, because there is no market standard on organizational leveling, reporting structure, or scope, the CISO is not always regarded as a corporate officer by the company, and therefore may not be fully indemnified and protected by the organization. Unlike positions such as General Counsel or Chief Financial Officer, the CISO role exists in a gray area, where some organizations may consider it a high-level executive position. In contrast, others view it as a firmly operational role.

Given the ongoing evolution of the CISO role, there is no immediate guarantee that a CISO will be considered an executive and, consequently, will be afforded the same protections as other executive officers. Accordingly, a CISO must determine whether they are entitled to the same insurance coverage as other executives, including that provided under the relevant directors and officers ("D&O") insurance policy. CISOs should not assume that they would receive the same indemnification protections that other executive officers may be afforded under relevant insurance policies and, further, should be aware that liability from cyber & privacy exposures is excluded by D&O policies.

> *"Given the ongoing evolution of the CISO role, there is no immediate guarantee that a CISO will be considered an executive and, consequently, will be afforded the same protections as other executive officers."*

Therefore, for both the organization and the incoming CISO, it is imperative to clarify with legal counsel which protections CISOs are provided with, and how (or if) they are covered with D&O insurance.

Fiduciary Duties: The Principal Duties of Executives

CISOs should begin by understanding their principal fiduciary duties. Most jurisdictions require these duties to be adhered to for any protection to be active. The specific two fiduciary duties executives owe to the company and its shareholders are the duty of care and the duty of loyalty, and potential nonadherence to these duties could be used as a basis for liability.

For CISOs, there is a growing argument that they are responsible for the proper protection of data assets within their organization and should therefore be expected to show appropriate fiduciary duty. Failure to do so could result in legal action against both the individual and the

company. However, there is an important caveat which CISOs should bear in mind – their fiduciary duties require them to, in good faith, try their best to provide proper protection of data assets, but they are not required to be omniscient. That is, provided a CISO has in good faith used their utmost ability to protect data assets adequately, even if a failure occurs, such an individual may not be liable for breaching their fiduciary duties.

Accordingly, CISOs should:

1. Identify the most critical cyber risks facing their company and establish a monitoring system that provides the board with timely information about these risks.
    a. This could include using third-party risk management tools or attack surface management tools.

2. Once the oversight system is established, pay attention and take corrective actions, as needed, such as conducting regular pen testing.

3. Construct an expansive documentation system – recording even minor actions could be the difference in proving good-faith compliance with fiduciary duties.

I would like to point out that interpretations of fiduciary duties can change as expectations for CISOs change. Historically, enacting proper controls to fix a cybersecurity incident was considered sufficient for CISOs to limit personal liability. However, following the SEC case against SolarWinds in 2023, CISOs are increasingly expected to have implemented sufficiently stringent security measures to prevent an attack before it occurs and to provide proactive reporting to the board about cyber vulnerabilities.

What is Indemnification

While fiduciary duty is the foundation upon which proper corporate governance is built, indemnification is the key protection for CISOs. Essentially, an agreement by the CISO's organization to cover costs, losses, and expenses in issues where a CISO's decision-making may be challenged, indemnification is a key protection for any CISO.

Indemnification protections are typically outlined in a company's bylaws and operating agreements and can vary in terms of their scope and coverage. However, these documents often contain expansive language that is open to interpretation. Therefore, CISOs should consult with their legal counsel to understand how indemnification works within their organization and to thoroughly review the details of their corporate bylaws immediately upon assuming the CISO position.

The evolving responsibilities executives face can put them at risk of litigation, even in cases where they may not be aware of this potential. The protection afforded to them by their organization can be the difference between having the entire organization defend them in a lawsuit or needing to protect themselves with their own personal assets.

D&O Insurance

Sometimes, even if CISOs and an organization are diligent in their duties, they may still face litigation and be required to cover the costs of defense. D&O insurance is a vital resource for executives and organizations to protect themselves in the event of such situations.

"Sometimes, even if CISOs and an organization are diligent in their duties, they may still face litigation and be required to cover the costs of defense."

Most organizations purchase D&O insurance, which, as a general matter, protects an organization's executive officers in many suits where they are sued in their capacity as executives. The key element to note for these policies is whether a potential suit involves an individual being sued themselves or in their capacity as an executive officer of an organization. D&O policies only offer protection in the latter circumstance.

D&O insurance can be sold either as a standalone policy or bundled with other types of insurance into a comprehensive corporate insurance package. This insurance will protect CISOs in two ways: it will safeguard their personal assets and protect the company's balance sheet. There are three primary D&O coverages:

- Side A Coverage: Personal Coverage - This is the coverage that kicks in when a CISO's organization can't (or won't) cover you. Examples include bankruptcy scenarios or certain derivative lawsuits in which the organization is barred from providing you with protection.
- Side B Coverage: Company Reimbursement – In circumstances where a CISO's organization does provide indemnification protection for the CISO, Side B coverage provides reimbursement to the organization itself for that coverage.
- Side C Coverage: Corporate Defense – Coverage here is provided to the organization itself directly, although this type of coverage can vary significantly depending on whether the organization is a public or private company.

The 2018 data breach announcement by Marriott provides an example where executives were protected because they were able to demonstrate their fiduciary duties were met and were therefore able to use the company's D&O policies to fund court proceedings. The judge dismissed both the securities suit and the derivative suit, as Marriott had provided disclosures showing that it believed proper cybersecurity measures were necessary, had highlighted potential risks within its cybersecurity infrastructure, and had outlined steps being taken to address those risks.

Beyond the non-indemnifiable actions listed above, executives may still be held personally liable for certain losses, particularly in cases of notably egregious conduct. The infamous Enron scandal provides a clear example: Enron's D&O policy limits would have been sufficient to cover the suits brought against its executives; however, the courts ruled that they should be held personally liable for the improper decisions they made, given the magnitude of the offense.

Selecting the right D&O insurance policy and ensuring its proper coverage is extremely important for executive (and organizational) peace of mind. It may be the only tool protecting an executive's personal assets from being seized to cover the costs of litigation.

Executive Liability Protection – The Key to Peace of Mind

The ever-changing responsibilities of CISOs can put them at risk of litigation, even in cases where they might not be aware. Knowledge of the protections afforded to them by their organization can be the difference between having the protection of their company in a suit or being forced to defend themselves via personal assets.

Note: Sanjiv Tata of Paul Hastings LLP acknowledges the supporting contribution from Halyna Vasylevska of Munich Re Ventures.

About the Author

Sanjiv Tata

PARTNER IN THE INSURANCE M&A PRACTICE AT PAUL HASTINGS

Sanjiv Tata is a partner in the Insurance M&A practice at Paul Hastings and is based in the firm's New York office. Sanjiv advises insurance companies, insurance intermediaries, and investment companies on a broad range of insurance regulatory and corporate matters, including the formation and licensing of insurance companies, mergers and acquisitions of insurance companies, reinsurance transactions, and enforcement, corporate governance, cybersecurity, enterprise risk, and general compliance matters.

Sanjiv regularly represents clients before state insurance regulatory authorities and has experience negotiating directly with nearly every insurance regulatory authority in the United States.

Sanjiv's experience also includes advising mutual insurers on regulatory aspects related to demutualization and mutual holding company transactions. Before joining Paul Hastings, Sanjiv was a partner at another international law firm, focusing on insurance regulatory work.

Show less

Reprinted with permission from SecurityInfoWatch.com.