AIG Statement Series℠ CISO Side A Liability Insurance

Chief information security officers (CISOs) and other technology officers are facing heightened scrutiny for actions and decisions made in their roles overseeing cybersecurity, technology, and data privacy operations. In addition to shareholder class actions and derivative lawsuits, which may name CISOs and other executives in addition to the company itself, recent enforcement actions by the Securities and Exchange Commission (SEC) and Department of Justice (DOJ) have sought to hold CISOs liable for their companies' cybersecurity and privacy failures. Meanwhile, many CISOs may not be covered by traditional directors and officers (D&O) Side A policies, leaving them unprotected and personally liable.

AIG Statement CISO Side A coverage provides a unique solution for this increasing exposure to help financially protect CISOs when they face regulatory or shareholder action.

Claims for management liability exposures connected to CISOs' activities are often excluded under security and privacy liability policies. D&O policies and their Side A insuring clauses typically cover these claims, however they often limit coverage to "duly elected or appointed" executives. Since many CISOs aren't duly elected or appointed executives, they may only be covered for securities claims or when named alongside a duly elected or appointed executive — highlighting the need for dedicated limits with broad coverage.

Coverage Highlights

- Broad coverage for corporate data officer and data department acts, including acts alleged in management and professional capacities
- Side A difference-in-conditions (DIC) enhancements, covering loss not paid by other insurance or corporate indemnification
- Broad definition of insured loss, including affirmative coverage for insurable fines and penalties
- Advancement of loss in the event other applicable insurance coverage fails to pay
- Broad choice of counsel, with no panel counsel requirement
- Limited exclusions, only conduct and prior and pending (P&P) exclusions

Broad — and Growing — Avenues of Exposure

Securities Class Actions

CISOs and other security officers are increasingly named as defendants in securities fraud class actions, alleging false or misleading statements about their cybersecurity practices or timely disclosure of an incident led to a drop in stock prices.

Breach of Fiduciary Duty and Derivative Actions

Cybersecurity officers face increasing legal liability as shareholders file suits alleging negligent oversight of cybersecurity programs and inadequate data protection measures, resulting in harm to the company's value.

SEC Disclosure Rules

The SEC's rules impose increased obligations on companies to promptly disclose "material" cyber incidents, but these are subject to interpretation. In any event, the disclosure requirements create additional potential liability for officers, directors, and cybersecurity executives.

DOJ and Criminal Actions

The recent conviction of a cybersecurity officer marked the first criminal prosecution of an executive for their handling of a data security incident, with potential penalties including substantial fines and prison time.

Privacy and Cybersecurity Laws

Companies and their directors and officers may also face penalties under state privacy and cybersecurity laws, such as those promulgated by the New York Department of Financial Services.

Case Study: SEC Charges CISO Following Cybersecurity Breach

Recent regulatory enforcement action signals a shift toward personal accountability by directors, officers, and information technology executives for organizations' cybersecurity failings.

A provider of IT management software used by tens of thousands of private and public-sector organizations worldwide experienced a cybersecurity breach. Threat actors, believed to operate under the direction of a nation-state, exploited a vulnerability in the software company's widely used network management product — a highly efficient IT supply-chain attack that gave perpetrators access to the software company's customers. The event, one of the largest cyber attacks to date, distributed malware to nearly 20,000 of the software firm's customers.

The SEC later charged the software company and its CISO with fraud and internal control failures, alleging the company misled investors regarding its cybersecurity practices and known cyber risks. The lawsuit marked the first time the SEC charged an individual CISO.

Even though a federal district court ultimately dismissed many of the SEC's charges, it did allow claims relating to the software company's security statements to proceed. The SEC's lawsuit alleged the company made misleading statements about its access controls and password protections, and the court indicated that accurate cybersecurity disclosures were important.

Separately from the SEC action, shareholders sued the software company and several of its officers, including its CISO, following the breach. Allegations in the lawsuit included the company's security officer making false and/or misleading statements regarding the state of the software company's cybersecurity and its security practices. The company agreed to pay more than $20 million to settle the investors' class action. The software company disclosed that it received proceeds from its D&O liability insurance relating to the cyber attack, offset by the class-action settlement. The company added it expected to incur additional legal expenses from the cyber incident, which it would pay from its own funds because it had exhausted its applicable insurance policies.

The AIG Statement Series provides succinct and transparent coverages to protect companies and their executives and employees from a wide range of corporate governance and operational exposures. It embodies our commitment to offering straightforward, statement-making products that provide cutting-edge coverages and wording.

Available coverages include:

- Directors & Officers Statement
- Directors & Officers Side A Statement
- Directors & Officers CISO Side A Statement
- Directors & Officers Clawback Statement*
- Employment Practices Statement*

Contact

For more information, please visit www.aig.com/aig-statement-series or contact your local Financial Lines underwriter or AIG Distribution partner.

*Directors & Officers Clawback Statement and Employment Practices Statement are not available for purchase through AIG affiliates domiciled in the U.S.

American International Group, Inc. (AIG) is a leading global insurance organization. AIG provides insurance solutions that help businesses and individuals in more than 200 countries and jurisdictions protect their assets and manage risks through AIG operations, licenses and authorizations as well as network partners.

AIG is the marketing name for the worldwide operations of American International Group, Inc. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries and jurisdictions, and coverage is subject to underwriting requirements and actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

489-05-0425US