AN A.S. PRATT PUBLICATION
OCTOBER 2024
VOL. 10 NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 8** **October 2024**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.
LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2024 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR
Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Emilio W. Cividanes
Partner, Venable LLP

Christopher G. Cwalina
Partner, Holland & Knight LLP

Richard D. Harris
Partner, Day Pitney LLP

Jay D. Kenisberg
Senior Counsel, Rivkin Radler LLP

David C. Lashway
Partner, Sidley Austin LLP

Craig A. Newman
Partner, Patterson Belknap Webb & Tyler LLP

Alan Charles Raul
Partner, Sidley Austin LLP

Randi Singer
Partner, Weil, Gotshal & Manges LLP

John P. Tomaszewski
Senior Counsel, Seyfarth Shaw LLP

Todd G. Vare
Partner, Barnes & Thornburg LLP

Thomas F. Zych
Partner, Thompson Hine

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2024 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Directors and Officers Insurance for Chief Information Security Officers: A Critical Shield in an Era of Increasing Personal Risk

By Geoffrey B. Fehling*

In this article, the author explains why chief information security officers need robust directors and officers liability insurance tailored to cybersecurity executives.

Recent high-profile cases involving chief information security officers (CISOs) have spotlighted the need for robust directors and officers (D&O) liability insurance tailored to cybersecurity executives.

In 2022, Uber's former CISO, Joe Sullivan, was sentenced to three years of probation and fined $50,000 after being found guilty of two felonies. Sullivan was found to have obstructed an FTC investigation by disguising the nature of payments made to hackers who had breached the company in 2016. Uber had paid $148 million to resolving similar cover-up allegations and many expected Sullivan to be acquitted, but the conviction was a wake up call for the potential exposure that CISOs face in the aftermath of a cyber incident.

More recently, a highly-anticipated ruling dismissed a substantial portion of the SEC's case against SolarWinds alleging that the company touted misleading cybersecurity practices and products and mislead investors about being targeted in a number of widely-reported cyber attacks. But the lawsuit also named the company's CISO, Timothy Brown, as a primary violator and aider and abettor of the charges. Not all of those charges were dismissed, as the court allowed the claims against Brown based on allegations of his knowledge of false public statements about the company's cybersecurity practices to proceed.

THE ESSENTIAL BACKSTOP OF D&O LIABILITY INSURANCE

Both cases underscore the growing personal liability risks faced by security leaders. The SEC's aggressive approach to cybersecurity enforcement has led to renewed discussion of appropriate internal account controls, disclosure controls and procedures, and potential securities fraud claims based on public disclosures.

All of that is geared towards more robust compliance and mitigation of enforcement risks in the first instance, but recent case studies have left boards, executives, and in

* The author, a partner in Hunton Andrews Kurth LLP, may be contacted at gfehling@huntonak.com.

particular CISOs wondering how to best protect themselves if a claim does occur notwithstanding the company's rigorous controls. One critical protection is building a liability insurance programs to protect against claims arising from cyber incidents. Guarding against cyber exposures ordinarily starts with analysis of cyber insurance policies, but as the costs to combat cyber incidents continue to climb, those cyber policies may be exhausted long before any follow-on securities lawsuits, investigations, or enforcement actions implicating CISOs and other key decision makers.

Understanding and improving all coverages beyond cyber, especially D&O coverage geared at protecting the personal assets of individuals like CISOs, can help increase recovery and avoid surprises in the event of a claim. Here are some of the key D&O insurance considerations for policyholders to consider:

1. *Increasing Liability*: The SolarWinds SEC case shows increasing regulatory risks for individuals, while the Uber CISO felony conviction for obstruction of justice highlights potential criminal liability for CISOs. The cost of cybersecurity events can be staggering ($9.48 million on average in the United States),[1] often eroding if not exhausting cyber policy limits in the immediate aftermath of an incident, leaving policyholders to look to other policies to provide coverage for follow-on claims by regulators, customers, and other litigants.

   That is why reviewing programs as a whole to ensure complementary coverages – like D&O, tech E&O, and cyber – work together as intended and do not result in unintended gaps with mismatched coverage grants and exclusions or defined terms. Taking a holistic approach to assessing coverage can minimize risks of surprise denials.

2. *Are CISOs "Insureds"*: Historically focused on board members and C-suite executives, D&O policies may not adequately cover the unique risks CISOs face. One recent survey reported that 38% of CISOs are not covered by their company's D&O insurance policy. Depending on corporate hierarchy and governance documents, CISOs may not fit the policy's definition of "insured."

3. *Criminal v. Civil Actions*: D&O policies typically cover civil liabilities based on negligence or non-intentional conduct, but they often exclude criminal or deliberately fraudulent activities. The Uber CISO's felony conviction shows the importance of limiting those exclusions, such as by robust "final adjudication" requirements.

[1] https://www.ibm.com/reports/data-breach.

4. *Government Investigation Coverage*: Regulatory coverage varies widely based on public versus private companies and whether regulators are investigating or taking action against individuals versus the company. Policyholders Policies should request affirmative coverage and understand any limitations, like sublimits, that may reduce coverage for regulatory action prior to a formal enforcement action.

5. *Cyber Exclusions*: Some policies may have broad exclusions barring coverage for claims arising from cyber incidents, potentially leaving CISOs exposed. Eliminating those exclusions, or at least negotiating carve backs or narrower lead-in causation language can help avoid rendering D&O insurance illusory for a large segment of cyber-related claims.

6. *Corporate Indemnification*: D&O insurance presumes broad corporate indemnification unless the company is unable to do so. Similar to CISOs sometimes falling through the cracks in meeting the definition of "insured," companies also may need to reassess their indemnification agreements with CISOs to ensure alignment with available insurance coverage.

7. *Review Insurance Programs, Not Just Policies*: Cyber-related risks may fall through gaps in traditional liability policies, which increasingly have exclusions or similar limitations to shift risks into cyber policies. Despite that, many traditional policies can provide coverage for critical cyber risks. Policyholders should audit their program as a whole and not focus on single policies, especially solely the cyber policy, to assess and improve potential coverage for cyber exposures.

CONCLUSION

As personal liability risks for CISOs continue to evolve, the availability and scope of D&O insurance will remain a critical factor in recruiting and retaining top cybersecurity talent. Companies that offer robust insurance protection may gain a competitive advantage in the tight market for skilled security leaders. Policyholders should proactively engage with brokers, coverage counsel, and other risk professionals to understand the scope of existing coverage and explore options for enhanced protection that addresses these growing liability risks.