Nutter uncommon law

INSIGHTS

*"By having a dedicated person to handle all of an organization's cybersecurity needs, it creates another pathway toward a more secure orientation."*

# How to Structure Your Organization's Cybersecurity Management

### Q: WHO IN A COMPANY IS VITAL FOR CYBERSECURITY MANAGEMENT?

***SETH P. BERMAN:*** Cybersecurity is everyone's responsibility. The board and senior management must set the priorities and shape the culture, but even the lowest-level employee has to play his or her role in keeping the organization secure. Having said that, it is also crucial that the organization appoint someone in charge of this effort. In most organizations this person is either the Chief Security Officer (CSO) or the Chief Information Security Officer (CISO). This person must work closely the General Counsel (GC) to ensure that the organization's cybersecurity protocols meet its legal requirements.

### Q: WHAT IS THE RESPONSIBILITY OF THE BOARD OF DIRECTORS?

***SB:*** Boards must play a role in weighing cyber risk. This role is required of public company boards by the SEC and even non-public boards have been strongly encouraged to consider cyber risk as a part of their responsibilities by organizations and legislation such as the National Association of Corporate Directors (NACD) and the European Union's GDPR. Turning this principle into action has proven challenging for many boards of directors. At most companies, boards members lack the experience and expertise necessary to provide the appropriate level of director oversight. As a result, they need to rely on outside experts and advisors. Boards should also push management to create a role that is focused solely on cybersecurity, such as the CISO or CSO, who can work with the board and the rest of the management team to define a cyber resilience strategy.

### Q: COULD YOU OUTLINE THE ROLE OF A CISO?

***SB:*** The CISO/CSO's job is to constantly assess an organization's evolving cyber risks, develop and implement a strategy to minimize those risks, oversee the monitoring of the organization's network for signs of intrusion or exfiltration, and act as the first responder in case of a cyber incident. This role was once primarily filled by the CIO, though it is now considered best practice to separate these two roles. Designating a CISO/CSO allows organizations to better separate the day-to-day technology needs of an organization from its security hygiene.

Specifically, a dedicated CISO can ensure an organization:

- demonstrates a strong management and board commitment to security
- remains focused on creating a security culture
- conducts honest assessments to measure and improve security
- creates a roadmap for improving its security posture
- monitors its network and other vulnerabilities
- implements and maintains an incident response plan
- reacts quickly to attacks

By having a dedicated person to handle all of an organization's cybersecurity needs, it creates another pathway toward a more secure orientation.

### Q: HOW DOES THE GC FIT INTO THIS PUZZLE?

***SB:*** Before a breach occurs, the GC needs to be involved with the CISO/CSO and the board to shape the cyber risk strategy in order to ensure that it incorporates the ever-evolving legal landscape around the obligations to protect against cyber risks. When a breach occurs, the GC's role will significantly expand. Indeed, in most instances, it is wise to have the GC, rather than the CISO/CSO or CIO, lead any investigation of a potentially significant security breach. Not only does the GC's involvement better protect the organization's attorney-client privilege, letting the CISO/CSO or CIO investigate a security breach puts him or her in the untenable position of examining the (potential) failings of his or her own department, which could be a serious problem if the company ever had to defend its conduct in court.



**Seth P. Berman**

**PARTNER**
Privacy and Data Security
617.439.2338
sberman@nutter.com

*Seth P. Berman leads Nutter's Privacy and Data Security practice group and is a member of the firm's White Collar Defense practice group. Corporations and their boards engage Seth to address the legal, technical and strategic aspects of data privacy and cybersecurity risk, and to prepare for and respond to data breaches, hacking and other cyber attacks. Seth also represents clients in white collar criminal matters, and has particular expertise in conducting cross-border internal investigations and in the data privacy implications of such matters.*

**PRESS CONTACT:**
Heather Merton
Senior Communications Manager
617.439.2166
hmerton@nutter.com

Nutter is a Boston-based law firm that provides legal counsel to industry-leading companies, early stage entrepreneurs, institutions, foundations, and families, across the country and around the world. The firm's lawyers are known for their client-centric approach and extensive experience in business and finance, intellectual property, litigation, real estate and land use, labor and employment, tax, and trusts and estates. Co-founded in 1879 by Louis D. Brandeis, who later became a renowned justice of the U.S. Supreme Court, Nutter is dedicated to helping companies prosper in today's competitive business environment.