ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

4 Reasons CLOs Increasingly Take the Lead on Cybersecurity

Compliance and Ethics

Information Governance

Technology, Privacy, and eCommerce

Recent survey data confirms what many chief legal officers (CLOs) have already experienced firsthand: cybersecurity is no longer just an IT concern — it's a fundamental business risk that demands legal leadership.

In the recently released 2025 State of Cybersecurity Report from the ACC Foundation, 38 percent of participants report that the CLO holds a leadership role in cybersecurity in the organization, up from just 15 percent five years ago. That percentage jumps to 57 percent at companies in the information sector, followed by professional services (53 percent), and insurance (47 percent).

!function(){"use strict";window.addEventListener("message",(function(a){if(void 0!==a.data["datawrapper-height"]){var e=document.querySelectorAll("iframe");for(var t in a.data["datawrapper-height"])for(var r,i=0;r=e[i];i++)if(r.contentWindow===a.source){var d=a.data["datawrapper-height"][t]+"px";r.style.height=d}}))}();

Meanwhile, 50 percent of participants say that the CLO is part of a team responsible for cybersecurity at the enterprise level, and just nine percent state that the CLO has no responsibilities in this area. This trend highlights the increasing importance of the CLO's involvement in cybersecurity, reflecting a broader recognition of the legal implications of cybersecurity and the need for comprehensive governance to address these challenges effectively.

"Cybersecurity, though anchored in IT, demands a holistic approach," said Blake Garcia, ACC's senior director of research and business intelligence. "The escalating legal ramifications of breaches necessitate CLO involvement beyond consultation. These officers are now essential strategists,

ensuring that cybersecurity frameworks are not only technically sound but also legally robust, safeguarding the organization from existential legal vulnerabilities."

Download the key findings or full report on the ACC Foundation's website

The role of in-house counsel has expanded beyond compliance oversight to become a driving force in cybersecurity governance, risk mitigation, and strategic decision-making. Here are four key reasons why CLOs are increasingly leading cybersecurity efforts:

1. Rising regulatory and compliance pressures

The legal and regulatory landscape surrounding cybersecurity is more complex than ever. With evolving laws such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), SEC cybersecurity disclosure rules, and industry-specific mandates, organizations must ensure compliance while mitigating enforcement risks. CLOs are uniquely positioned to interpret these laws, align cybersecurity policies with regulatory expectations, and establish a defensible compliance framework.

2. Managing legal risk and liability exposure

Cyber incidents are no longer just operational disruptions — they can be legal crises. Data breaches trigger litigation, regulatory investigations, and reputational damage, requiring swift legal action. CLOs play a critical role in incident response planning, breach notification strategies, and contract negotiations to limit liability. By embedding cybersecurity risk into broader corporate risk management, CLOs help ensure the organization is legally protected before, during, and after an incident.

ACC Members: Download the exclusive Cybersecurity Toolkit for In-house Lawyers

3. Increasing board and executive oversight

Cybersecurity has become a boardroom priority, with directors and executives demanding stronger governance and transparency. CLOs, as trusted advisors to the board, are stepping in to bridge the gap between legal, risk, and technical teams. Leading cybersecurity efforts allows CLOs to ensure the company's strategy aligns with investor expectations, regulatory scrutiny, and best practices in corporate governance.

Learn more about the importance of the CLO's Seat at the Table.

4. Cybersecurity as a cross-disciplinary business risk

Unlike traditional IT issues, cybersecurity risks extend across legal, compliance, HR, public relations, and finance. CLOs already operate at this intersection, making them well-suited to lead a cross-functional approach to cybersecurity. From negotiating vendor agreements with stronger cybersecurity provisions to training employees on legal risks related to phishing or data security, CLOs bring a holistic, enterprise-wide perspective to cybersecurity leadership.

Visit ACC's Privacy and Cybersecurity Resource Center

In-house counsel as a strategic cybersecurity leaders

As organizations recognize cybersecurity as a legal and business imperative, CLOs are stepping into leadership roles that go far beyond legal compliance. Whether influencing board-level strategy, strengthening legal protections, or guiding cross-functional collaboration, today's CLO is an essential architect of cybersecurity resilience.

"Despite IT's core role in cybersecurity, CLOs are now strategic linchpins, their legal risk expertise decisively shaping organizational defenses in a world where breaches carry unprecedented legal consequences," Garcia said.

Download the 2025 State of Cybersecurity Report: An In-house Perspective today.

Join ACC today for more cybersecurity resources!

Staff

ACC