2025

_state of CYBERSECURITY REPORT

ACC Foundation
Association of Corporate Counsel

_key(findings):

01

The Strategic Influence of CLOs in Cybersecurity Continues to Expand

The Chief Legal Officer (CLO) is transitioning into a more central cybersecurity leadership role. They are increasingly integrated into cybersecurity teams, holding leadership positions, and frequently reporting to boards on cyber matters. This shift signifies the rising importance of legal and governance considerations in cybersecurity, necessitating CLO expertise in incident response, strategic planning, and effective board communication.

02

One-Third of Legal Departments Now Have a Dedicated In-house Cybersecurity Lawyer

Legal departments are responding to the escalating cybersecurity landscape by significantly expanding their in-house cyber expertise. There is a notable increase in departments with dedicated cyber law specialists, and a growing trend towards hiring internal cyber counsel. Furthermore, these positions are increasingly being elevated to senior executive levels, highlighting the strategic importance of legal cybersecurity guidance.

03

Top Breach Concerns: Reputation, Liability, and Business Continuity

Businesses are seeing a significant evolution in their cybersecurity concerns. While reputational damage remains a primary worry, the focus is expanding. Notably, liability to data subjects and threats to business continuity have risen sharply, indicating a growing awareness of the tangible legal and operational risks associated with breaches.

04

Nearly All Organizations Now Require Mandatory Cybersecurity Training for All Employees

Organizations are demonstrating a clear and substantial commitment to bolstering employee cybersecurity awareness through training. Mandatory cybersecurity training has become almost universal, with a dramatic increase in adoption. Furthermore, the frequency of these training sessions has also significantly risen.

05

Key Company Policies Focus on Data Security and Emerging Technology

Organizations are placing a heightened emphasis on establishing and maintaining robust internal cybersecurity policies. Core policies like document retention, acceptable use, and password security remain prevalent. Growing adoption of BYOD ("Bring Your Own Device") and the rapid emergence of AI policies signal a proactive approach to evolving tech and work styles.

06

Legal Teams Are Gaining Confidence in Vendor Cybersecurity as Evaluation Practices Improve

Legal teams are showing a gradual increase in confidence regarding their vendors' cybersecurity capabilities. This improvement is accompanied by a significant rise in organizations actively evaluating their vendors' security practices. This evaluation is becoming more rigorous, with increased use of detailed questionnaires and demands for proof of cybersecurity certifications.

07

Legal Departments Are Playing an Increasingly Active Role in Third-Party Risk Management

Legal departments are experiencing a noticeable expansion in their responsibilities within third-party risk management. There is a clear upward trend in their active participation, with a larger proportion of legal teams being "often involved" and a marginal increase in those "sometimes involved." Notably, the number of legal departments that "never" engage in third-party risk management has significantly decreased.

QUESTIONS? CONTACT: research@acc.com **VIEW THE FULL REPORT: acc.com/cyber2025**

ACC Foundation
Association of Corporate Counsel

ACC Headquarters Office
1001 G St., NW, Suite 300W | Washington, DC 20001 USA
Tel +1 202.293.4103 | acc-foundation.com