

HOW CHIEF LEGAL OFFICERS CAN LEAD ON CORPORATE DATA SECURITY

CONTENTS

- CLOs Are At Forefront of Data Risk Management Despite Formidable Challenges
- Compliance Ambiguity is Eroding CLOs' Confidence, Hindering Proactive Risk Mitigation
- 10 Ways CLOs Can Lead on Corporate Data Security

It has now become commonplace for Chief Legal Officers (CLOs) to juggle myriad responsibilities. While this reflects heightened organizational awareness regarding risk, it also thrusts CLOs into unfamiliar territory. With data security increasingly assuming critical importance, the absence of robust data management strategies in nearly half of organizations exacerbates this dilemma. Despite efforts by many CLOs to implement tactics to stay on top of compliance obligations, a surprising fraction of CLOs have done nothing to prepare for these requirements with respect to data security. Compounded by ever-changing and overly complex regulatory obligations, CLOs are becoming less confident in their ability to combat emerging data threats.

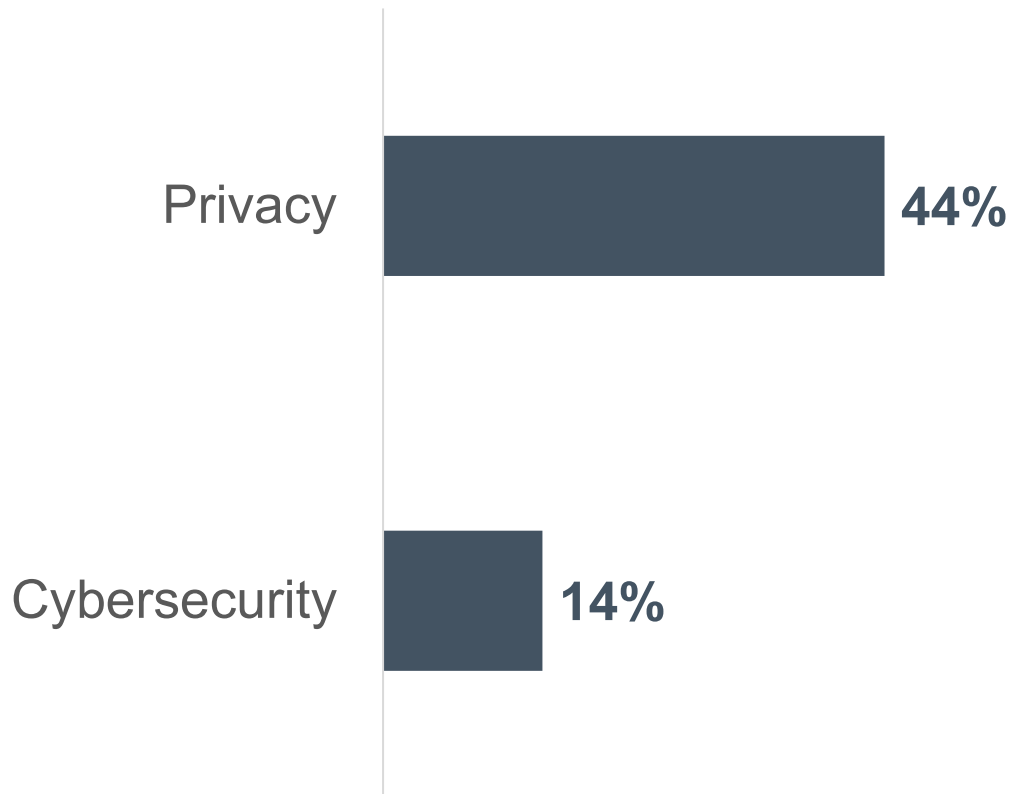
To bolster their efficacy, we offer ten actionable strategies empowering CLOs to lead with confidence in navigating corporate data security challenges, supported by key ACC legal resources.

All data cited in this report is sourced from the [2024 ACC Chief Legal Officers Survey](#).

CLOs ARE AT FOREFRONT OF DATA RISK MANAGEMENT DESPITE FORMIDABLE CHALLENGES

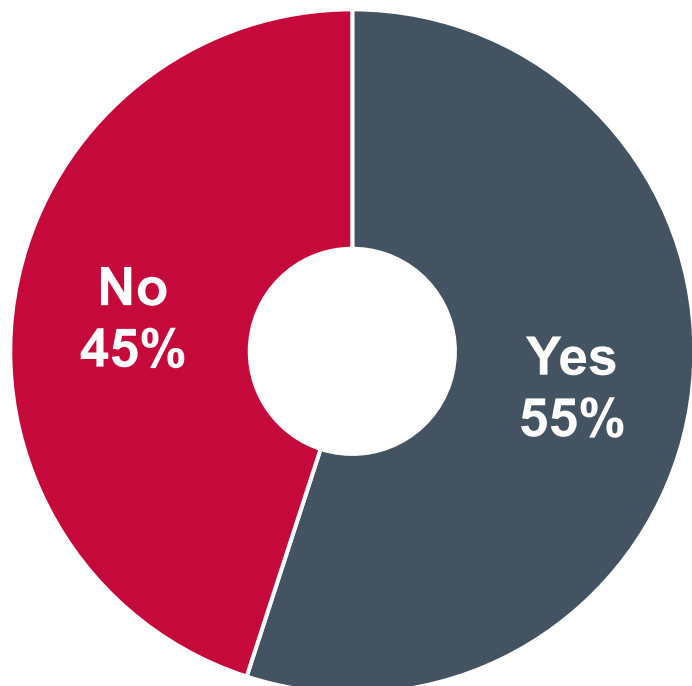


CLO BUSINESS FUNCTION OVERSIGHT



58 Percent of CLOs are now overseeing three or more business functions beyond legal, and 27 percent oversee five or more. These often include areas such as ethics and risk, but are now including privacy with 44 percent and 14 percent of CLOs are now overseeing the cybersecurity function for their organization. This is a clear indication that businesses are becoming more attuned to the significant risks that their data assets pose and are reaching to their top lawyer for guidance and oversight.

ORGANIZATIONS WITH A COMPREHENSIVE DATA MANAGEMENT STRATEGY



Despite this increased awareness of and sensitivity to data risks, nearly half of CLOs are finding that their organization has no comprehensive data management strategy and are facing an uphill battle to inventory and understand the vast array of data that their organization possesses.

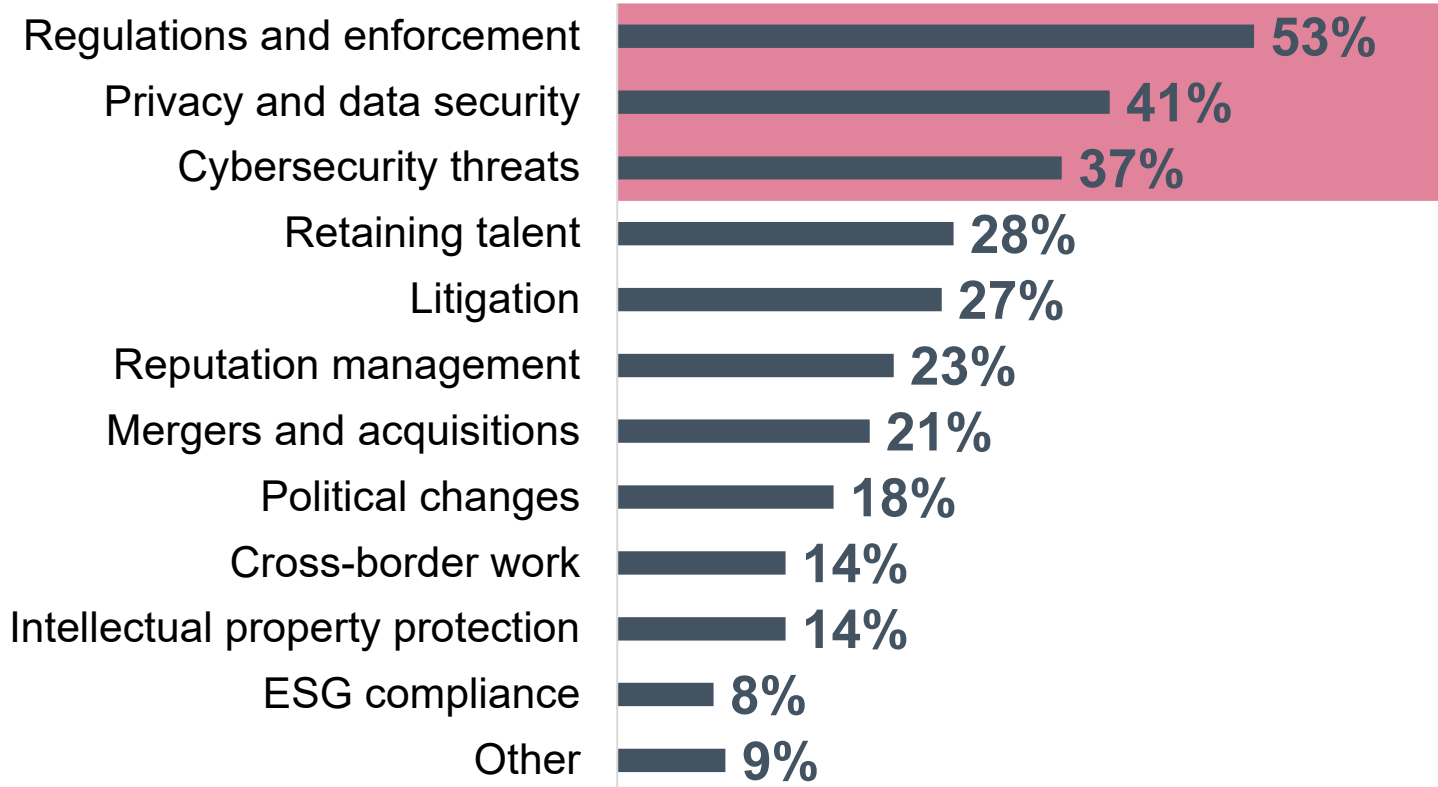
CONFIDENCE IN ORGANIZATION'S ABILITY TO CONSISTENTLY RESPOND TO CYBERSECURITY INCIDENTS AND DATA BREACHES



■ Very confident ■ Moderately confident ■ Somewhat confident ■ Only slightly confident ■ Not at all confident

Given the lack of strategy around data security at many organizations, the bulk of CLOs are only “moderately” or “somewhat confident” in their ability to respond to cyber incidents and data breaches. One in five CLOs are only slightly or not at all confident.

ISSUES KEEPING CLOs UP AT NIGHT



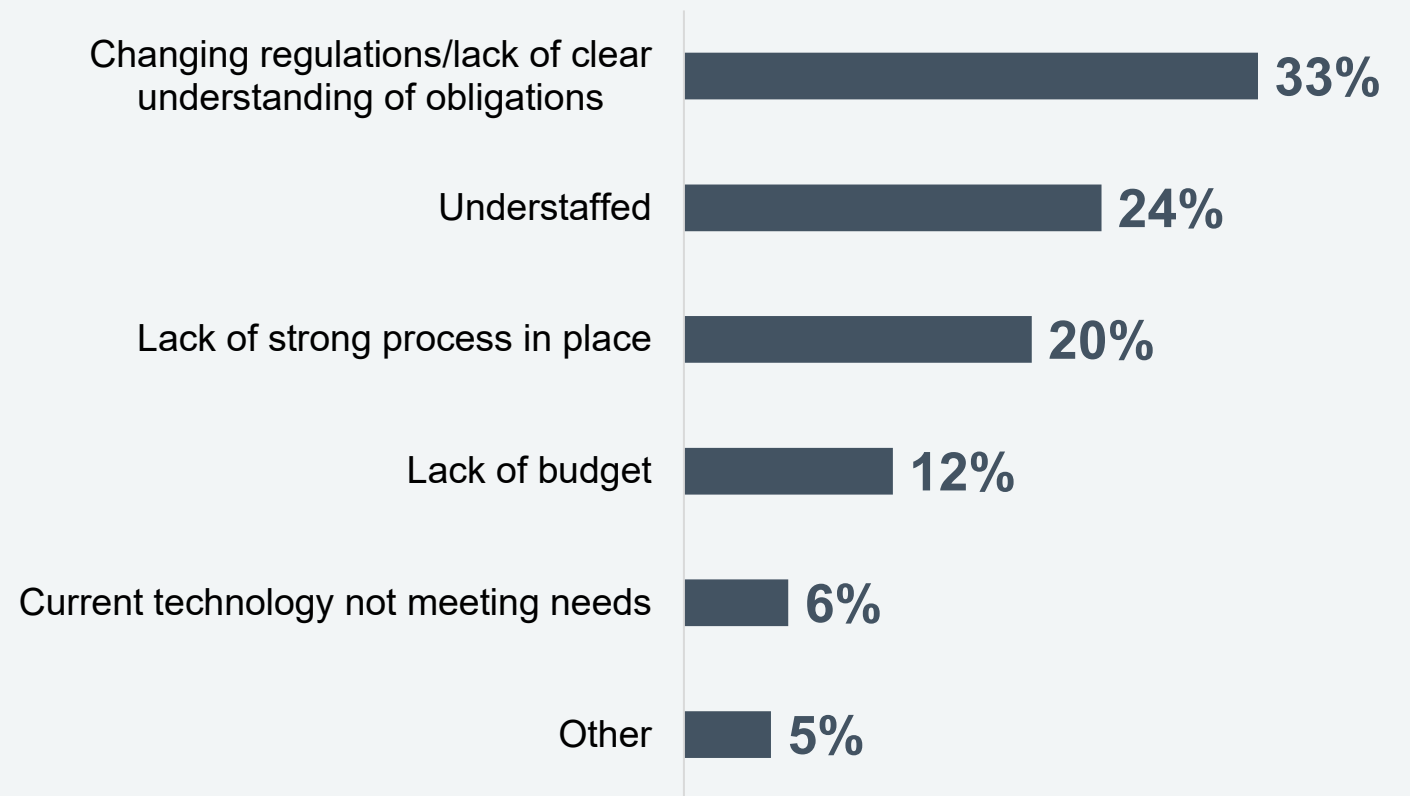
It is no surprise that the most pressing issues CLOs are grappling with currently are privacy, data security, cyber threats, and increasingly complex regulations, as well as concern about the harsher penalties for non-compliance.

**COMPLIANCE
AMBIGUITY IS ERODING
CLOs' CONFIDENCE,
HINDERING PROACTIVE
RISK MITIGATION**



When asked about the barriers preventing more effective responses to their data-related compliance obligations, CLOs primarily cited a lack of clarity around those obligations, in addition to being understaffed and lacking processes and budget.

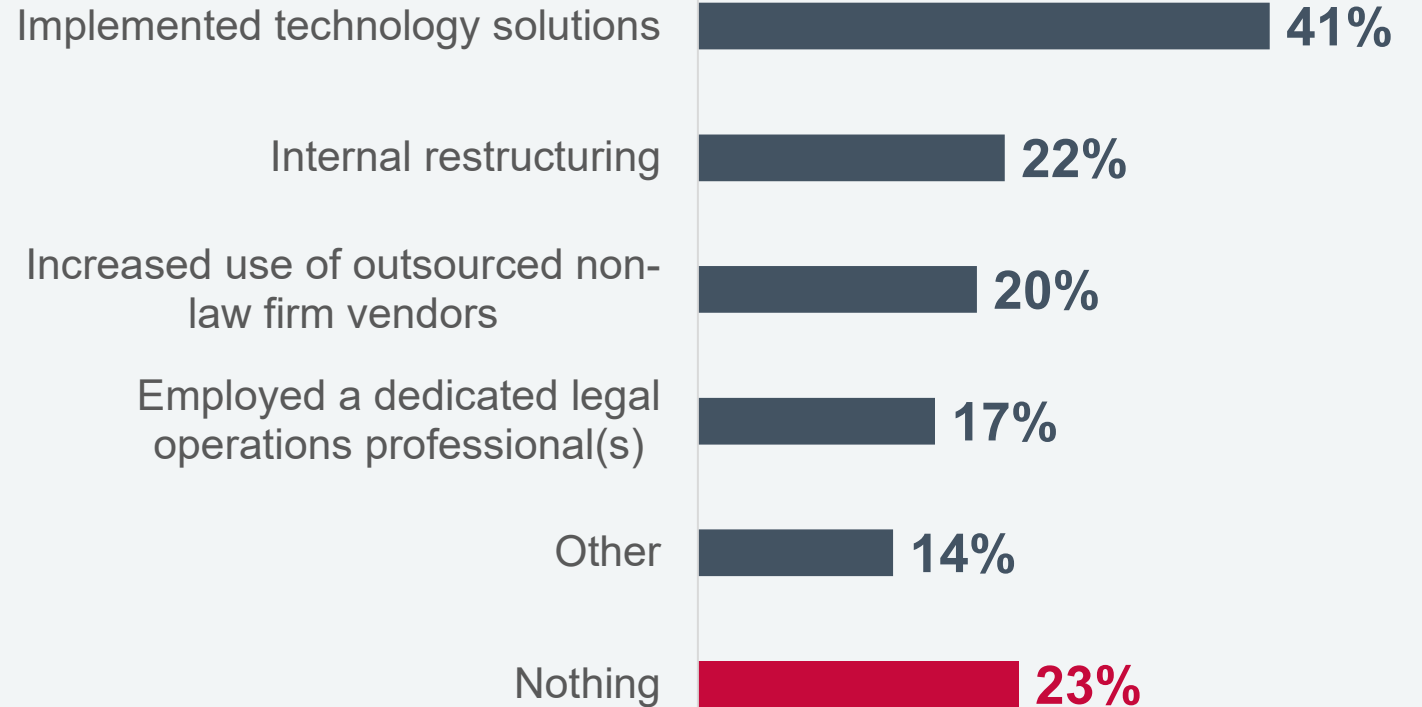
TOP BARRIERS PREVENTING EFFECTIVE RESPONSE TO LITIGATION, PRIVACY, AND COMPLIANCE OBLIGATIONS



Despite these limitations, with respect to data privacy regulations in particular, 41 percent of CLOs say they have implemented technology solutions to help with compliance. Others have restructured internally and changed how they source work.

However, nearly one in four CLOs say they have done nothing to prepare their organizations to comply with these regulations!

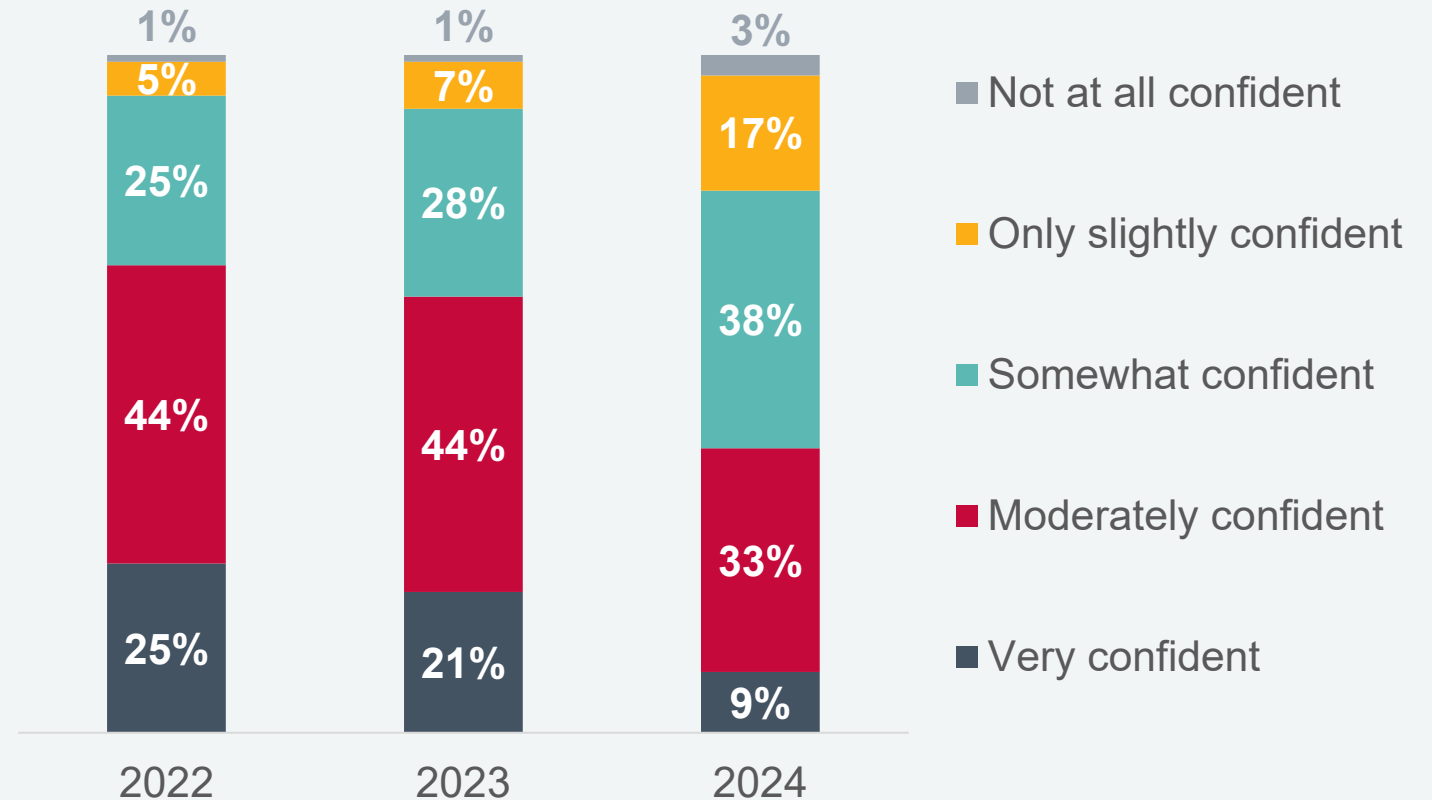
HOW HAVE YOU PREPARED THE ORGANIZATION TO COMPLY WITH DATA PRIVACY REGULATIONS?



It is possible that CLOs who indicated they have done nothing to prepare for their compliance obligations are reporting this because they are already fully prepared and believe nothing more is needed. However, when asked about their confidence in mitigating against emerging data risks, those who have done nothing were least confident of all.

Confidence has also been declining year-over-year as compliance obligations have become increasingly difficult and ambiguous.





CONFIDENCE IN ORGANIZATION'S ABILITY TO MITIGATE AGAINST EMERGING DATA RISKS






10 WAYS CLOs CAN LEAD ON CORPORATE DATA SECURITY



UNDERSTAND APPLICABLE LAWS & REGULATIONS




-  This point may be obvious but is still important to mention as a critical component in any overarching legal approach to data security. Make sure to stay updated on relevant data protection laws and regulations, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Health Insurance Portability and Accountability Act (HIPAA), and others potentially relevant to your industry or business.
-  Conduct regular reviews to ensure that your company's data security practices are aligned with the legal requirements in all jurisdictions where you operate.
-  Engage with your legal staff, compliance officers, and potentially outside counsel to interpret complex legal requirements and ensure that your data security strategies are compliant.
-  ACC partners with Lexology to offer members a [daily newsfeed](#) of legal analysis and updates tailored to the work areas and jurisdictions you select. [Learn more](#) and [join ACC!](#)

DEVELOP COMPREHENSIVE DATA SECURITY POLICIES

-  Collaborate with IT and cybersecurity teams to develop robust data security policies that address all aspects of data protection, including data encryption, access controls, data handling procedures, and incident response protocols. Remember that 45 percent of organizations have no overall data management strategy. This is a key opportunity for CLOs to take the lead.
-  Tailor policies to the specific needs and risk profile of your organization, considering factors such as the types of data collected, industry regulations, and business operations.
-  Regularly review and update policies to adapt to evolving threats and changes in legal requirements.

 [Sample Company Data Privacy and Protection Policy](#)




IMPLEMENT EMPLOYEE TRAINING & AWARENESS PROGRAMS

-  Develop training materials and conduct regular training sessions to educate employees about data security best practices, including recognizing phishing attempts, creating strong passwords, and securely handling sensitive data. This will require strong coordination with IT and cyber teams as many of the technical details will need to be developed and communicated by those teams.
-  Foster a culture of security awareness by providing ongoing communication and reinforcement of security policies and procedures.
-  Incorporate data security training into onboarding processes for new employees and provide refresher training sessions periodically.






[Top Ten Steps to Planning and Training for Security Incidents](#)

COLLABORATE WITH IT & SECURITY TEAMS




-  Establish a cross-functional team consisting of legal, IT, and cybersecurity staff to collaboratively develop and implement data security strategies. This may be an easier task for the 14 percent of organizations where the CLO already oversees IT and cyber teams.
-  Work closely with IT and cybersecurity teams to understand technical security measures and ensure alignment with legal requirements.
-  Conduct regular meetings and workshops to facilitate communication and collaboration between legal and technical teams on data security initiatives.

MONITOR COMPLIANCE & CONDUCT AUDITS

-  Establish processes for monitoring compliance with data security policies, including regular audits and assessments of security controls.
-  Conduct periodic risk assessments to identify vulnerabilities and areas for improvement in data security practices.
-  Implement mechanisms for tracking and documenting compliance efforts, including incident response activities and remediation efforts.

 [ACC-Ethisphere Data Privacy Program Assessment Tool](#)




ACTIVELY MANAGE VENDORS

-  Evaluate the data security practices of third-party vendors and service providers through due diligence processes and security assessments.
-  Include data security and compliance requirements in vendor contracts and service level agreements, specifying expectations for data protection measures and incident response procedures.
-  Monitor vendor compliance with contractual obligations through regular reviews and audits.



[ACC's Data Steward Program](#)




CONDUCT INCIDENT RESPONSE PLANNING

-  Develop a comprehensive incident response plan that outlines roles and responsibilities, escalation procedures, and communication protocols in the event of a data breach or security incident.
-  Ensure that legal requirements for reporting data breaches are clearly defined in the incident response plan and that relevant regulatory authorities are notified in a timely manner.
-  Conduct regular tabletop exercises and simulations to test the effectiveness of the incident response plan and identify areas for improvement.



[Privacy Data Breach Response Policy](#)

USE PRIVACY BY DESIGN PRINCIPLES

-  Advocate for privacy by design principles in the development of products and services, emphasizing the importance of integrating privacy and security considerations from the outset.
-  Collaborate with product development teams to incorporate privacy and security features into the design phase of projects, such as data minimization, consent management, and anonymization techniques.
-  Provide guidance and training to ensure that developers and designers understand and adhere to privacy by design principles throughout the development lifecycle.



[Product Privacy Done Right](#)




STAY INFORMED ABOUT EMERGING THREATS

-  Stay abreast of emerging cybersecurity threats and trends by actively participating in industry groups, attending conferences, and engaging with peer organizations.
-  Subscribe to relevant threat intelligence feeds and information sharing platforms to stay informed about new vulnerabilities, attack vectors, and mitigation strategies.
-  Use insights gained from monitoring emerging threats to continuously enhance data security strategies and prioritize resource allocation to address evolving risks.



[AI—Cybersecurity Solution or Threat?](#)

INTEGRATE DATA SECURITY INTO BOARD REPORTING & GOVERNANCE PRACTICES

-  Keep the board of directors informed about the company's data security posture through regular reporting and updates on data security initiatives, risk assessments, and compliance efforts.
-  Work with the board to establish clear governance structures and oversight mechanisms for data security, including the establishment of board-level committees or advisory groups focused on cybersecurity.
-  Provide guidance and support to the board on understanding the legal and regulatory implications of data security risks and the importance of prioritizing investments in data protection measures.



[Cybersecurity and Data Breaches: How In-House Counsel Can Engage the Board](#)

CONTACT US

research@acc.com

membership@acc.com

[30-Day Trial Membership](#)