ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

6 Cybersecurity Best Practices in the Age of Generative AI

Technology, Privacy, and eCommerce

Banner artwork by nine2nine / *Shutterstock.com*

Cybersecurity is no longer just an IT issue; it is a fundamental business risk with significant legal and regulatory implications. And in-house counsel play a critical role in managing cybersecurity risk, from ensuring regulatory compliance to mitigating liability in the event of a breach.

As cyber threats grow more sophisticated — fueled by ransomware, AI-driven attacks, and supply-chain vulnerabilities — legal teams must work closely with security professionals to implement best practices that align with leading frameworks, such as the NIST Cybersecurity Framework, ISO 27001, and regulatory guidance from agencies like the SEC, FTC, and European Data Protection Board.

This article outlines key cybersecurity strategies that in-house counsel should champion to strengthen their organization's security posture.

1. Multi-factor authentication: A critical first line of defense

Industry experts agree that compromised credentials remain one of the most common causes of cyber breaches. Multi-factor authentication (MFA) significantly reduces the risk of unauthorized access by requiring additional verification methods. In-house counsel should:

- Ensure vendor contracts include MFA requirements for third-party access to corporate systems and sensitive data.
- Advocate for company-wide MFA adoption in collaboration with IT and compliance teams, particularly for high-risk users such as executives and finance personnel.
- Monitor evolving regulatory requirements, such as SEC disclosure rules, that increasingly expect organizations to implement strong authentication controls.

ACC Members: Visit ACC's Cybersecurity and Privacy Resource Collection

2. Software updates and patch management: Reducing legal and compliance risks

Cybersecurity incidents often result from exploiting known vulnerabilities in unpatched software. A strong patch management policy can protect against such attacks and reduce liability. Legal teams should:

- Ensure security patching policies are formalized in corporate governance documents and compliance programs.
- Include contractual obligations for timely security updates in vendor and cloud service agreements, particularly for SaaS providers.
- Maintain audit trails of patch management efforts, as failure to apply patches has been cited in regulatory enforcement actions following data breaches.

3. Secure system configurations and endpoint protection

According to leading cybersecurity reports, misconfigured systems and inadequate endpoint security remain top attack vectors. Legal teams should:

- Work with IT to align security configurations with best practices from organizations like the Center for Internet Security (CIS).
- Ensure vendor risk assessments include security baselines for cloud services, software providers, and third-party integrations.
- Document security controls and defenses, as failure to implement basic protections can be viewed as negligence in legal proceedings.

4. Employee training and insider threat mitigation

Cybersecurity experts consistently highlight human error as a leading cause of security breaches. Employees who fall victim to phishing or social engineering attacks can inadvertently expose sensitive data. In-house counsel should:

- Ensure cybersecurity training is a formal compliance requirement, particularly for employees handling sensitive customer or financial data.
- Incorporate cybersecurity policies into employee handbooks, clearly outlining responsibilities and consequences for noncompliance.
- Advocate for leadership engagement, as executive buy-in is critical to fostering a security-first culture.

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

5. Data security, governance, and AI-driven threats

With the rise of AI-powered cyber threats, data governance is more critical than ever. Leading cybersecurity frameworks emphasize the need to classify, protect, and monitor sensitive data. Legal teams should:

- Ensure data classification and protection measures align with compliance requirements such as General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and industry-specific regulations.
- Work with IT to implement data loss prevention (DLP) policies, preventing unauthorized access and exfiltration of sensitive corporate data.
- Monitor emerging AI regulations and security risks, particularly those related to deepfake technology and AI-driven phishing scams.

6. Incident response strategy and playbooks

Having a robust incident response strategy is crucial. Detailed playbooks tailored to various types of cybersecurity incidents, with step-by-step procedures for identifying, containing, eradicating, and recovering from incidents are essential. In-house counsel should:

- Regularly review and update the playbooks to ensure they remain relevant and effective. Not sure where to start? Download the Ten Key Items to Strengthen Preparedness for Data Incident Response checklist.
- Include up-to-date infrastructure diagrams and documentation in playbooks to provide clear understanding of the network and system architecture.
- Conduct regular exercises to simulate cybersecurity incidents to test effectiveness of the playbooks.
- Implement feedback from the exercises and adjust the playbooks based on evolving threats.

Taking the lead in cybersecurity

Cybersecurity is an evolving risk that demands legal, technical, and business alignment. By implementing best practices — such as MFA, patch management, employee training, and robust data governance — organizations can strengthen their security posture while reducing regulatory and litigation risks.

In-house counsel must take an active role in shaping cybersecurity policies, negotiating stronger vendor agreements, and ensuring compliance with evolving legal frameworks. Proactive engagement in cybersecurity risk management is not just a best practice; it is a business imperative.

For more best practices from your in-house peers, join ACC now!

Ranti Okunoren

Principal Corporate Counsel

Microsoft

Ranti Okunoren is a principal corporate counsel at Microsoft with extensive legal expertise in contracts,

intellectual property, data privacy, compliance, and responsible AI. Okunoren leads strategic legal support for the Global Retail and Consumer Goods, Global Energy & Resources, and Global Azure Gaming Industry sales teams, enhancing customer adoption of Microsoft's AI products and addressing legal challenges.

Before joining Microsoft, Okunoren was deputy general counsel at the Army and Air Force Exchange Service (AAFES), providing strategic legal counsel on e-commerce, business strategies and transactions for US military installations worldwide. She holds a JD from Southern Methodist University (SMU) Dedman School of Law and a BS in Information Systems from the University of Texas at Arlington.