NRF Center
for Digital Risk & Innovation

# NRF Center for Digital Risk & Innovation Workshop Report

## Cyber Regulatory Change Management in Retail

PREPARED IN
COORDINATION WITH

pwc

New cybersecurity and technology-related regulations are reshaping how retailers manage their cybersecurity governance and risk management activities. In light of these changes, the National Retail Federation's (NRF) Center for Digital Risk & Innovation (CDRI) collaborated with PwC to hold retail practitioner workshops in Dallas and Washington, D.C., in the fall of 2024 to better understand retailers' concerns about new policies and regulations, gain insights into how retailers are addressing and complying with them, and document industry-leading practices and future strategies.

This report highlights key findings from the discussion at these two workshops. All findings and observations below are anonymized but reflect input and dialogue from senior-level cybersecurity, technology, and legal leaders at national U.S.-based retail companies, representing a variety of subsectors.

## Cybersecurity and technology regulatory landscape

The current regulatory landscape was a central topic of discussion. While some participants expressed support for regulation that provided clarity for investment, several concerns were expressed:

- **Inconsistent requirements**: The patchwork of varying state regulations and the lack of federal preemption was identified as a significant challenge, creating complexity for businesses operating across different jurisdictions.
- **One-size-fits-all approach**: Participants noted that regulations often fail to consider the specific needs and resources of different businesses, particularly small and medium-sized enterprises (SMEs). There's a recognized need for different levels of regulation and avenues of implementation to confirm SMEs aren't overwhelmed.
- **Resource constraints**: Limited budgets and staffing, coupled with growing responsibilities, make compliance difficult for many organizations. This concern is especially pertinent as cybersecurity and technical teams are often asked to do more with less.
- **Specific regulations**: The Securities and Exchange Commission's (SEC) cyber disclosure rule, which mandates public companies disclose cyber incidents, and the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), a federal law requiring critical infrastructure companies to report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA), were highlighted as key regulatory activities impacting the cybersecurity landscape for retailers. Participants also noted the importance of understanding cross-sector dependencies and the impact of state and international data breach laws.

Participants acknowledged that regulations could help organize cybersecurity leaders to advocate for security investments. However, there's a recurring tension between investments focused on compliance versus direct improvements to security. The limited resources available are being spent on tools and tracking modules instead of on improving the security environment itself.

# Internal alignment and efficiency

The workshops highlighted the critical need for better internal alignment and efficiency within retail companies to address new cyber regulatory requirements:

- **Breaking down silos**: Cross-functional collaboration between legal, cybersecurity, privacy, and other relevant teams is essential for effective data governance and compliance. Some cybersecurity leaders have counterparts in legal and compliance roles, but these relationships are still evolving and maturing in many companies. Collaboration should focus on the impacts and risks related to new regulations, and what's realistic and feasible for a company to implement.

- **Early integration of security**: Participants spoke to the importance of having security integrated early in the technology development cycle. Companies that implement security well have it built in from the start, with cross-functional teams that include enablement, security, and governance groups.

- **Board engagement**: Educating boards on cybersecurity risks and their business impact is crucial. However, a lack of technical experience on boards often hinders effective decision-making on cybersecurity and related technology risk questions. Having board members with security and technology backgrounds, including from other sectors, can help to translate complex technology questions to other board members.

- **Shifting the budget narrative**: Consider reframing cybersecurity from a cost center to a strategic investment tied to brand reputation and customer trust. Measuring the impact of cybersecurity on revenue can be challenging, and companies are cautious about making financial projections based on security investments.

- **Cyber insurance**: The role of cyber insurance is another factor that drives internal coordination and prioritization. While cyber insurers' requirements have helped some CISOs make the case for investment, there's ongoing concern about the cost of cyber insurance, leading some companies to explore self-insurance options. Other participants expressed concerns about insurers changing coverage without clearly communicating the changes — for example, excluding coverage for state-sponsored attacks.

- **Third-party cyber risk management:** Managing third-party risk is becoming increasingly complex, as retailers rely on a growing network of vendors and service providers. The lack of clarity around ownership of third-party risk and limited visibility into vendor security practices are key challenges that retailers should address. Leveraging contracts to enforce stronger security standards among vendors is crucial but difficult to implement across the board. Some companies are using data processing agreements (DPAs) to address this issue.

## AI and emerging technologies

While the discussions focused primarily on cybersecurity policy and regulation, other policy areas can have an adjacent impact, most notably with respect to privacy and artificial intelligence (AI). Key areas of discussion on these topics included:

- **AI and privacy-related governance alignment**: Workshop participants discussed opportunities to align their cybersecurity activities with analogous governance activities related to privacy and AI and leverage common internal resources instead of creating siloes for each.
- **AI risk management around customer engagement:** The use of AI tools creates significant new opportunities for retailers, but also elevates risks (e.g., potential AI model bias, targeted marketing related to sensitive purchases) that should be addressed by cross-functional risk management teams.
- **Employee use of AI tools:** Several workshop participants noted concerns about employee use of public AI tools that pose risks to retailers' intellectual property and security. This highlights the importance of training and upskilling employees on AI, including those in non-technology roles.
- **Third-party use of AI**: Many retail vendors are integrating AI tools, sometimes without notice, which creates new risks for their retail customers. Understanding how these AI models function and what data they're using is critical.

## Key takeaways for retailers

The discussion in the two workshops yielded a number of actionable takeaways for retailers. Retail leaders should prioritize efforts in these five areas to respond to increasing cyber and tech regulation:

- **Develop an enterprise cyber risk management framework**: Integrate cybersecurity, technology, compliance, legal, and other relevant business units into the process.
- **Prioritize board education**: Conduct tailored training sessions and provide regular updates on cybersecurity and other technology risks and mitigation strategies.
- **Explore emerging technologies**: Invest in tools to enhance visibility into third-party data usage, security practices, and regulation tracking.
- **Reframe the cybersecurity narrative**: Communicate the value of cybersecurity investments in terms of brand reputation, customer trust, and business resilience.
- **Actively participate in industry groups**: Engage with organizations like NRF and the Retail and Hospitality ISAC (RH-ISAC) to share leading practices and advocate for policy changes.

# Looking ahead

NRF expects the policy context around these issues — also echoed and addressed in PwC's 2025 Global Digital Trust Insights survey — will continue to rapidly evolve over the next several years. While the specific elements of current and pending cyber rules may change or be harmonized with each other, and ongoing efforts to improve software security may mitigate some cyber risks, there will still be an imperative for retailers to invest in their cybersecurity programs and increase internal alignment around risk management.

Regulatory complexities, resource constraints, and evolving cyber threats will likely continue to challenge retailers, but these challenges also present an opportunity to strengthen internal alignment, enhance board engagement, and reframe cybersecurity as a business enabler rather than just a compliance requirement. By fostering cross-functional collaboration, leveraging emerging technologies responsibly, and advocating for regulatory clarity, retailers can navigate the shifting policy landscape while maintaining resilience and customer trust.

Ultimately, cybersecurity is not just a regulatory obligation — it's a core component of brand integrity, operational stability, and long-term business success. Retailers that invest in effective cybersecurity programs and actively engage with industry peers and policymakers can be better positioned to adapt to future regulatory changes and emerging risks. NRF and PwC intend to continue monitoring developments and supporting retailers in shaping a cybersecurity strategy that's not only compliant but also forward-thinking and resilient.

## About NRF

The National Retail Federation passionately advocates for the people, brands, policies and ideas that help retail succeed. From its headquarters in Washington, D.C., NRF empowers the industry that powers the economy. Retail is the nation's largest private-sector employer, contributing $5.3 trillion to annual GDP and supporting more than one in four U.S. jobs — 55 million working Americans. For over a century, NRF has been a voice for every retailer and every retail job, educating, inspiring and communicating the powerful impact retail has on local communities and global economies.

## About the NRF Center for Digital Risk & Innovation

The NRF Center for Digital Risk & Innovation is the National Retail Federation's hub for engagement on key technology issues that have significant policy and risk management implications for the global retail industry. The Center engages with retailers, industry partners and other stakeholders to develop guidelines and recommended best practices on technology issues and inform decision-making and risk management by retail business leaders.

## About PwC

With offices in 152 countries and nearly 328,000 people, PwC is among the world's leading professional services networks. We help organizations and individuals create the value they're looking for by delivering quality audit, tax and consulting services. As the needs of PwC's clients and stakeholders have changed, so has PwC. We look at the world through the eyes of clients, anticipating and listening to their needs, helping them to solve problems while capitalizing on the opportunities brought on by new technologies. PwC's mission is to build trust in society and solve important problems. We work alongside our clients to help deliver solutions and address challenges using the strength of our business services lines and our global network of firms. PwC's global Cybersecurity, Risk & Regulatory practice of 5,000+ practitioners include specialized consultants, risk management professionals, former law enforcement agents, cyber-forensic investigators, intelligence analysts, technologists, attorneys and industry leaders. Our team has deep experience helping global businesses across industries strategically assess, design, deploy and improve their cyber, risk and regulatory programs.