Clifford Chance

BRIEFING

Consumer goods & retail: Cybersecurity issues

31 March 2026

Cyberattacks are a major risk for consumer goods and retail businesses, disrupting trading and causing significant financial losses and regulatory scrutiny. Those risks are increasing, driven by AI-enabled attack methods that are becoming faster and more effective, alongside increased activity by state-linked groups. How boards prepare and respond is crucial. Operational impact, enforcement action, litigation exposure and reputational damage will turn on the strength of directors' planning and governance frameworks and how they handle an incident when it occurs.

Key takeaways

1. Businesses should strengthen identity and access controls.
2. Track regulatory obligations across all jurisdictions.
3. Carry out active governance of supply chains and train boards on cyber security, cyber incidents and planning for business continuity.

Sophisticated threats, increasing losses

We expect cyber-attacks across Europe, APAC and the US to continue to increase. Criminals are becoming more sophisticated at exploiting weaknesses in IT systems and authentication controls, and AI is making it easier for them to scale attacks more quickly. Consumer goods and retail companies are acutely exposed to cyber failures. Even with insurance in place, cyber failures can create significant financial losses – and coverage may not extend to all impacts.

As part of mitigating these risks, businesses need to strengthen identity and access controls. Reinforced helpdesk and authentication processes can reduce the risk of an attack succeeding through impersonation of a legitimate user, while privileged access management and segmentation

frameworks must meet evolving regulatory expectations and withstand scrutiny following a cyber incident. Companies should check their business interruption insurance to ensure that the terms regarding non-physical damage are sufficiently broad and to maximise their ability promptly to instruct lawyers and specialists (such as crisis comms; and forensic IT providers) of their choice in the event of a cyber incident.

Increasing regulatory obligations

Boards now face increasing scrutiny as cyber regulations across jurisdictions expand reporting duties, raise expectations on governance and accountability and work to different timelines.

The EU has introduced a suite of regimes – including NIS2, the Cyber Resilience Act and the Critical Entities Resilience Directive – that impose mandatory risk management, incident reporting, supply chain security and board-level accountability obligations. For example, under NIS2 which can apply to certain companies in the consumer goods and retail sector, in-scope companies must provide early warnings within 24 hours of significant incidents, followed by detailed reporting within 72 hours. These laws are evolving, including through the January 2026 cybersecurity package proposed by the European Commission, which broadly intends to improve resilience and capabilities for cybersecurity. It includes the introduction of a single-entry point for notifications currently required under various digital regimes (for example, AI, data access, privacy and cybersecurity), as proposed in the Digital Omnibus, and seeks to harmonise substantive NIS2 obligations. While the practical impact of some of these proposed changes remains to be seen, many companies are likely to need to review and adjust their EU incident response processes when the legislative positions crystallise. In addition, the Cyber Resilience Act, which came into force in December 2024 on a phased basis, introduced cybersecurity obligations for products with digital elements such as mobile apps and internet of things (IoT) supply chain tools through their lifecycles.

In the UK, the Cyber Security and Resilience Bill was introduced to Parliament in November 2025, extending obligations to certain digital services, managed service providers and supply chains. The bill brings data centres specifically into scope and introduces 24-hour incident-notification requirements aligned with EU NIS2 timeframes. Separately, the UK government has consulted on proposals to ban ransomware payments for public sector bodies and critical national infrastructure operators, alongside mandatory incident-reporting requirements.

In the US, the Securities and Exchange Commission is tightening cybersecurity disclosure expectations. In addition, the Federal Trade Commission expanded requirements under the Children's Online Privacy Protection Act (COPPA) regulations for website and online services operators regarding collection of personal information for children under 13 years of age. These regulations took effect on June 23, 2025. The FTC has intensified its enforcement focus for consumer brands, using Section 5 "unfair or deceptive practices" authority to enforce cybersecurity expectations.

The US Federal Communications Commission has also introduced a voluntary program for wireless interconnected smart products (IoT), where a U.S. Cyber Trust Market logo will appear on products that meet the program's cybersecurity standards. US States continue to pass new cybersecurity legislation and amend existing legislation; for example,

shortening breach reporting timelines and broadening the definition of personal data.

In APAC governments are also strengthening cybersecurity and resilience requirements. For example, China's amendments to its Cybersecurity Law became effective in January 2026, including expanded extraterritorial outreach over activities that may be subject to enforcement, increased fines and penalties for both individuals and companies, and the inclusion of explicit supply chain obligations. Australia's recent Cyber Security Act and its associated rules introduce mandatory reporting of ransomware incidents for certain entities and, from 4 March 2026, mandatory security standards and statements of compliance will be required for certain consumer-grade connected products, such as smart devices.

Continuous monitoring of relevant regulations and how they are interpreted by regulators in all the jurisdictions in which businesses operate is essential. New regulations often introduce conflicting timelines and different definitions of key concepts such as "personal data" and "sensitive data". For example, in the UK, in a case arising from a cyber-attack on a large electronics retailer, Courts recently confirmed that the former term is to be interpreted expansively, which may pave the way for further increases in enforcement activity by data protection regulators, which are taking a robust approach to enforcement.

Multinational companies should track developing regulatory obligations and approaches across jurisdictions and anticipate multi-jurisdictional reporting, parallel investigations and differing regulatory timelines. Boards should be equipped to meet heightened expectations under NIS2, UK disclosure rules and emerging US requirements, as well as new ones in APAC.

Supply chain governance

Consumer goods and retail companies remain acutely exposed to cyber failures within their supply chains. Businesses must move beyond basic vendor audits towards active, ongoing governance of suppliers to ensure resilience. Recent cyber incidents underscore that weaknesses in third-party arrangements can materially increase regulatory and liability exposure.

Businesses should have contract and cyber law specialists review vendor due diligence processes and contractual protections with particular attention on audit rights, incident cooperation obligations, responsibilities relating to changes in legal obligations, and clarity on when suppliers may rely on force majeure.

An increased focus on board responsibilities

Cybersecurity is now a core corporate governance expectation globally. The first 24 to 72 hours following a cybersecurity incident frequently determine regulatory outcomes; without a real-time tracking mechanism, a company risks missing a "24-hour" requirement in one country while focused on a "72-hour" deadline in another.

Board members may benefit from continual training on cybersecurity and their reporting obligations to data authorities and, potentially, to financial services' regulators. Planning and preparation are essential to ensure effective incident response oversight, reduce criticism and, in some circumstances, personal liability following a major incident. For example, under NIS2, members of the management bodies of essential entities can be temporarily banned from exercising managerial functions following

serious and repeated infringements of their cybersecurity obligations. This sanction does not extend to important entities, making the essential/important classification a critical threshold for boards to assess. Most consumer goods and retail companies are likely to fall outside the high-criticality sectors listed in Annex I to NIS2 (which cover areas such as energy, transport, banking, health and digital infrastructure) and would therefore be classified as important rather than essential entities. However, companies operating large online marketplaces are expressly listed in Annex I, meaning they could qualify as essential entities subject to the stricter regime, including the management ban.

Planning and preparation should include:

- Maintaining a concise, role-based incident response plan and notification playbook that is jurisdiction-specific and takes account of the evolving state-of-the-art, including AI-related issues, and which is well understood across leadership.
- Rehearsing board-level decision-making on ransomware, sanctions and multi-jurisdictional notification, where timing and consistency of messaging have proven decisive in investigations.
- Reviewing business continuity planning. Regulators and insurers increasingly expect demonstrable resilience measures, along with clear documentation of how internal processes and policies meet legal and supervisory requirements across different regions/jurisdictions.

Increasing litigation risks following cyber breaches

Cyber failings will likely lead to more class actions under data protection and other laws in certain jurisdictions. For example, affected consumers may be able to make claims for distress and loss of control over personal data following unauthorised access to names, contact details and order histories. Regulators and courts will increasingly scrutinise the adequacy of organisational security and the harm caused by compromised data, even where no direct financial loss is sustained.

For further information, please see:

Cyber survival strategies for boards

All aboard the Digital Omnibus? Highlights from the EU's Digital Simplification Package; and

EU cyber reforms proposed, including overhauled Cybersecurity Act.

Thibaud d'Ales
Partner, Co-Head of the Consumer Goods & Retail Sector, Paris

thibaud.dales@cliffordchance.com
+33 6 18 63 27 56

Valerie Kong
Partner, Co-Head of the Consumer Goods & Retail Sector, Singapore

valerie.kong@cliffordchance.com
+65 9177 2583

Stella Cramer
Partner, Singapore

stella.cramer@cliffordchance.com
+65 9011 1196

Megan Gordon
Partner, Washington

megan.gordon@cliffordchance.com
+1 202 250 4063

Jonathan Kewley
Partner and Co-Chair of the Global Tech Group, London

jonathan.kewley@cliffordchance.com
+44 78 3489 0170

Patrice Navarro
Partner, Paris

patrice.navarro@cliffordchance.com
+33 6 79 21 71 02

Dessislava Savova
Partner, Head of Continental Europe
Tech Group, Paris

dessislava.savova@cliffordchance.com
+33 6 88 88 29 46

Samantha Ward
Partner, London

samantha.ward@cliffordchance.com
+44 79 6233 8245