Cyber security in the Retail & Consumer industry: Protecting your brand from hackers and how to deal with cyber attacks

In a digitalised economy, companies in the retail sector are big targets for cyber criminals. The new cyber security risk landscape has been transformed by the increase in remote working, the growth in the number of connected devices, and the ever-growing sophistication of threat actors, e.g. through ransomware attacks. Between 2019 and 2023 an amount of more than EUR 300 billion of lost revenues are estimated due to cyber attacks by the retail industry worldwide. Further, such issues are under growing public scrutiny, illustrated, for example, by the latest Log4Shell vulnerability.

Why is cyber security relevant especially for companies in the retail sector?

- The retail industry typically processes huge amounts of personal data from their customers.
- Hackers select targets based on their financial capability. Many big retail companies are thus attractive targets for extortion.

Which (direct and indirect) sources of law obligate companies to implement cyber security measures?

- Cyber security law is unfortunately fragmented.
- Obligations for retail companies can thus stem from various sources in public and private law, for example the GDPR, product liability and product security law, EU directives on cyber security as well as from contracts with customers or business partners.

How may cyber security be required to protect your intellectual property?

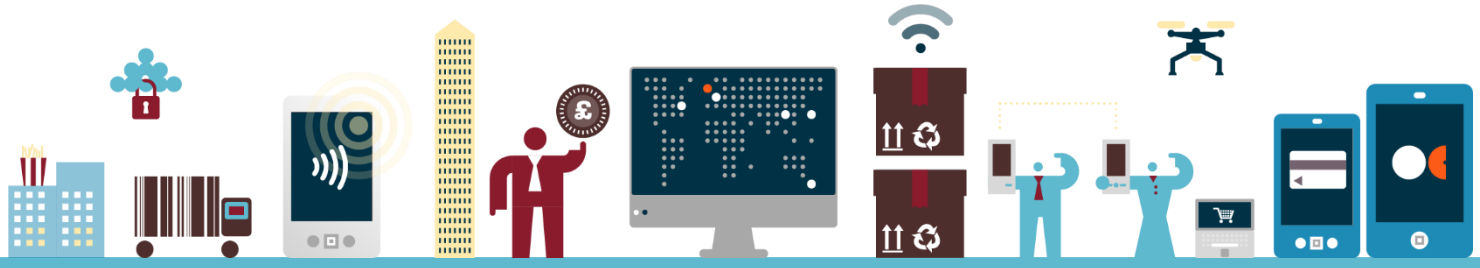
Besides the obvious economic self-interest of each company to keep its IP confidential, insufficient protection of IP against cyber risks may also have legal implications. For instance, under EU law, trade secrets only remain protected as such if safeguarded by appropriate (cyber) security measures.

What legal consequences can arise if your brand falls victim to a cyber attack?

- notification obligations of your company vis-á-vis authorities
- investigations, measures and sanctions by authorities
- claims by affected parties, such as consumers or contractual partners.

What to do in the first place to protect you brand from cyber attacks?

Besides the obvious factual need to implement any such measures, from a legal perspective it is imperative to produce appropriate documentation as well as internal measures on how to protect company asset. Further, a company should, in preparation to any such incidents, clearly allocate responsibilities among its personnel and appropriate contingency plans. For example, these should set out clearly reporting obligations towards authorities and reporting lines inside the company.



Aspects where cyber security becomes a legal matter – and where we can help

Preparedness

- Identification and mapping of legal requirements with industry standards
- Delegation of responsibilities / establishment of governance structures
- Drafting corporate guidelines and other relevant documents
- Conceptualisation of incident response and reporting processes
- Vendor selection / contractual commitment of service providers
- Contractual clauses in contracts with customers

Response

- Verification and execution of notification obligations (internal/external**; global, to authorities or affected persons)**
  - Data protection (Art. 33, 34 GDPR)
  - NIS Directive
  - Ad hoc publicity
- Entrepreneurial scope / room to manoeuvre for directors
- Coordination / correspondence with security authorities

Follow-up / Enforcement

- Accompanying internal investigations / as well as investigations by authorities
- Evaluate and, if necessary, adapt existing policies, processes, etc.
- Defence against official sanctions / fines
- Examination and prosecution of claims against service providers
- Examination and defence of claims against oneself (for example by users or business partners)

We will be happy to support you in all legal matters relating to cyber security:

Dr. Tobias Rothkegel
Counsel
Germany

+49 40 55436 4090
tobias.rothkegel@osborneclarke.com

Anne Leßner
Associate
Germany

+49 30 7262 18049
anne.lessner@osborneclarke.com