

BUILDING AN AGILE CYBERSECURITY OPERATING MODEL FOR A MULTI-CHANNEL RETAILER

Capgemini Invent collaborated with a leading consumer electronics retailer to increase cyber resilience and align the cybersecurity operating model with the organization's new digital and IT strategies.

"Above all we appreciate the agile and efficient cooperation with Capgemini Invent. The measures which we have jointly applied across the organization are absolutely invaluable when it comes to handling potential risks."

CISO

Leading Consumer Electronics Retailer

The cutting edge of retail digitalization

As customers increasingly prefer to shop online, the retail industry has undergone massive changes and is facing further disruptive transformation. In 2019, online retail sales in Germany alone amounted to over 72 billion euros (Source: German E-Commerce and Distance Selling Trade Association). It comes as no surprise, then, that a leading consumer electronics retailer wanted to prioritize ecommerce and establish an innovative, multi-channel approach to integrate online and offline retailing.

Countless online transactions take place across the retailer's platforms every day, each signifying a potential weak spot that could incur a security breach. The e-commerce sector is especially prone to cybersecurity attacks, with hackers looking to compromise customers' personal data and commit identity fraud or credit card theft. Increasingly sophisticated attacks require a comprehensive target operating model (so called ISMS - Information Security Management System) to proactively flag and monitor any vulnerabilities.

Overview

Customer: International Consumer Electronics Retailer

Industry: Retail

Location: Germany

Client Challenges / Business Need:

The retailer wanted to improve its cybersecurity processes and capabilities in order to support a rapidly growing online business and to introduce a security operating model to meet regulatory requirements and standardize information security

Solution-at-a-glance:

By partnering with Capgemini Invent, the retailer designed and introduced a target model based on ISO 27001, reviewed and streamlined its cybersecurity strategy and transformation roadmap, and developed a new governance model

Results:

- Increased transparency of the as-is situation of information security
- Enhanced visibility of procedures that process critical business data
- Improved awareness among business stakeholders
- Development of security guidelines ready for ISO certification



Bringing cybersecurity to the next level

The retailer demonstrated a high degree of cybersecurity maturity, with monitoring (SIEM) processes already in use and awareness campaigns taking place across the organization. However, the retailer was faced with the following challenges:

- Widespread digitalization has increased the risk of cyber attacks due to widening attack vectors
- Stringent regulatory requirements e.g. the enforcement of GDPR in mid 2018
- Growing expectations and demands from customers and suppliers

The challenge was to embed cybersecurity processes throughout the organization by implementing pragmatic but also effective measures and policies. For the project to succeed, various stakeholders needed to align with the Cybersecurity Department, including Corporate Risk Management, Audit, Legal, Compliance, and Group Management, right up to the product owners.

In order to take cybersecurity to the next level, fortify the resilience of the company and meet market requirements, the retailer decided to implement an ISMS based on the international security standard ISO 27001. This specific guiding standard was chosen because it is considered a best practice and provides a holistic approach to information security, covering a wide range of topics such as software development, innovation management, and teleworking standards.

Getting ready for ISO 27001

The retailer partnered with Capgemini Invent to design and implement an ISMS based on their proven approach. This collaboration was based on the numerous successful projects the two had completed together in the past. The project began with a comprehensive review and streamlining of the cybersecurity strategy. A gap analysis revealed the need for a holistic asset inventory extension, a new policy framework and the clear definition of roles within security processes. Capgemini Invent conducted criticality and risk assessment workshops to prepare the organization for the new risk management processes.

Capgemini Invent proposed a governance model based on new product-led organizational structures, which built responsible teams around products, facilitating interdisciplinary collaboration and clearer communication channels. An additional aspect was the design and implementation of a policy framework to comply with all areas of ISO 27001 and assign clear process responsibilities. The organization's internal digital platform was designated as the single source of truth for the policy framework to ensure group-wide distribution of cybersecurity practices. The partners also collaborated to design and implement a holistic asset inventory and meet the requirements for ISMS tooling.

Embedding cybersecurity into agile IT

Capgemini Invent was able to design an agile cybersecurity organization with roles adapted to include security aspects, resulting in new positions such as DevSecOps Expert, Red Team Expert, and Data Privacy Expert.

Capgemini Invent ensured that the retailer was ISO 27001 ready by delivering the following elements:

- Improved cybersecurity awareness among top management and key business stakeholders, especially product owners
- Creation of security guidelines (e.g. secure development guidelines and teleworking guidelines) based on Capgemini Invent best practices, which are ready for ISO certification and ensure compliance with internal and external requirements
- Enhanced visibility of business-critical data relating to payment, customers, employees, and supply chain. The data mapping allows protection needs and risk mitigation to be continuously integrated into ongoing processes
- Improved risk assessment due to cross-department collaboration with agile product-centric structure
- Transparency of the as-is situation of information security and indication of risks and gaps
- Optimized reporting dashboards for categorizing levels of vulnerabilities or breaches

Combining technology with governance

The next project phase will involve the technical implementation of an advanced ISMS. This final stage will consolidate the retailer's agile structure with innovative technology to ensure the organization can continuously respond to threats in the future.

The Collaborative Approach:

The retailer and Capgemini Invent benefited from a longstanding partnership and close communication over the entire six month duration of the project. Together they acted as true partners, open for discussion in all areas of the project especially when designing a new cybersecurity operating model and cyber risk management approach. The high level of flexibility made it possible to quickly react to necessary changes that emerged throughout the process.

About Capgemini Invent

As the digital innovation, consulting and transformation brand of the Capgemini Group, Capgemini Invent helps CxOs envision and build what's next for their organizations. Located in more than 30 offices and 22 creative studios around the world, its 6,000+ strong team combines strategy, technology, data science and creative design with deep industry expertise and insights, to develop new digital solutions and business models of the future.

Capgemini Invent is an integral part of Capgemini, a global leader in consulting, technology services and digital transformation. The Group is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of almost 220,000 team members in more than 40 countries. The Group reported 2019 global revenues of EUR 14.1 billion. People matter, results count.

Visit us at

www.capgemini.com/invent

Capgemini Invent Contact:

Paul Lokuciejewski,

Head of Cybersecurity & Trust

paul.lokuciejewski@capgemini.com