Retail resilience: defending against cyber attacks in the age of digital transformation

With increased digitisation within the UK retail sector due to a surge in online shopping and technology innovations, consumers are demanding seamless, personalised purchases at discount prices. There is an accelerating shift to e-commerce platforms, mobile apps and integration of AI machine learning and IoT (Internet of Things) for a more seamless and personalised experience.

However, with its vast digital touchpoints and transactions, the retail sector faces the growing risk of data breaches, identity theft and cyber attacks. Protecting customer information and maintaining trust must be paramount to any retail business.

Retailers are also contending with cyber security threats driven by a demand for greater supply chain and warehouse efficiency, through increased adoption of IoT, AI solutions, robotics and GPS tracking data.

Furthermore, complex supplier ecosystems and point-to-point solutions implemented with the aim of protecting network estates also open up the potential for cyber attacks. Attacks on retailers' digital infrastructure are becoming alarmingly common. In the last 12 months alone, nearly a third (32%) of UK businesses identified a cyber security breach or attack.[1]

This is made even more challenging by the migration to cloud services and SaaS (Software as a Service) solutions.

The UK retail market is particularly vulnerable to ransomware attacks. The sector has experienced a 264% surge in ransomware attacks globally on eCommerce and online retail businesses.[2] One in every five ransomware attacks target an online retail business.[3] These attacks can have damaging ramifications for supply chains and cause network system downtime, as well as economic and reputational loss.

In April 2022, UK retailer The Works was forced to close some stores, with others forced to only carry out cash transactions after they were the target of a cyber attack. It resulted in delays in stock arrivals and late deliveries of some online customer orders.

[1] UK Government, Department for Science Innovation and Technology. (2023) Cyber security breaches survey 2023
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023#chapter-4-prevalence-and-impact-of-breaches-or-attacks
[2] Charged. (2022) Cybercriminals target retail with 264% surge in attacks
https://www.chargedretail.co.uk/2022/02/17/cybercriminals-target-retail-cyberattacks/
[3] Sonicwall. (2023) 2023 Sonicwall Cyber Threat Report
https://www.chargedretail.co.uk/2022/02/17/cybercriminals-target-retail-cyberattacks/

Key security considerations

There are some key issues for retailers to consider when mapping out strategic business priorities when it comes to cyber security. These include:

- Implementing a robust security framework that covers all aspects of the retail business, such as network, cloud, endpoint, mobile and web security.
- Adopting a proactive approach to threat detection and response, such as conducting regular vulnerability assessments, monitoring network traffic and having an incident response plan.
- Enhancing customer trust and loyalty by ensuring data privacy and security, such as encrypting sensitive data, complying with data protection laws and notifying customers of any breaches.
- Collaborating with suppliers and partners to ensure cyber security across the supply chain, such as setting clear expectations, sharing threat intelligence and auditing third-party vendors.
- Educating and training employees on cyber security best practices, such as using strong passwords, avoiding phishing emails and reporting suspicious activities.

It doesn't matter what size your retail business happens to be - whether you have 50 or 50,000 customers - it's crucial to regularly refresh your cyber security strategy, as the data you retain on your customers and staff is of huge value to cyber criminals. Sixty-eight percent of Chief Information Officers (CIOs) rank cyber security as the number one tech investment priority for retailers.[4]

Cyber criminals will target retail businesses both remotely and at their operational and suppliers' locations, such as warehouses and stores. So, it's vital that retailers protect supply chains and consolidate supplier network estates to reduce risk.

It's critical retail businesses view cyber security threats through the lens of a wider security ecosystem. As digital threats become more sophisticated and organised, and regulations become tighter, the best defence is a multi-layered, fully integrated approach.

This means drawing on partnerships with your supply chains – which have become a standard attack surface for cyber criminals - that blend the latest digital technologies in cyber security to keep employees and customers secure, and your company compliant.

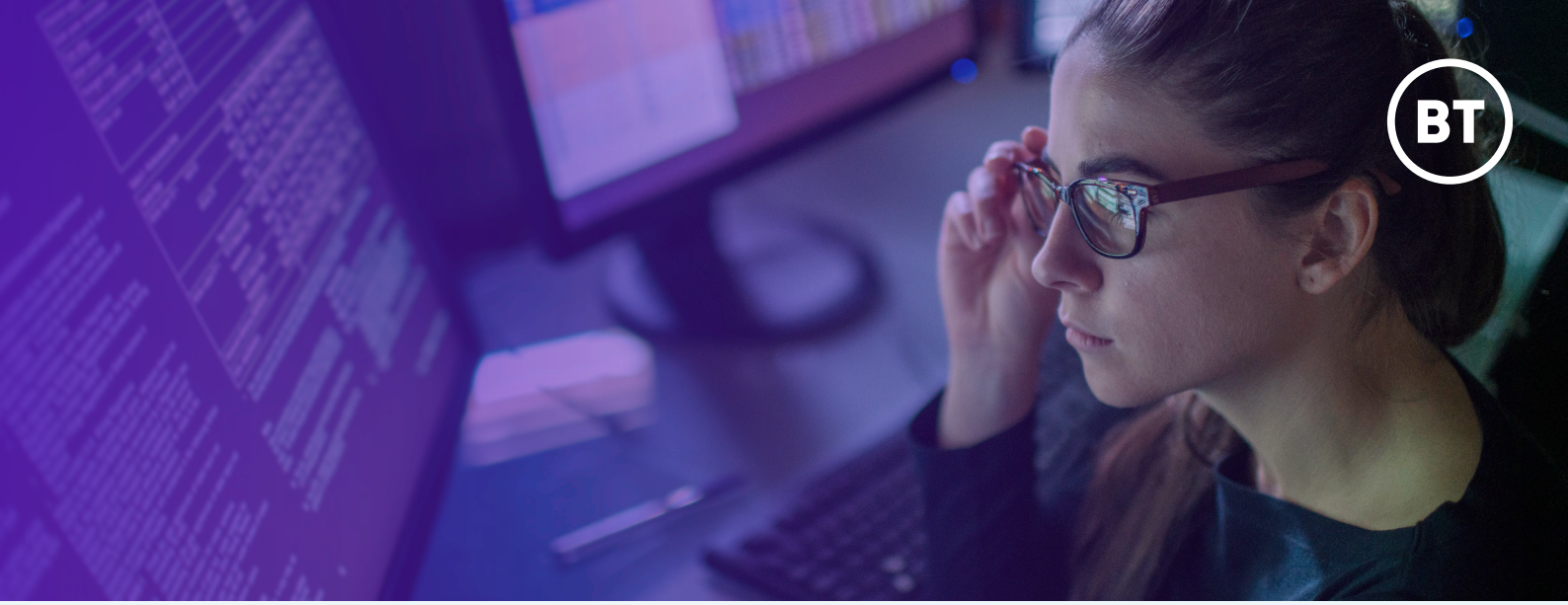
As one of the UK's leading technology companies, we have more than 70 years' experience protecting thousands of businesses in the UK. We are a trusted pair of hands in this space.

We deliver and manage much of the UK's digital infrastructure and have proven experience protecting thousands of businesses, so we know how to safeguard the most precious assets.

We do so by employing more than 3,000 security experts to ensure businesses are one step ahead of the cyber criminals.

We are vendor agnostic and only sell the best, most well-tested cyber security solutions on the market, that enable businesses of all sizes to stay ahead of the attackers with the latest digital solutions. We have taken the best security products from 200 vendors and have strategic partnerships with 16 of them, so can advise retailers on which solution is best for their business, without bias.

[4] Gartner. (2023) 2023 CIO Agenda Insights for the Retail Industry: How your peers are investing in tech to deliver on digital initiatives https://infogram.com/1p5lwe5jwkn51php7kv0l7k6q1h3w5n9nd7?live



How to improve security defence across your retail estate

Cyber security health check

We'll work with you to assess your security level and help you put a plan in place to ensure the best levels of cyber security protection. A BT cyber security health check enables businesses to understand where their security level is against the rest of the retail industry, using one of the industry's recognised frameworks, such as the CIS Critical Security Controls.

We also offer cyber security advisory and consultation services that can help businesses at every stage of their security journey.

Secure connectivity

As a leading connectivity provider, our solutions equip retailers with cutting-edge security with an encrypted network, giving them greater control over their network and helping them meet their ever-increasing bandwidth demands.

Protect online payments

In an age of online shopping and seamless payment transactions, there is an increasing threat of data breaches and non-compliance. With rapidly increasing card payment volumes, it is vital that retailers have a secure and flexible network solution in place to process their card transactions.

A simple, cloud-managed and PCI compliant payment solution enables consumers to utilise their preferred payment method.

Scalable and flexible contact centre security solutions

Ensuring security and compliance for retailers' contact centres is at the heart of what we do. Contact centre compliance and security solutions ensure retailers are secure and compliant with the latest regulations. All these solutions are scalable and flexible, making them easy to implement and manage.

Cyber security that delivers

As global security threats to UK businesses evolve, it's vital retailers update and enhance their cyber security strategies, and implement robust and flexible solutions within the security ecosystem to safeguard their organisations and supply chains.

We are perfectly placed to deliver those essential cyber security solutions and future-proof every retail business in the UK. For more information on our security products and services please visit

https://www.globalservices.bt.com/en/digital-industries/digital-sustainability

---

Lee Stephens

Principal, Security Advisory Services, BT Business