

# Lessons from recent cyber- attacks on major UK brands.

Impacts at every level & resilience  
planning.

October 2025



**In recent months, high-profile cyber-attacks have struck renowned automotive manufacturers Jaguar Land Rover and Renault in the UK. These incidents have sent ripples throughout the manufacturing & logistics sectors, exposing critical vulnerabilities in supply chain operations & raising pressing concerns for both business leaders and IT professionals.**

However, the wave of cyber threats has not been limited to the automotive industry. Other major UK brands, such as M&S (Marks & Spencer) and Co-op, have also fallen victim to catastrophic cyber-attacks, further highlighting the escalating risks across diverse sectors. As cyber threats grow in frequency and sophistication, the lessons gleaned from these events are of paramount importance for organisations reliant on complex supply networks.

*Globally, customer confidence in affected brands drops by an average of 22% following a publicised data breach, with long-term effects on loyalty and market share.*







**THE LESSONS ARE CLEAR:  
CYBER THREATS ARE  
PERSISTENT, THEIR IMPACT  
IS PROFOUND, AND ONLY A  
PROACTIVE,  
COLLABORATIVE APPROACH  
CAN MITIGATE THE RISKS.**

## Overview of the attacks

The cyber-attacks on Jaguar Land Rover and Renault unfolded within a rapidly evolving threat landscape. In early 2025, both companies reported significant disruptions attributed to ransomware campaigns targeting their IT systems and third-party suppliers. The attacks involved unauthorised access to sensitive networks, causing immediate operational halts at several manufacturing sites and affecting the flow of components across the UK and Europe.

For Jaguar Land Rover, the incident led to a temporary suspension of production at key plants, with the company confirming that critical data - including supplier contracts and logistics information - had been compromised. Renault faced similar challenges, with supply chain management systems rendered inaccessible, leading to delayed deliveries and inventory shortages.

The timeline of these attacks underscores the speed at which threat actors can cripple interconnected business processes, often before traditional security responses can mobilise. Likewise, retail giants such as M&S and Co-op have experienced severe cyber incidents in recent years, resulting in massive disruptions to customer-facing services, supply chain delays, and data breaches impacting millions of customers.



## Consequences for customers

For customers, the consequences extended beyond delayed vehicle deliveries. Service interruptions at dealerships, postponed maintenance appointments, and a lack of visibility into order statuses eroded trust and satisfaction. More concerning, the exposure of sensitive customer data - such as contact details, transaction histories, and vehicle identification numbers - raised the spectre of identity theft and fraud. Retail and grocery customers at the likes of M&S and Co-op have likewise faced service outages and data compromises, highlighting that cyber security failures have a very real and direct impact on everyday consumers.

Trust, once lost, is difficult to regain. These incidents serve as a stark reminder that robust cyber security is not merely an internal concern, but a cornerstone of customer confidence and brand reputation.

## Impact on supply chain organisations

The repercussions for supply chain organisations were immediate and far-reaching. With just-in-time logistics disrupted, numerous suppliers - particularly smaller tier-two and tier-three partners - found themselves unable to fulfil scheduled shipments.

This dependency on digital platforms and real-time data exchange amplified the impact, as even minor system outages cascaded into widespread delays and financial strain.

Moreover, the attacks highlighted the systemic risk present in today's interconnected supply networks. A single compromised supplier became a conduit for broader exposure, illustrating the "weakest link" effect. This dependency risk has prompted business leaders to re-examine not only their own cyber defences but also those of their strategic partners.

The experiences of M&S and Co-op further demonstrate how cyber-attacks in one sector can reverberate throughout related industries and supply chains, impacting everything from food logistics to retail inventory management.





# THE FACTS

- According to the UK's National Cyber Security Centre, ransomware attacks on manufacturing organisations increased by over 35% in 2024 alone.
- Industry estimates place the average cost of a supply chain cyber-attack at £3.5 million, factoring in operational downtime, lost revenue, and remediation expenses.
- Survey data suggests that 60% of automotive suppliers feel inadequately prepared for a significant cyber incident, underscoring persistent gaps in cyber resilience across the sector.
- Globally, customer confidence in affected brands drops by an average of 22% following a publicised data breach, with long-term effects on loyalty and market share.



## Lessons learned

### **Supply chain visibility is crucial:**

businesses must have a comprehensive understanding of their digital supply networks, including third-party risks, to anticipate and mitigate vulnerabilities.

### **Cyber incidents are no longer outliers:**

the frequency of attacks highlights the necessity of treating cyber resilience as an ongoing strategic priority rather than a box-ticking exercise.

**Customer trust is fragile:** transparent communication and swift incident response are essential to maintaining customer relationships in the aftermath of a breach.

### **Investment in prevention pays**

**dividends:** proactive security investments - ranging from staff training to advanced threat detection - yield substantial returns by preventing costly disruptions.

## Steps for cyber resilience

### **Assess and map supply chain risks:**

conduct thorough risk assessments of suppliers and critical dependencies, prioritising those with access to sensitive systems or data.

### **Implement multi-layered security**

**measures:** deploy a combination of endpoint protection, network segmentation, and anomaly detection to reduce attack surfaces.

### **Strengthen third-party security**

**standards:** include cyber security requirements in vendor contracts and regular audit compliance.

### **Enhance incident response plans:**






prepare and regularly test response protocols, ensuring clear lines of communication with suppliers and customers.

**Invest in staff training:** educate employees and partners about phishing, social engineering, and other common attack vectors.

**Adopt industry frameworks:** Align with standards such as ISO 27001 or NIST to benchmark and continuously improve cyber maturity.

**The recent cyber-attacks on Jaguar Land Rover, Renault, and other major UK brands like M&S and Co-op are a wake-up call for all organisations operating within complex supply chains.**

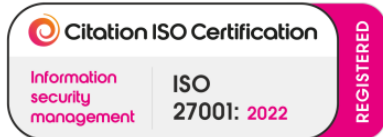
# Equity's comprehensive cyber-security solution

<b>Microsoft 365 Business Premium</b>	Implements advanced identity management controls, including policy based multi-factor-authentication (which must be enabled), along with enhanced security and endpoint (protection for your device) detection and response (EDR).	
<b>Managed Detection and Response (MDR)</b>	<p>Provides the capability and power of a Security Operations Centre (SOC) without the cost of one. Includes features such as user and identity behaviour analytics, compliance reporting, and threat intelligence in real-time, which is monitored by actual human beings 24x7. Malicious activity often happens out of hours, without MDR it could be up to 16hours before a traditional EDR product detects a breach at the device level, by which time it is too late. MDR monitors not just your devices, but also your 365 environment and can also be extended to the firewalls on your network.</p> <p>The Microsoft Business Premium license provides the baseline level of protection, while MDR (Managed Detection and Response) delivers remediation capabilities in the event of a breach. Equity now recommends this as the minimum standard for all customers. Given that email and web browsing are among the most common attack vectors, customers are strongly encouraged to enhance this baseline by implementing the following additional security solutions to further reduce their risk of a breach.</p>	
<b>Egress Defend</b>	Enhanced email security which proactively scans every email coming into an organisation using a combination of both heuristics and artificial intelligence to help ensure legitimacy.	
<b>Web Protection</b>	All internet activity is sent via advanced traffic analysers to check that the website is genuine and does not contain any harmful code or malware. It is also a good way of blocking access to sites of poor taste, and other productivity-degrading internet-based destinations.	
<b>Cyber Essentials</b>	<p>Equity recommends that all businesses work toward achieving Cyber Essentials compliance - a minimum-security baseline endorsed by HM Government.</p> <p>We offer this certification through the CyberSmart platform, which simplifies the process of attaining and maintaining Cyber Essentials or Cyber Essentials Plus certification each year.</p> <p>In addition to compliance support, CyberSmart includes cyber awareness training for staff and cyber insurance coverage up to £250,000 (Oct 25) in the event of a security breach, providing both preventative and responsive protection.</p>	

# ACT NOW

Business leaders and IT professionals must act now to assess vulnerabilities, strengthen defences, and foster a culture of cyber resilience. By doing so, they not only protect their own operations, but also safeguard the trust and confidence of their customers in a digital world.

**ALL businesses are at risk of cyber-attacks and having at least our recommended minimum security measures is essential.**



**CONTACT EQUITY TO DISCUSS  
YOUR IMMEDIATE MINIMUM  
SECURITY REQUIREMENTS**

**0330 3331 888**  
**[enquiries@equity-it.co.uk](mailto:enquiries@equity-it.co.uk)**  
**[www.equity-it.co.uk](http://www.equity-it.co.uk)**

**Equity**  
**Proxima**  
**1 Grenfell Road**  
**Maidenhead**  
**SL6 1HN**

