Red Helix

Retail Security: Protecting Your People, Products, and Profits

A practical guide to understanding your current levels of protection, with steps you can take to a multi-layered approach to security.

CONTENTS

DIGITISATION AND CYBER RISK IN THE RETAIL SECTOR

Retail is among the most rapidly digitised industries, driven by customer expectations and operational demands. The sector has embraced modern technologies to meet evolving consumer expectations, manage increasingly complex operations, and compete in a marketplace that never stands still. Retail businesses are more connected than ever via e-commerce platforms, cloud-based systems, digital point-of-sale solutions, and more.

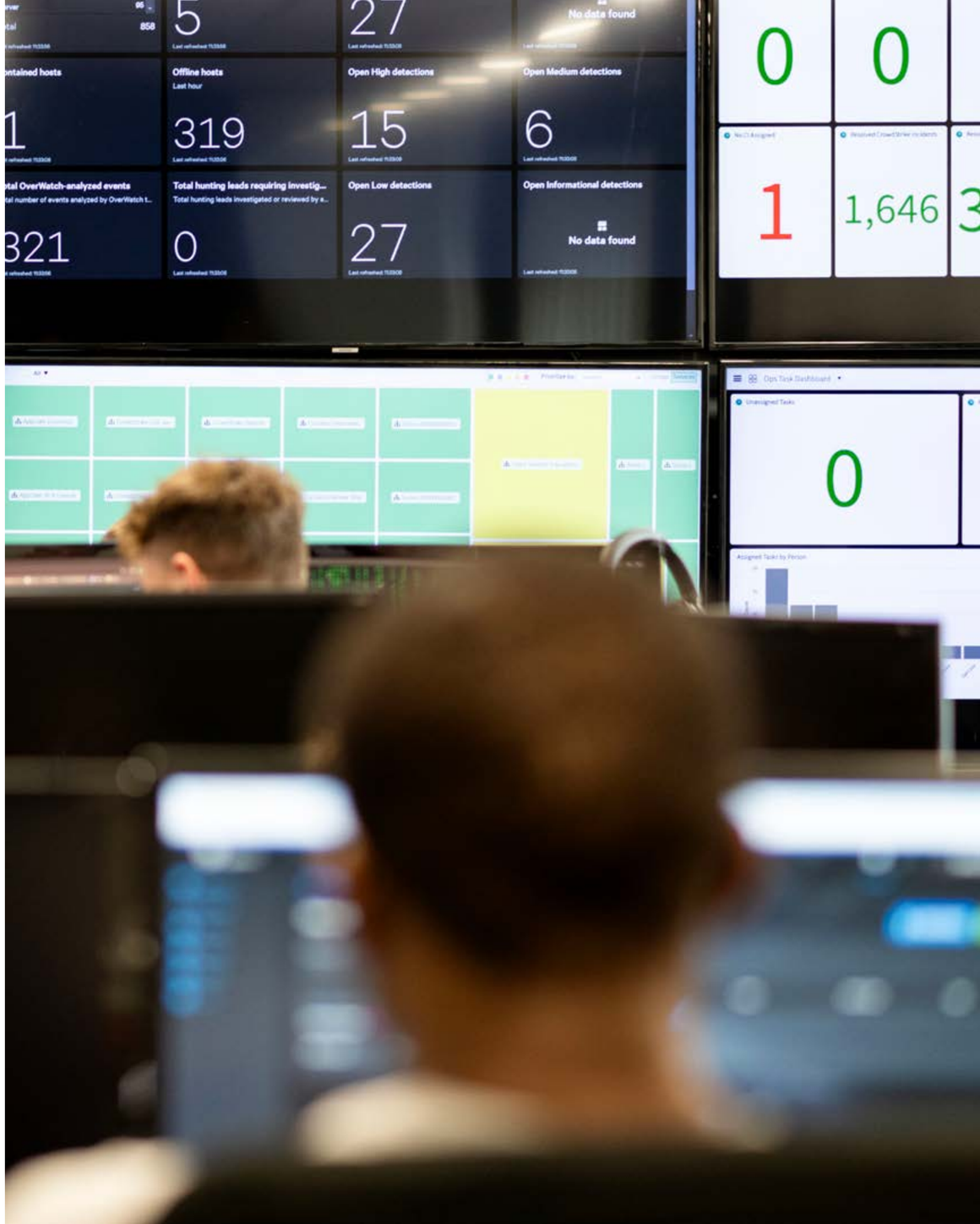
This transformation has been driven not only by innovation but also by necessity. Over the past couple of years, many organisations have moved away from manual, localised systems, and instead opt for hybrid and digital replacements. New, centralised, cloud-hosted tools are adopted as they offer better flexibility, faster decision-making, and enhanced customer experiences.

Retailers' increased reliance on digital systems also expands their exposure to cyber threats. Sensitive customer information, financial records, loyalty data, supply chain access points, and operational platforms are all part of an extended digital footprint that cyber criminals actively target. Retailers have become high-value targets due to the volume and variety of data they process daily, as well as the complexity of their customer/vendor ecosystems, which often involve third-party software, logistics partners, and payment processors.

We have also seen a growing presence of automation in cyber-crime. Bots are being employed to probe for system weaknesses, and enhanced phishing campaigns are now engineered with psychological precision. Cumulatively, this means that retail organisations must think beyond historic defences. It is no longer sufficient to only react when incidents occur.

Cyber risk is now considered a business risk, due to its vast implications for customer trust, brand reputation, and operational continuity. Protecting your organisation calls for cultural change, strategic foresight, and ongoing investment in both people and technology.

This white paper provides a practical starting point for retail leaders seeking to understand and improve their cyber security. It outlines how to identify weaknesses, implement better safeguards, and foster a workplace where digital security becomes part of everyday thinking. As a result, it aims to enable retailers to innovate as needed, while still protecting customer trust and operational continuity.



IS YOUR ORGANISATION CYBER-RESILIENT?

How strong is your cyber security posture?

In today's retail environment, the strength of your cyber security is a fundamental business concern. As retailers expand digital capabilities to meet customer expectations and streamline operations, their infrastructure becomes more exposed to cyber threats.

Although most retail organisations recognise the importance of cyber security, implementing the right mix of tools, processes, and training remains a challenge. The marketplace has become saturated with vendors, and the landscape is quickly evolving. It is often unclear which solutions are effective, and which are adding unnecessary complexity. Many retail leaders find themselves unsure whether their security stack is keeping pace with the risks.

To build genuine resilience, retail businesses must adopt a multi-layered cyber security strategy that spans governance, users, applications, and network infrastructure. Each of these areas requires active management and alignment with both technical capabilities and the day-to-day realities of running a customer-facing business.

A multi-layered approach is necessary to protect your company	
Governance	**1** Perform regular, thorough risk assessments **2** Maintain compliance **3** Stay informed of cyber trends **4** Prepare your response **5** Allocate budget and resource
End User	**6** Multiple device endpoint protection **7** Email malware filtering **8** Cyber awareness training **9** Spoofing protection **10** Monitoring Access Management
Applications	**11** Check your software updates **12** Review outdated technology **13** Monitor logs in-depth
Network	**14** Test your public and private networks **15** Upgrade from VPN to ZTNA models **16** Manage your firewall

The key steps to strengthening your cyber defences

Governance

1 Perform regular, thorough risk assessments:
Identify and document potential threats to your retail systems, especially POS devices, e-commerce platforms, and supply chain software. Repeat this quarterly to keep pace with threats.

2 Maintain compliance:
In the retail sector, adherence to standards such as PCI DSS are important. Review the regulations around BYOD (bring your own device), cloud storage, vendor access, and customer data handling.

3 Stay informed about cyber trends
Reputable sources such as the NCSC and the British Retail Consortium are important fonts of information.

4 Prepare your response:
Practice incident response plans regularly, using scenarios such as e-commerce site defacement or ransomware locking down EPOS systems.

5 Allocate budget and resource:
The 2025 Marks & Spencer cyber attack led to **an estimated £40 million a week in lost sales.** Budgeting for cyber defence is no longer optional, consider outsourcing to an MSSP if your organisation's in-house resources are stretched.

End User

6 Multiple device endpoint protection:
Retail environments rely on multiple endpoints, across POS devices, and mobile devices, tablets, and tills used on the shop floor. These endpoints must be secured, especially as we have seen cyber criminals gain access through endpoint infiltration, which in 2023, resulted in a successful ransomware attack on Clarks Shoes.

7 Email malware filtering:
Email is still the most common delivery mechanism for malware. In retail, attackers often impersonate suppliers or customer service contacts to trick staff into clicking malicious links.

8 Cyber awareness training:
Training both HQ and in-store staff on phishing risks, suspicious requests, and secure password practices are paramount.

9 Spoofing protection:
Protect your domain from spoofing, especially as attackers target your customers by imitating retail brand communications. **During the 2023 festive season, Amazon customers were targeted** by fake order confirmation emails leading to credential theft.

10 Monitoring Access Management:
Access for temporary and seasonal workers needs to be paid close attention as they increase access risk. Retailers with high staff turnover should ensure offboarding processes are watertight.

Applications

11 Check your software updates:
Ensure POS software, e-commerce platforms, inventory systems, and internal apps are all patched regularly.

12 Review outdated technology:
Old tills, scanners, and back-office servers often cannot support modern security protocols. Upgrading these reduces vulnerabilities and long-term support costs.

13 Monitor logs in-depth:
In 2023, Mango identified credential stuffing attempts only after reviewing web logs. This proves the importance of monitoring tools like SIEMs. They can identify malicious patterns across customer transaction systems, loyalty platforms, and third-party integrations.

Network

14 Test your public and private networks:
Run penetration tests on in-store Wi-Fi, online platforms, and warehouse networks. Often public Wi-Fi networks are exposed to access or improperly segmented.

15 Upgrade from VPN to ZTNA models:
Zero Trust Network Access (ZTNA) is becoming vital for large retail networks, especially when connecting distributed stores and third-party contractors. It follows the Zero Trust principles, allowing least privileged access to ensure only authorised users can gain visibility of specific data for a limited time. In comparison, legacy VPNs can create lateral movement risk if compromised.

16 Manage your firewall:
Ensure firewalls are segmenting in-store systems from customer Wi-Fi, e-commerce platforms from finance systems, and blocking unnecessary access to internal retail tools.

Retail organisations are under mounting cyber pressure. High transaction volumes, sensitive customer data, and growing reliance on digital systems make the sector a prime target for cyber attacks. In fact, a 2024 IBM report noted that the retail industry was the second most targeted sector globally, with ransomware, business email compromise, and supply chain intrusions leading the types of threat.

To strengthen your organisation's cyber resilience, the following actions should be prioritised across governance, users, applications, and networks.

Choosing the right cyber protection for retail environments

Retailers cannot afford to treat cyber security as a generic function. The threats are real, the consequences are immediate, and the cost of both reputational and operational downtime is growing. Cyber resilience is not about size; it's about your organisation's preparedness and readiness. As we have seen, no retail organisation is too large or too small to be targeted.

Especially in the retail sector, protecting your businesses endpoints, emails, and vendor access points are now critical infrastructure, serving as common entry points for cyber criminals. Employing managed services such as Red Helix can bridge expertise and capacity gaps in internal IT teams as we can support you with Email Security Protection, EDR, NDR, SIEM and ZTNA, with service levels shaped for your organisation.

Ransomware

The threat: Retailers have become a prime target for ransomware groups because they are highly visible and hold high-value data (customer, payment, inventory). These attacks have become automated, indiscriminate, and opportunistic.

Any organisation can fall victim. Chilled food distributor Peter Green suffered a ransomware attack that impacted deliveries to major supermarket chains, as operations and supply chain coordination were disrupted. This proves how an attack on a single supplier can ripple across the sector.

The solution: To limit the impact of ransomware, retailers need Anti Ransomware protection. This tooling you can stop ransomware without extra costs or resources. It includes prevention, detection and remediation capabilities with little to no downtime.

Another solution lies with Endpoint Detection and Response (EDR) which continuously monitors devices for threats and respond in real time. Both can be used separately or in conjunction to protect and prevent ransomware affecting your organisation.

Phishing and spoofing

The threat: Phishing remains the most prevalent cyber-attack vector, and in retail, the stakes are even higher. With high staff turnover and a mix of front-line and back-office employees, attackers often exploit low awareness and inconsistent device use.

In 2023, JD Sports disclosed a data breach affecting 10 million customers, believed to have originated from a phishing email. Similarly, Harrods experienced attempted spoofing attacks on its customer service communications in 2024, aimed at intercepting customer responses during high-sales periods.

The solution: Cyber awareness training is essential to educate your employees about phishing threats, especially during seasonal surges or promotional campaign periods. Email Security Protection adds a vital second layer, it scans attachments, blocks impersonation attempts, and neutralises credential-harvesting links before they reach inboxes. These defences are crucial to protect both customer data and your brand reputation.

Attacks on Third Parties

The threat: Retailers rely on an extensive web of suppliers, technology partners, and payment providers. This interconnected ecosystem creates significant third-party risk.

A stark example came when a supply chain attack on Blue Yonder disrupted operations for UK retailers including Morrisons and Sainsbury's.

The solution: Zero Trust Network Access (ZTNA) is a modern, scalable approach to secure internal systems and extend safe access to third parties. It guarantees users only have the necessary visibility, so the rest of the network remains hidden and protected. This is especially valuable when working with outsourced services or temporary partners during peak trading periods.

Implementing other common practises such as Multi Factor Authentication (MFA) policies also contribute to creating a robust security culture within your business.

44%

of UK businesses have basic technical cyber security skills gaps

Addressing the cyber security skills gap

In the face of this talent gap, more retail companies are turning to Managed Security Service Providers (MSSPs) to shore up their defences. MSSPs offer continuous monitoring and incident response, access to cutting-edge threat intelligence, support with regulatory compliance, and the expertise needed to identify and respond to the latest attack vectors. This outsourcing model allows retailers to maintain a strong cyber posture without the overheads of building large in-house teams, particularly in a market where cyber expertise is scarce and expensive.

However, not all providers are created equal. It's increasingly important for retail businesses to partner with MSSPs that are not simply IT generalists offering cyber as a bolt-on. Instead, retailers should seek out firms with a proven track record in delivering core cyber services, with deep sector understanding and the ability to support highly specific retail use cases, whether that's securing online point-of-sale systems, protecting supply chains, or managing customer data in compliance with GDPR and PCI DSS standards. The right MSSP partner ensures that businesses remain secure, compliant and resilient, even without large internal security teams in place. As a result, your organisation is afforded protection and peace of mind.

The UK retail sector is grappling with a significant cyber security skills gap, underscoring the critical need for robust cyber defences and access to qualified professionals. This shortfall equates to more than 600,000 businesses lacking the internal capabilities needed to manage even fundamental cyber hygiene practices. Due to its extensive digital infrastructure and high volume of customer data handling, the retail sector is particularly vulnerable.

The key benefits of working with the right MSSP

1. 24/7 Threat Monitoring Across Distributed Retail Environments: MSSPs offer continuous monitoring of in-store systems, eCommerce platforms, mobile apps, and POS networks, identifying suspicious activity in real time. This is particularly critical for retailers operating extended hours or with geographically dispersed locations, where internal monitoring capacity may be limited.

2. Access to Enterprise-Grade Security Tools Without the Capital Investment: Retailers gain access to leading security platforms such as EDR, NDR, SIEM, and web application firewalls (WAF). These are vital for protecting the customer-facing technologies, but is often resource-intensive to deploy independently.

3. Sector-Specific Threat Intelligence and Expertise: MSSPs familiar with the retail threat landscape can rapidly identify and neutralise risks such as card skimming, e-skimming, credential stuffing, and loyalty fraud.

4. Rapid Incident Containment to Protect Revenue and Brand Trust: MSSPs provide structured incident response that ensures swift containment, communication, and recovery. This is essential during peak trading periods or major sales events.

5. Predictable, Scalable Cost Structures to Support Tight Margins: With fixed monthly fees and scalable service levels, MSSPs help retail organisations manage cyber security without unexpected costs, supporting financial planning in a low-margin, high-volume business model.

6. Automated Patch Management for POS and Backend Systems: MSSPs ensure timely patching of vulnerabilities in retail software and hardware, including legacy POS systems and third-party plugins used in eCommerce. This reduces exposure to attacks exploiting outdated technology.

7. Support for Regulatory Compliance and Industry Standards: Retailers face strict requirements under PCI DSS, GDPR, and consumer data protection laws. MSSPs assist in maintaining compliance through continuous auditing, data encryption best practices, secure customer authentication processes, and breach notification procedures.

8. Operational Efficiency for In-House Teams: teams to focus on strategic digital transformation, store innovation, and customer experience improvements. as daily tasks such as threat monitoring, log analysis, and incident response are offloaded onto the MSSPs, enabling internal IT and security capabilities.

9. Visibility Across Omni-Channel Retail Infrastructure: MSSPs consolidate security telemetry from all customer touchpoints, from online platforms, mobile applications, IoT devices, kiosks, and in-store systems. This provides retailers with centralised, real-time insight into their cyber risk posture.

10. Proactive Defence Through Retail-Focused Threat Intelligence: Leading MSSPs incorporate global and sector-specific threat intelligence into their monitoring systems, helping retailers stay ahead of seasonal threats, new ransomware variants, and supply chain attacks targeting retail software vendors.

WHAT RETAILERS NEED TO KNOW ABOUT CYBER INSURANCE

Cyber insurance is not a preventative measure, nor can it restore stolen data or undo reputational damage. However, it is a financial defence to mitigate the losses incurred during a cyber incident. Therefore, understanding the limitations and evolving nature of cyber insurance is essential.

Historically, cyber insurance has served to offset the costs associated with a breach such as forensic investigations and compensation for affected consumers. For example, when in August 2023, **up to 300 independent UK retailers across various sectors were impacted by a cyber attack on IT supplier Swan Retail.** The breach compromised back-office systems, hindering online trading and order fulfilment capabilities.

The increasing frequency and sophistication of cyber attacks have led insurers to reassess their risk exposure. As a result, cyber insurance policies are becoming more expensive and harder to obtain. Insurers are imposing stricter underwriting criteria, often requiring evidence of robust cyber security measures such as multi-factor authentication, endpoint detection, and employee training programs. Failure to meet these standards can result in denied coverage or reduced payouts.

Moreover, insurers are introducing more exclusions in their policies. Notably, some UK insurers have introduced clauses that exclude coverage for incidents attributed to “state-sponsored” attacks, reflecting concerns over the increasing frequency and severity of such attacks.

Given the diminishing likelihood of full compensation and the rising expectations from insurers, the imperative for strong cyber security has never been greater. Retail organisations must prioritise resilience, employee awareness, and strategic planning as a prerequisite for coverage and a defence against growing cyber threats.

In today’s climate, cyber insurance is not a standalone solution, it is simply a vital aspect of a layered risk management strategy.

RETAIL CYBER HYGIENE: PRACTICAL IMPROVEMENTS YOU CAN MAKE TODAY

Despite advancements in digital defences, the human element remains a critical vulnerability in retail cyber security. Social engineering attacks occur when adversaries manipulate individuals into compromising security protocols. The National Cyber Security Centre (NCSC) has emphasised the seriousness of these incidents, categorising them as organised crimes rather than isolated events. This method has become increasingly prevalent involving sophisticated social engineering methods which pose significant risks to retailers.

In early 2025, **the UK retail sector experienced a 74% increase in ransomware attacks in Q1 alone.** Notably, major retailers such as Marks & Spencer and The Co-operative were targeted by the cyber criminal group Scattered Spider. M&S faced significant disruptions, including the suspension of online orders and in store offers, resulting in an **estimated £3.8 million loss in online sales per day and a £700 million decrease in market value**.

The financial repercussions of these types of attacks in the retail sector are substantial. Beyond immediate revenue losses, **UK retailers are encountering premium hikes of up to 10%,** following the string of high-profile attacks in early 2025. Insurers are reassessing the entire sector’s risk profile and consequently, all are facing increased cyber insurance premiums.

WHY CYBER PROTECTION IS CRITICAL FOR YOUR BUSINESS' SUCCESS

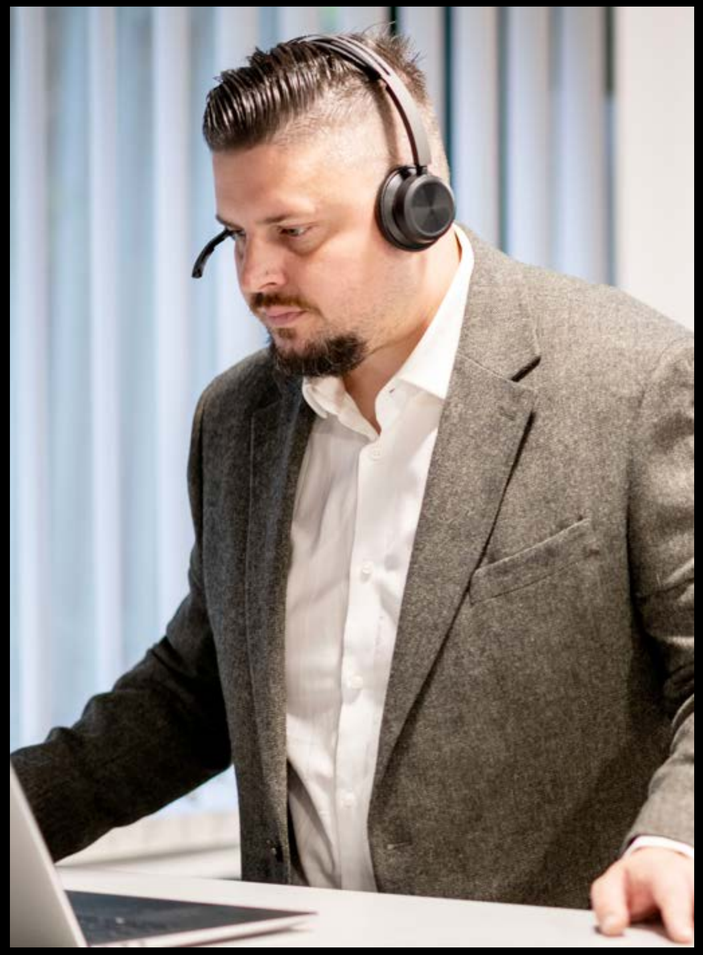
Cyber-crime poses one of the most serious risks to UK retailers today. In 2023, the sector faced estimated losses of £11.3 billion from cyber attacks, fraud, and data breaches. Businesses in the luxury and fashion retail space were among the hardest hit, with average losses reaching into the millions.

A notable incident occurred in September 2024, when Harvey Nichols reported unauthorised access to its systems, resulting in a data breach that affected customer information. While the company stated that the compromised data was non-sensitive, such events can significantly damage customer trust and raise questions about the adequacy of current defences. Around the same time, UK authorities began investigating the hacker group known as Scattered Spider, which has been linked to a series of targeted attacks on British retail organisations in 2025 using advanced infiltration techniques and
social engineering.

Whilst there has been a trend of growing awareness around cyber risks, there are still many retailers continue to underestimate the complexity of modern cyber threats. Cyber security must be treated as an ongoing and dynamic process, requiring regular assessment of systems, technologies, and internal processes.

All staff must understand the risks and recognise their individual responsibilities in protecting sensitive information. Many of the most damaging breaches in recent years have originated from simple errors, such as clicking on phishing emails or using weak passwords, that could have been avoided with proper training and oversight.

Maintaining strong cyber security practices is essential for retail organisations, ensuring compliance and risk mitigation, and maintaining long-term customer confidence and commercial resilience.



This white paper has outlined several practical steps and innovative security solutions that can be used as a starting point to improve the protection offered by your organisation, but it is an ongoing battle which will require continuous attention.

For further support, we can assess your current level of security and help to implement the cyber solutions and practices
you need.

To discuss how to provide better protection to your firm, employees and clients, contact Red Helix for a free, no obligation consultation.

Simply enquire at www.redhelix.co.uk/contact and one of our team will be in touch to discuss how we can support you.

+44 (0)1296 397711

info@redhelix.co.uk

Phoenix House
Smeaton Close
Aylesbury
Buckinghamshire
HP19 8UW

Red Helix

redhelix.com