knowbe4

IT and Cybersecurity Trends in UK Retail

WWW.KNOWBE4.COM

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

02590925

Inside this Report

03 Executive Summary

05 The Retail Landscape

06 Rising Cyber Threats and Areas of Concern

07 Executive Response Requires Greater Attention, Budgets and Employees

08 Key Investment Areas in IT Security

09 Proactive Audits and Incident Preparedness

10 Ransomware Readiness and Recovery Strategies

11 Confidence Levels and Executive Attitudes

12 Securing Retail Through Human Risk Management

Executive Summary

A 2025 survey of 250 UK retail IT security professionals reveals a sector on high alert. In the wake of major cyberattacks affecting household brands like Marks & Spencer, Co-op and Harrods, the retail industry is responding with increased investment, greater executive attention and stronger preparation efforts. But beyond technical controls, the survey underscores the growing importance of Human Risk Management (HRM) as a strategic pillar of cyber resilience.

Key findings

Threats are escalating sharply

Nearly all respondents reported increases in phishing, fraud, supply chain exploitation and social engineering attacks. Helpdesk scams and credential theft attempts were among the most common threats. Only 0.4% reported no increase in threats.

Supply chain is a major vulnerability

A significant 46% of respondents identified third-party suppliers as their biggest cybersecurity gap, highlighting the importance of extending HRM strategies beyond the perimeter to partners and vendors.

Security budgets and leadership attention have grown

The majority (72%) reported greater management focus on cybersecurity, 62% have hired more security staff and 58% have increased budgets. This reflects a board-level shift in how cyber risk is prioritised.

Human-centric controls lead investment

The top investment area was security awareness training (74%), followed by email security (69%) and risk assessment tools (64%). This marks a clear recognition that human behaviour remains a frontline risk - and opportunity.

Culture over compliance

Education alone isn't enough. Retailers are increasingly aware that empowerment, culture and decision-making environments are critical to secure behaviours. The emergence of AI-enhanced cyber threats adds new dimensions to an already complex cybersecurity environment, which requires thoughtful preparation and response.

Proactive audits and response planning now widespread

A huge percentage (91%) of retailers conducted formal security reviews and 96% have an incident response plan, though only 65% have tested them in practice.

Ransomware budgets reflect pragmatic risk planning

Though generally discouraged, the reality is that 71% of retailers have set aside dedicated budgets for potential ransom payments, showing a controversial but realistic acceptance of ransomware as a business continuity threat.

Security leaders are confident but should avoid complacency

A whopping 94% of IT leaders say they are confident in employees' ability to make secure decisions and 90% are confident in their current cyber strategy. However, a previous global study this year indicated that as many as 50% of employees have fallen for a cyberattack. Therefore, overconfidence can create new risks unless resilience is continually tested and reinforced.

Retailers are no longer treating security solely as a technology problem, they are investing in the human layer in the form of security awareness training which is encouraging. Yet, it shouldn't stop there. Changing behaviours and improving secure decision-making demands a cultural shift towards managing human risk throughout the entire lifecycle of policy, training, tooling and daily operations. In a sector where cyberattacks are increasingly targeting people, not just infrastructure, those that embed HRM into their strategy will ultimately be the most resilient.

The emergence of AI-enhanced cyber threats adds new dimensions to an already complex cybersecurity environment, which requires thoughtful preparation and response.

The Retail Landscape

The UK retail sector has become a prime target for cyberattacks, with multiple high-profile breaches garnering headlines in early 2025 including incidents at Marks & Spencer, Co-op, Harrods and even global brands like Adidas and Victoria's Secret. This wave of attacks has laid bare the operational and financial risks that arise as a result of cyberattacks. For example, Marks & Spencer reportedly halted online orders for weeks and estimated losses up to £300 million from a ransomware hack.

Against this backdrop, a new survey of 250 UK retail IT security professionals (conducted June 2025 by Censuswide) reveals how the industry is responding. The data highlights surging cyber threats and the corresponding shifts in investment, executive focus and confidence levels among retail IT leaders. The report analyses the top trends and standout figures from the survey, connecting them to the broader context of escalating cyberattacks in UK retail and applying a Human Risk Management (HRM) lens to understand how organisations are empowering their people and building security-aware cultures.

Rising Cyber Threats and Areas of Concern

Survey respondents overwhelmingly reported an increase in cyber threat activity over the past year. Nearly every participant noted upticks in one or more attack vectors, especially social engineering and third-party attacks. The most commonly heightened threats were:

58%

Helpdesk/IT support scams (password reset scams, etc.) were experienced more by about 58% of organisations

54%

Fraud and credential theft attempts increased for 54% of retailers

48%

Attacks via third-party suppliers/ partners were experienced more by almost half of respondents (48%)

47%

Phishing targeting employees was seen by 47%

47%

Malicious email attachments were noted by 47% of respondents as a growing threat

Organisations reported increases across multiple threat types. Between 27% and 46% of respondents cited growing concerns about AI-driven deepfakes, business email compromise, and insider threats. Perhaps most telling, only 0.4% of respondents reported no increase in cyber threats. Suggesting almost everyone is experiencing more attacks.

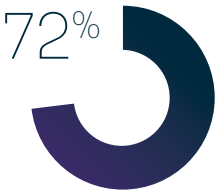
This aligns with broader research. Industry-wide, it has been reported that 75% of organisations saw cyberattacks rise in 2024 and government data shows 74% of large UK businesses had a breach in the past 12 months. In retail specifically, the supply chain stands out as a weak link, with 46% of retail security pros flagging third-party suppliers as the single biggest gap in their cybersecurity defences. Notably, the prolonged Marks & Spencer outage was traced to a phished third-party vendor, exemplifying this risk. Close behind, cloud infrastructure insecurities were cited by around 40% as a top vulnerability, followed by issues in identity management (38%) and inadequate email security (34%).

Retail IT teams see threats coming from many directions, with social engineering, supply chain exploits and phishing-based attacks dominating the threat landscape.

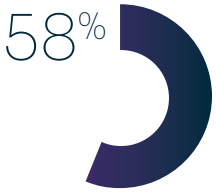
These threat vectors highlight the human dimension of modern retail cyber risk. Phishing, credential theft, and helpdesk scams all exploit human decision-making. While technical controls are critical, lasting protection depends on people being equipped, supported and empowered to detect and respond to threats. This reinforces the need to move beyond basic awareness to measurable behaviour change to ultimately create a resilient security culture.

Executive Response Requires Greater Attention, Budgets and Employees

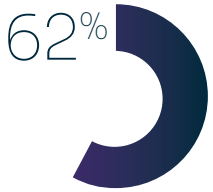
The survey indicates that the recent cyberattacks have triggered a strong executive and organisational response in the retail sector:



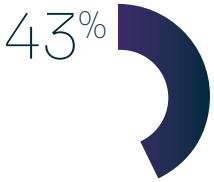
of respondents noted a significant **increase in upper-management attention** to cybersecurity.



have **boosted their security budgets**.



of organisations have allocated **more IT security employees**.

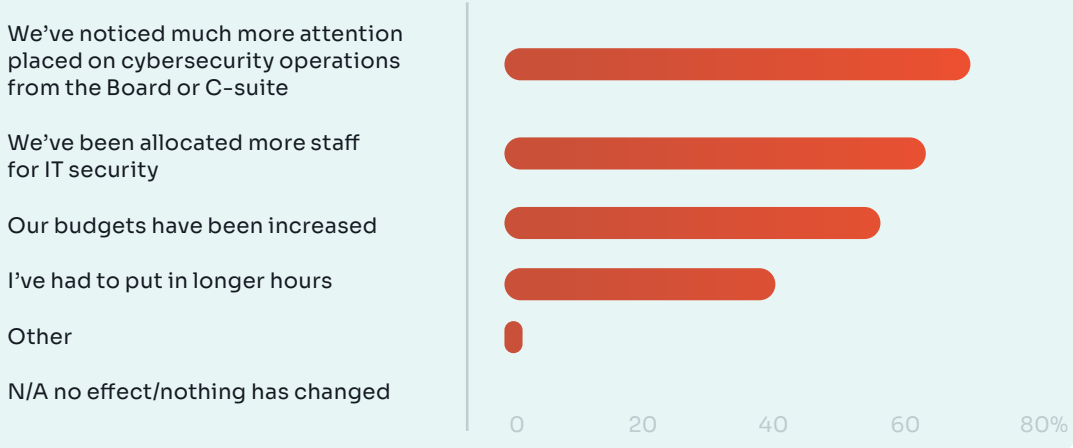


of security leaders said they personally have had to put in **longer work hours.**

No one reported “no effect” from the attacks; virtually everyone has seen changes, demonstrating how these breaches have become catalysts for transformation.

This increased executive attention is pivotal. When boards are engaged, they not only fund new technologies but also set the tone for cultural change. Security becomes a shared business priority, not just an IT concern. HRM flourishes when leadership supports frontline teams, enables secure choices and models security-conscious behaviour.

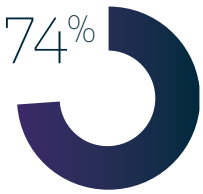
What effects have the recent retail attacks on Marks & Spencer and Co-Op had on your security operations, if any?



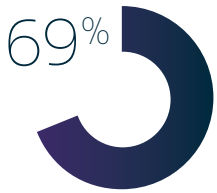
Key Investment Areas in IT Security

With new resources in hand, retail IT departments are channelling investments into specific cybersecurity capabilities. The survey asked which areas of cybersecurity have seen increased investment in the past year and the results reveal clear priorities.

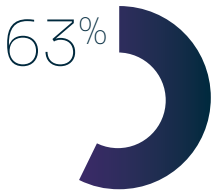
The top focus areas for investment, each cited by a majority of respondents, are:



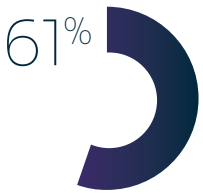
Security awareness training



Email security



Risk assessment tools



Supply chain security

Security awareness training reflects recognition that human behaviour remains the frontline of cyber defence. However, HRM extends this further: education alone doesn't ensure behaviour change. People need contextually relevant training, timely nudges and tools that make secure behaviour easy. Integrating human-centric security design with behavioural data and insights is essential.

This survey indicates that retailers are beginning to adopt an early stage HRM approach, combining education with improved technical controls (email, identity, and risk tools) and cultural change efforts. Investments are moving toward empowering secure choices, not just increasing knowledge.

What areas of cybersecurity, if any, have you placed more resources into in the past 6 months?

Proactive Audits and Incident Preparedness

Another standout finding is the near-universal commitment to proactively auditing security and preparing for incidents. In the aftermath of recent attacks, 91% of retail organisations say they have conducted a cybersecurity review or audit in the past year. Only about 9% had not done a review and virtually none were unsure, indicating that executives are insisting on formal security assessments across the industry. Such reviews often involve external experts or 'red team' exercises, and given how prevalent they are, it suggests a broad sweep of the sector is ensuring security controls are up to scratch.

Likewise, business continuity and incident response planning appear to be standard practice in retail IT. An overwhelming 96% of organisations have a cybersecurity incident response plan of some form already in place. However, the quality and maturity of these plans vary. About 65% of respondents say they have detailed plans that have been successfully tested (e.g. via drills or past incidents), and while this is a majority, clearly there is still some room for improvement with the remaining 30% that have plans partially or completely untested. Virtually no respondents admitted to not having a formal cyber incident plan - even those without a finalised plan are at least "in the process of developing" one (4% are currently working on plans).

Simulations, red teaming and crisis exercises that include realistic human factors, like phishing simulations or decision-making under stress, help bridge the gap between plans and practice. Retailers are demonstrating a level of maturity by not only having plans but also testing them with a view to continuous improvement.

The focus on resilience is further evidenced by the fact that 93% plan to re-evaluate their cybersecurity tools/solutions in the next 12 months to see if improvements or changes are needed. Continual re-evaluation indicates an agile, never-satisfied approach to security posture.

Ransomware Readiness and Recovery Strategies

One particularly striking insight is how many retailers are preparing for worst-case ransomware scenarios, including the possibility of paying attackers. The survey asked if organisations have a budget set aside for ransomware payments and 71% responded “Yes”.

In other words, nearly three-quarters (75%) of UK retail companies have a dedicated fund to pay ransom demands should their systems be encrypted by ransomware. Only about 28% said they do not have such a budget, and a tiny fraction (1%) were unsure. This finding underscores a pragmatic yet controversial strategy. Many retail executives prefer to plan financially for a potential ransom rather than be caught unable to restore operations during an outage. Given the recent spate of retail ransomware attacks, which in some cases forced businesses offline for extended periods, it appears organisations are hedging against downtime by ensuring funds are available to pay and quickly decrypt data if absolutely necessary.

Security experts often advise against paying ransoms, but the reality seems to be that when customer-facing operations are paralysed, business leaders want the option on the table.

The prevalence of ransomware budgets suggests that boards are having frank conversations about cyber risk trade-offs and are opting to transfer some risk via cyber insurance or earmarked reserves. It is a sober recognition that, despite all preventive efforts, a successful ransomware attack could still occur, and retailers prize rapid recovery to protect their brand and revenues (even if it means paying criminals in the worst case). On the flip side, the fact that 28% refuse to allocate a ransom fund may reflect either confidence in their defences, a principled stance against paying or reliance on backups and insurance alone.

Security experts often advise against paying ransoms, but the reality seems to be that when customer-facing operations are paralysed, business leaders want the option on the table.

Confidence Levels and Executive Attitudes

Despite the onslaught of threats, retail IT security leaders exhibit very high confidence in their organisations' cyber readiness. A significant 94% of retail IT leaders say they feel confident employees can make secure decisions and 90% are confident in their organisation's ability to withstand a targeted attack like those high-profile attacks on Marks & Spencer and Co-op. This optimism likely reflects recent investments and increased board-level support.

This high confidence comes at a time when investment in employee training is also at its peak, suggesting that leaders recognise the crucial role people play in cybersecurity. Rather than complacency, this may indicate a shift toward refining and sharpening existing employee capabilities, not simply filling gaps. Retailers are showing they understand that human behaviour is a linchpin in cyber defence and that continued investment is needed to sustain and enhance secure decision-making.

However, this high confidence should be viewed with a bit of caution. It is worth noting that many retailers still fell victim to breaches recently despite presumably feeling prepared, a reminder that no one is immune to cyberattacks. The UK government's Cyber Breaches Survey found 43% of UK businesses overall had a security breach in the past year, meaning even with strong defences, incidents do happen.

It's also likely that the retail security leaders' optimism may reflect overconfidence - which seems to be a recurring theme with similar studies over the past year - to some degree. Nonetheless, it is encouraging that none reported being outright unconfident; this likely means leadership engagement and risk management efforts have eased much of the pessimism that security teams sometimes face.

The survey results portray a collaborative executive mindset; boards are engaged, supporting their IT security departments with resources and, as a result, the security professionals feel empowered and fairly confident in their organisation's cyber resilience. HRM sharpens this insight as confidence must be tested and validated, not assumed. Simulated phishing campaigns, behavioural baselining and metrics that track actual risk reduction are key. Retailers must ensure that confidence is grounded in observed behaviour, not just perceptions.

Retailers are showing they understand that human behaviour is a linchpin in cyber defence and that continued investment is needed to sustain and enhance secure decision-making.

Securing Retail Through Human Risk Management

The 2025 survey reveals a UK retail sector that is actively fortifying. But beyond the technical fixes and boardroom strategy, a deeper transformation is underway, one that places human behaviour at the heart of cyber resilience.

Cyber threats are intensifying and phishing, fraud, and social engineering dominate the landscape. These are human-first attacks, requiring human-first defences. Retailers understand this, with security awareness training leading the way in investment priorities.

But awareness alone is not enough.

True resilience comes from empowering people to act securely, with the tools, culture and leadership support to make secure behaviours the default. That means:

- Designing systems and processes that make secure choices easier.
- Training that is role-specific, timely, and reinforced by behavioural science.
- Culture-building that celebrates good decisions and encourages reporting.
- Metrics that go beyond knowledge checks to track behaviour change.

This is Human Risk Management in action. It aligns people, processes and technology to reduce behavioural risk and enhance resilience. The high confidence levels seen in the survey are promising, but they must be continuously validated through measurement and improvement.

The survey findings suggest that UK retailers are on the right track, aligning people, process and technology to mitigate cyber risks. If the current momentum in cybersecurity investment and collaboration holds, the retail sector will be far more prepared to withstand the next wave of cyberattacks, maintaining customer trust and operational stability even in a challenging threat landscape.

Learn More

Methodology
KnowBe4 used Censuswide to survey 250 IT security professionals in UK retail companies with 50+ employees. The data was collected between the 3rd and 12th June 2025. Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Censuswide is also a member of the British Polling Council.

Free Phishing Security Test

Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program

Create a customized Security Awareness Program for your organization

Free Phish Alert Button

Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check

Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test

Find out if hackers can spoof an email address of your own domain

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk. For more information, please visit www.KnowBe4.com

knowbe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com