

Bridging the gap:

How retailers address physical and digital security



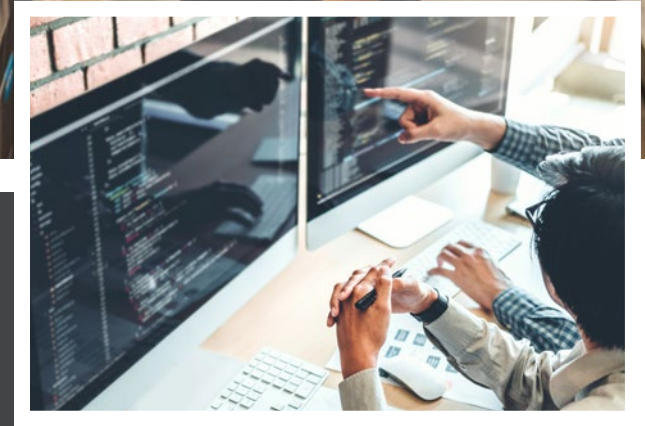
Introduction

With the frequency of security threats on the rise and criminal methods becoming increasingly sophisticated – whether targeting physical or digital stores – retailers are facing the dual challenge of ensuring both their in-store and cybersecurity strategies are in order.

As cyber-attacks become increasingly common, brands must prioritise the protection of consumer information – particularly given the detrimental impact a data leak can have on both consumer and employee trust. Meanwhile, in the physical store, retailers face pressure to identify and reduce inventory shrinkage and other losses caused by theft, fraud and clerical errors, whilst also providing a safe environment for their staff and customers.

While converging the physical and digital using the latest technologies can turn a retailer's security strategy into a competitive advantage in the long-term, rather than a cost, it's not always easy to achieve this.

The results of this report offer a representative snapshot of the key challenges and drivers currently facing the retail industry as companies carry out their physical and digital security strategies whilst addressing key considerations such as sustainability and cloud transformation.



Methodology

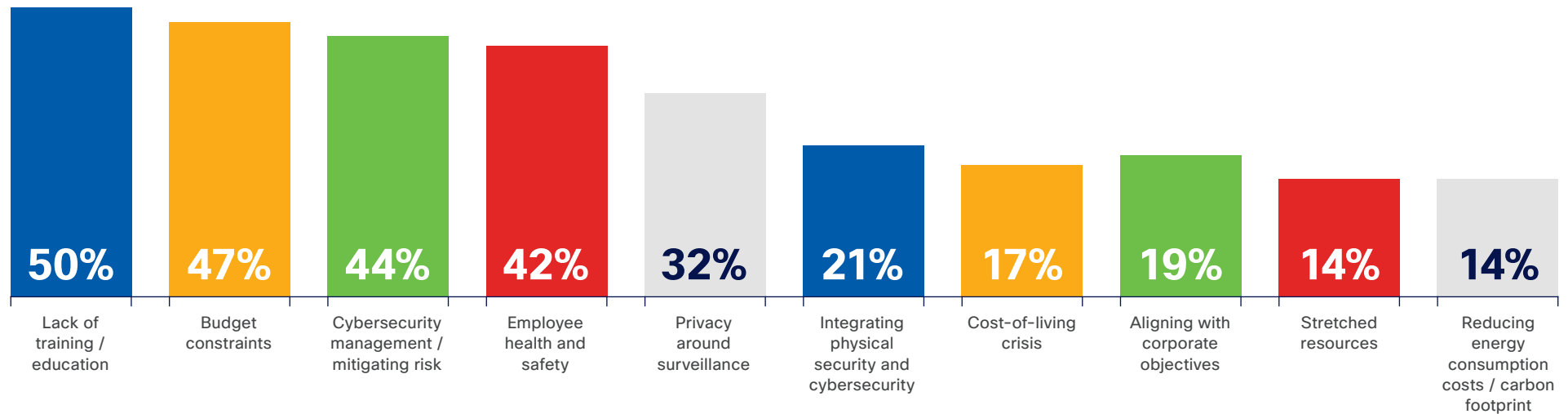
Retail Systems and Cisco Meraki conducted a survey of 100 retail professionals in the UK to assess the top priorities and hurdles for retailers as they attempt to manage and integrate their physical and digital security systems.

Contents

Q1	– Top challenges	4
Q2	– Major roadblocks to cloud security	5
Q3	– Physical security priorities	6
Q4	– Bridging the gap between digital and physical security	7
Q5	– Physical security technologies	8
Q6	– Sustainability targets	9
Q7	– Importance of sustainability when choosing new technology	10
Q8	– Barriers to rolling out physical security technology	11
Q9	– Physical security technology budget	12
Q10	– ROI	13

Q1. What are currently the top challenges for your organisation?

(select top three)



When retailers shifted their focus towards e-commerce during the pandemic and some back-office staff moved to hybrid working, it was a given that cyber criminals would take advantage of the widened attack surface. Given these pressures, which have continued beyond the pandemic, it's unsurprising to see that cybersecurity is a key concern for retail professionals in the UK.

Cybersecurity management or mitigating risk was highlighted as a top-three challenge for over two-fifths of respondents, while integrating physical security and cybersecurity has also been flagged as a problem for one in five retailers. With the right security solution, retailers can help address some of these challenges while continuing with their digital transformation without fear of a cyber incident leading to a data breach or ransom.

After shops reopened following the lifting of pandemic-related restrictions, retailers once again needed to prioritise preventing theft, as well as other threats like POS fraud, by monitoring their stores. Given this, plus privacy being a contentious topic

in today's society, it's not a surprise to see privacy around surveillance identified as a significant worry for almost a third of respondents.

While each of these challenges are unique, they all suggest that security - whether physical or digital - is something that many retailers are struggling with.

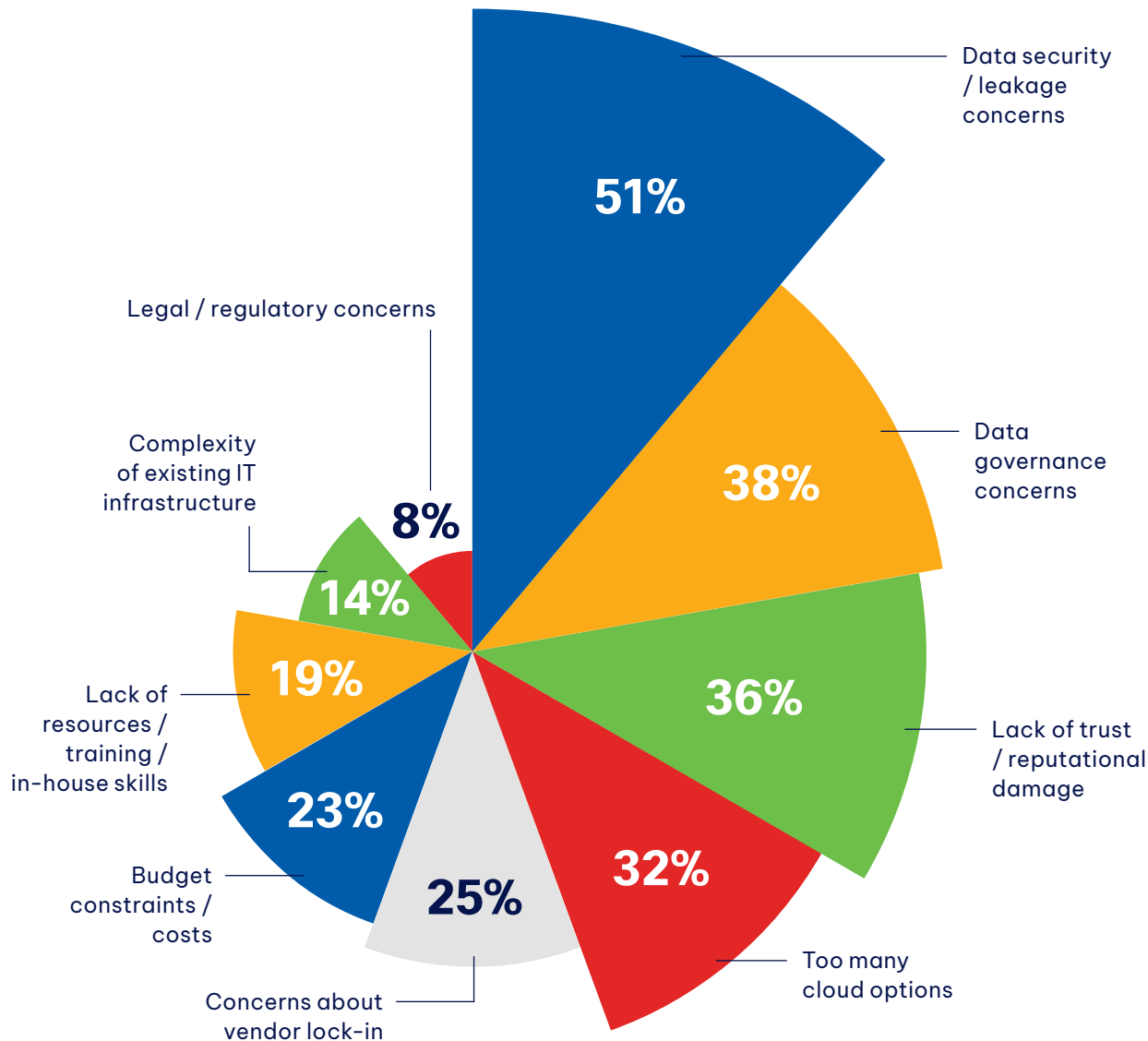
With wider trends suggesting that sustainability is a key concern for retailers and their customers, it's unusual to see that less than a fifth of those surveyed chose reducing energy consumption costs or carbon footprint as a top-three challenge. Some companies might already be on the road to implementing an ESG strategy, while for others, sustainability may simply not be a priority or something the firm is actively focused on and investing largely in right now - especially given the fact that retailers are facing thin margins and a poor consumer inflationary economy. These results could also suggest that some sustainability targets are more relevant to larger organisations which are obliged to do due diligence and must be seen to be leading the pack.

Leading global companies are also using sustainability as a market differentiator to gain a competitive advantage.

Lack of training or education across the organisation was also named as a big worry for retailers - with half of respondents choosing this option. Businesses are struggling to upskill and retain staff with key skills, but it's crucial that employees across departments - whether in merchandising, compliance, operations, information security, digital, or data - adapt to the constantly changing market through education. By delivering the right training content for both physical client-facing staff and back-office employees, a range of issues from theft in-store to phishing attacks can be avoided.

Almost 50 per cent of respondents said that they are currently concerned about budget constraints, reflecting an economic climate in which inflation has reached record highs and consumers face an ongoing cost-of-living crisis. Many retailers are bearing the brunt of rising costs in order to avoid passing these onto consumers, while others are holding back on investment to weather the storm.

Q2. What are the major roadblocks for your organisation in successfully rolling out a modernised cloud security strategy? (select all that apply)



While the general consensus is that retailers are finding a lack of training and budget constraints to be a challenge in their wider business, this is less of an obstacle when it comes to rolling out a cloud security strategy. The results of the survey could suggest that companies are relying on third-party providers to implement their strategy, so are not as concerned about education or costs.

The report demonstrates that many retailers are concerned about the data governance and security implications of moving highly sensitive data to a cloud security system. Their concerns are likely further driven by the fact that they are operating in a riskier security threat landscape during a time of unprecedented disruption.

Nearly two-fifths highlighted data governance concerns as a major roadblock to successfully rolling out a modernised cloud security strategy, while data security and leakage concerns was also identified as a key blocker, with over half choosing this option. And with more than a third worried about reputational damage, the results demonstrate that protecting customer data is an imperative for retailers. Data breaches and leaks can see retailers lose the trust they carefully build with their customers - which is the last thing they want.

However, an integrated, cloud-based platform can actually prevent these types of incidents by managing distributed workforces at scale - especially important given the shift to hybrid working - as well as keeping data safe on-premises, in the cloud, and in hybrid environments across the company's entire ecosystem, and detecting threats quickly throughout an organisation.

Q3. Which of the following are currently a priority for your organisation's physical security strategy? (select all that apply)

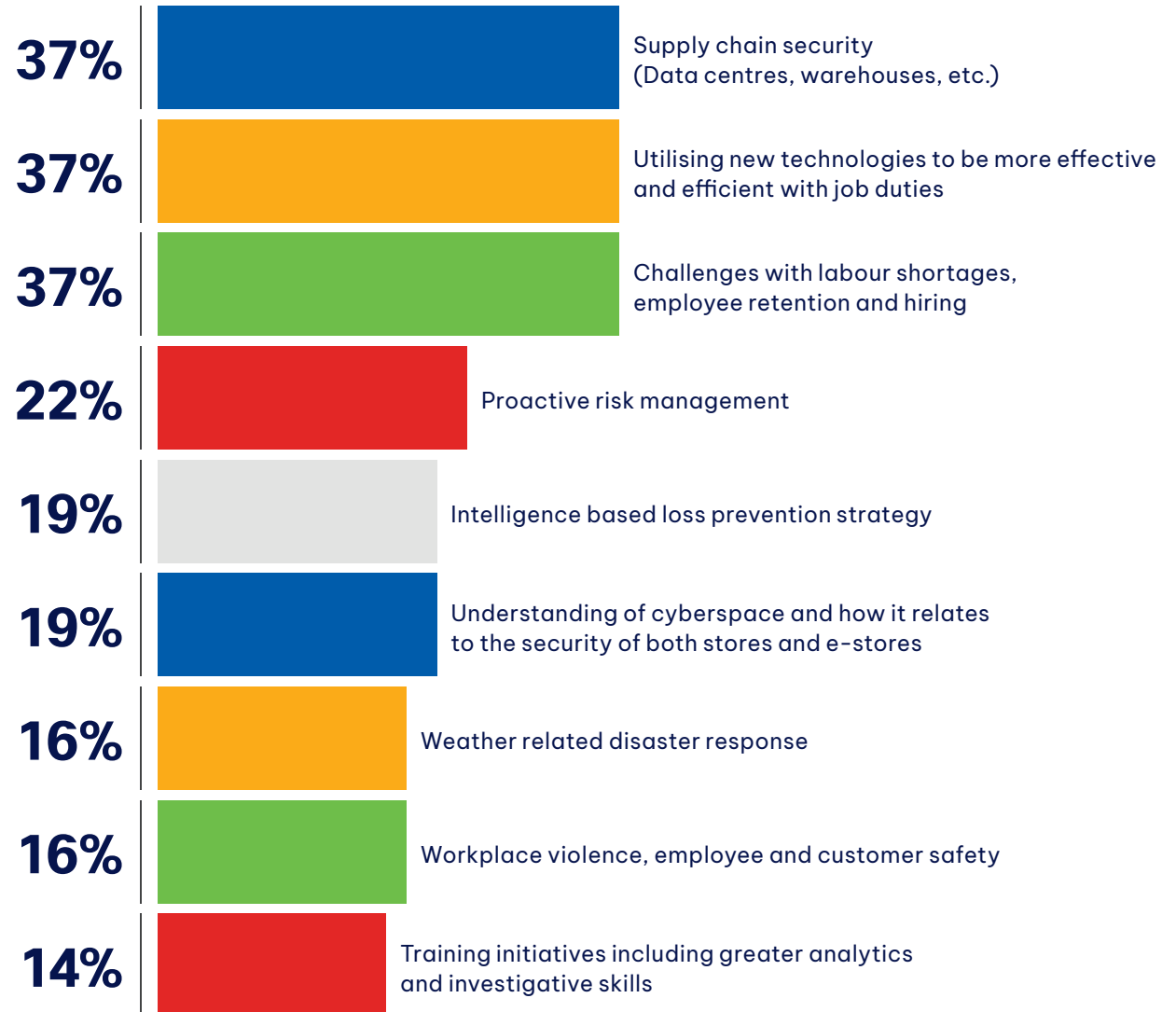
The top-three priorities for retailers when it comes to their physical security strategy are supply chain security, utilising new technologies, and addressing labour shortages – with all three options chosen by just under two-fifths of respondents.

As supply chains become increasingly complex, with an influx of huge change from Brexit, the cost-of-living crisis, and the Russia-Ukraine conflict impacting Europe and the UK, it is not a surprise that this is a priority area for retailers. If the security of one area of business is failing, this can have consequences for the entire supply chain.

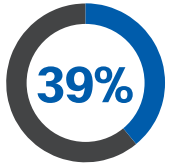


Ongoing labour shortages are also a very real problem for today's retailers, particularly as a wave of redundancies sweeps the market. Without the right staff, it's easy for mistakes to be made and impossible to implement a seamless security strategy.

It's promising to see that a fair number of companies – 37 per cent – are exploring new technologies to improve job duties. This is not a surprise given that automation is increasingly a priority for retailers, particularly when it comes to physical security.



Q4. What steps are you taking to manage the convergence of digital and physical security? (select all that apply)



Conducted vulnerability assessments



Establishing a convergence team



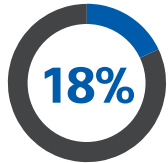
Limiting access to security systems



Increased collaboration between relevant departments



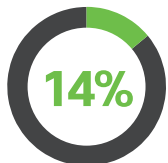
Increasing training for staff



Identifying linked assets



Implementing a new security strategy



Having conversations with senior leadership



We are not taking any steps



While it's encouraging to see that none of the respondents said that they are not currently taking any steps to manage the convergence of digital and physical security, it is perhaps concerning that there is generally a low uptake of many of the methods necessary to successfully bridge the gap between the two.

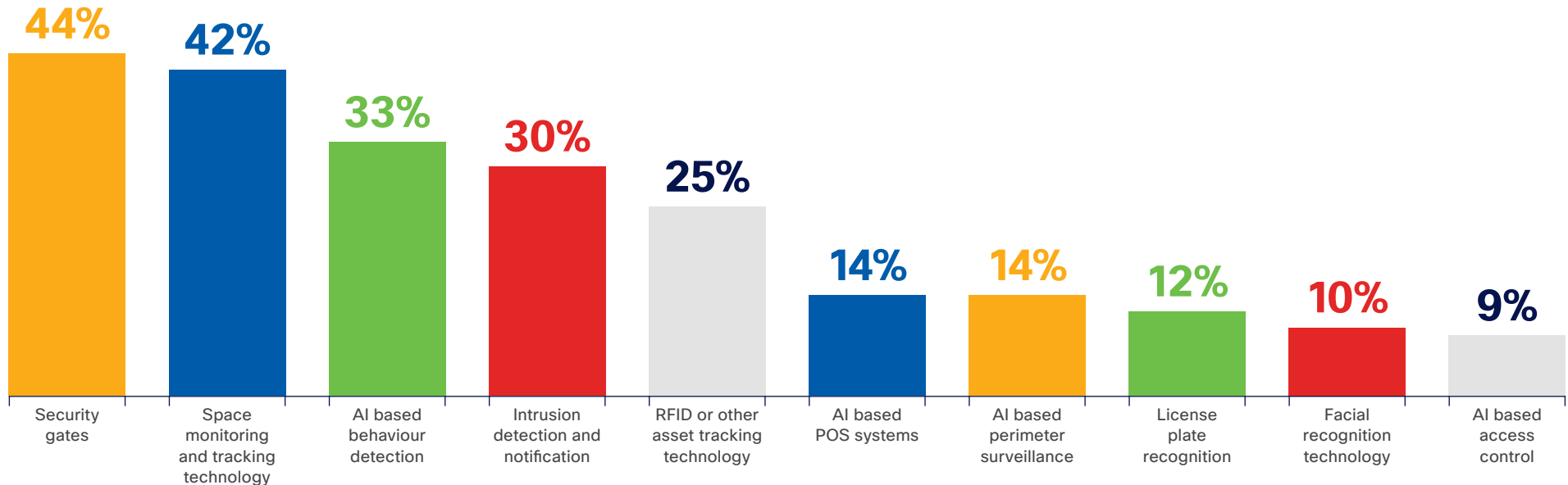
Having conversations with senior leadership, identifying linked assets, and implementing a new security strategy were all chosen by less than 20 per cent of retail professionals. Meanwhile, increasing training for staff was chosen by only 18 per cent of respondents.

Conducting vulnerability assessments had the highest response, with just under two-fifths highlighting this as an action they are rolling out; an unsurprising result given that retailers are required to do their due diligence.

Over a quarter said that they are establishing a convergence team, while a further fifth said they are increasing collaboration between relevant departments. These are both important steps towards truly bridging the gap between the digital and physical to provide a holistic approach to security.



Q5. Which of the following physical security technologies is your organisation currently implementing? (select all that apply)



The report shows that retailers are experimenting with a wide variety of physical security technologies, with all of the options being chosen by at least one in 10. However, it's clear from the figures that some technologies are more popular than others.

Space monitoring and tracking technology was in clear first place with over two-fifths choosing this option, while a further third of retailers in the survey are implementing AI-based behaviour detection. These technologies can be handy tools for both security and personalisation. Retailers are often looking for ways to achieve the seamless experience of e-commerce in their stores. By using smart cameras that incorporate AI models, they can identify congestion hot spots or cold spots where products are less popular, as well as understand customer behaviour to improve the

customer experience. Alongside this, they can optimise stock levels based on past or predicted demand and map a customer's in-store browsing either through in-store video or smart devices.

At the same time, claims against retailers for slip-and-fall and workers compensation are on the rise. Smart cameras can also help to identify dangerous, illegal, or illegitimate activity, enabling retailers to provide a safe, secure, and compliant store.

While retailers seem to be exploring AI when it comes to analysing behaviour, other AI-based technologies - like perimeter surveillance, POS systems, and access control - have proved less popular.

It's no surprise that the results show facial recognition is low on the agenda given the privacy and ethical concerns associated with it. Concerns about the technology have in the past led to campaigners making legal complaints against retailers.

With just under a third choosing intrusion detection and notification as a technology they are currently rolling out, the report demonstrates that the majority of retailers are missing out on cameras and intrusion sensors which can deliver real-time analytics on occupancy, guest traffic flow, and object detection to safeguard both visitors and stock. The right camera can also measure store occupancy and maintain social distancing, identify key surveillance events, block security breaches at data centres and stores, and mitigate product loss with motion search.

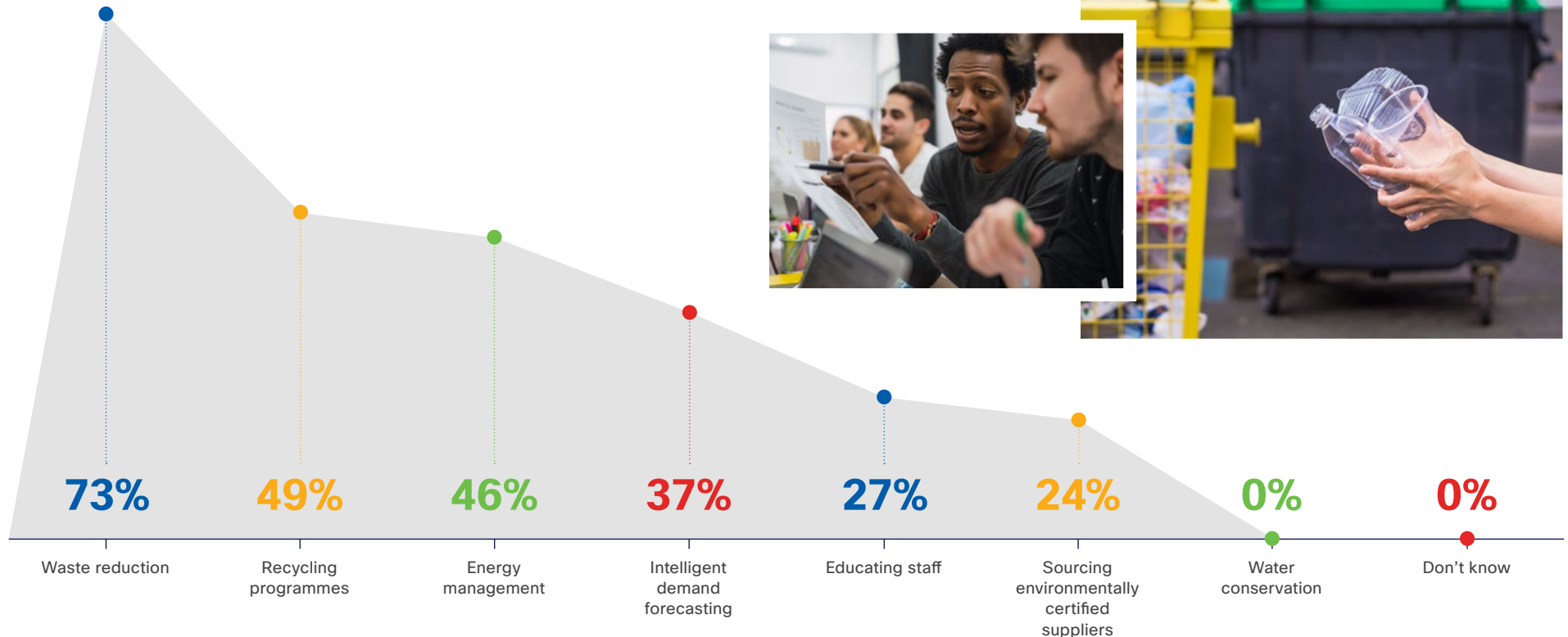
Q6. Which of the below methods is your organisation currently implementing to meet its sustainability targets? (select all that apply)

Retailers are rolling out a range of methods to meet their sustainability targets, with some approaches being implemented more than others.

Top of the list for retailers is waste reduction, chosen by nearly three quarters of respondents. This is a big challenge for retailers, with companies feeling the pressure from their customers to minimise wastage – whether it be food, unsold goods, or too much packaging.

Retailers are also aware of the impact of energy wastage as part of their sustainability goals, with nearly half of respondents highlighting energy management as a method they are currently using. Higher energy prices are also likely to have driven this into the spotlight for many retailers. Physical security technologies can actually play a role in monitoring energy usage, for example integrated sensors for temperature and movement, which can also turn off lights or heating when it's not needed.

Sourcing environmentally certified suppliers is lower on the agenda for retailers, with less than a quarter currently implementing this as a method. This may become more of a priority for retailers as the urgency of achieving sustainability and transparency throughout the supply chain and across third-parties heightens, particularly given that this is increasingly what customers demand.



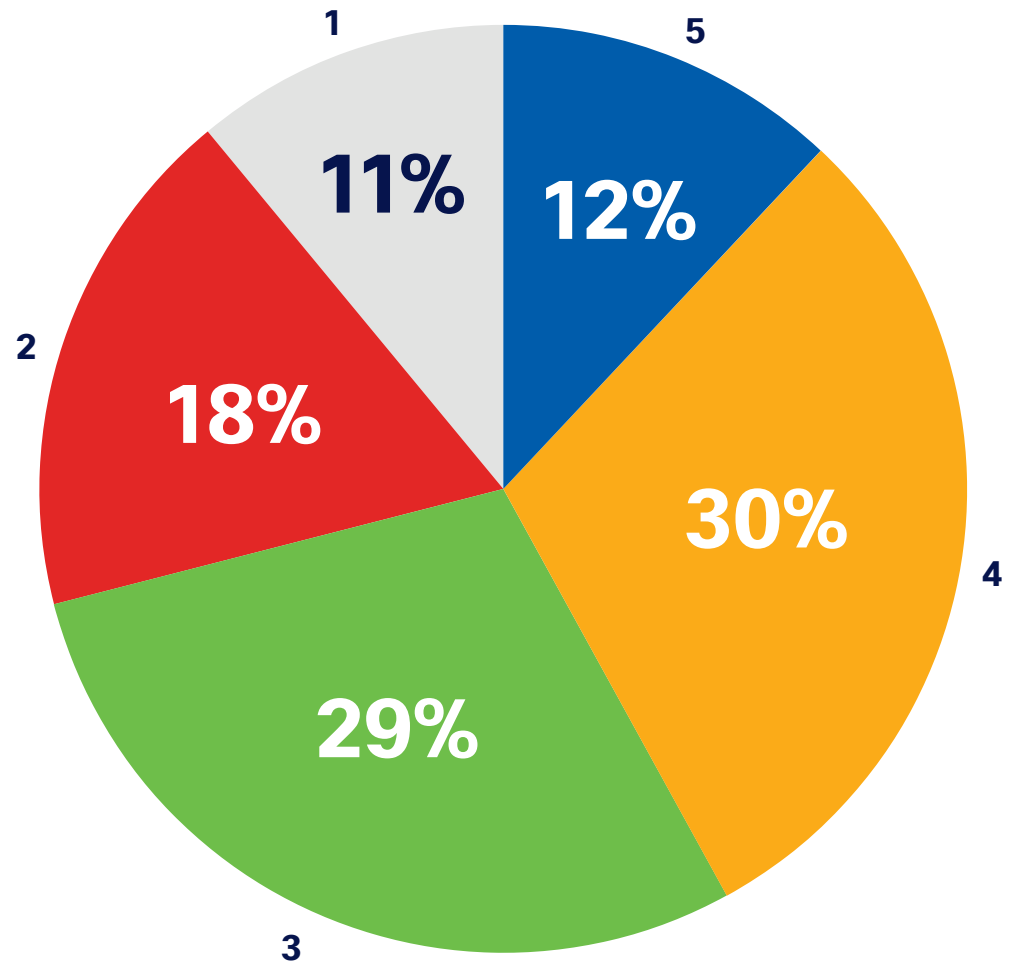
Q7. On a scale of 1–5, how important is sustainability and low energy consumption when choosing new technologies? (select one option)

There was hardly anything to split companies that find sustainability to be very important when choosing new technology and those which don't think it is important at all – with just over one in 10 respondents choosing each of these disparate options.

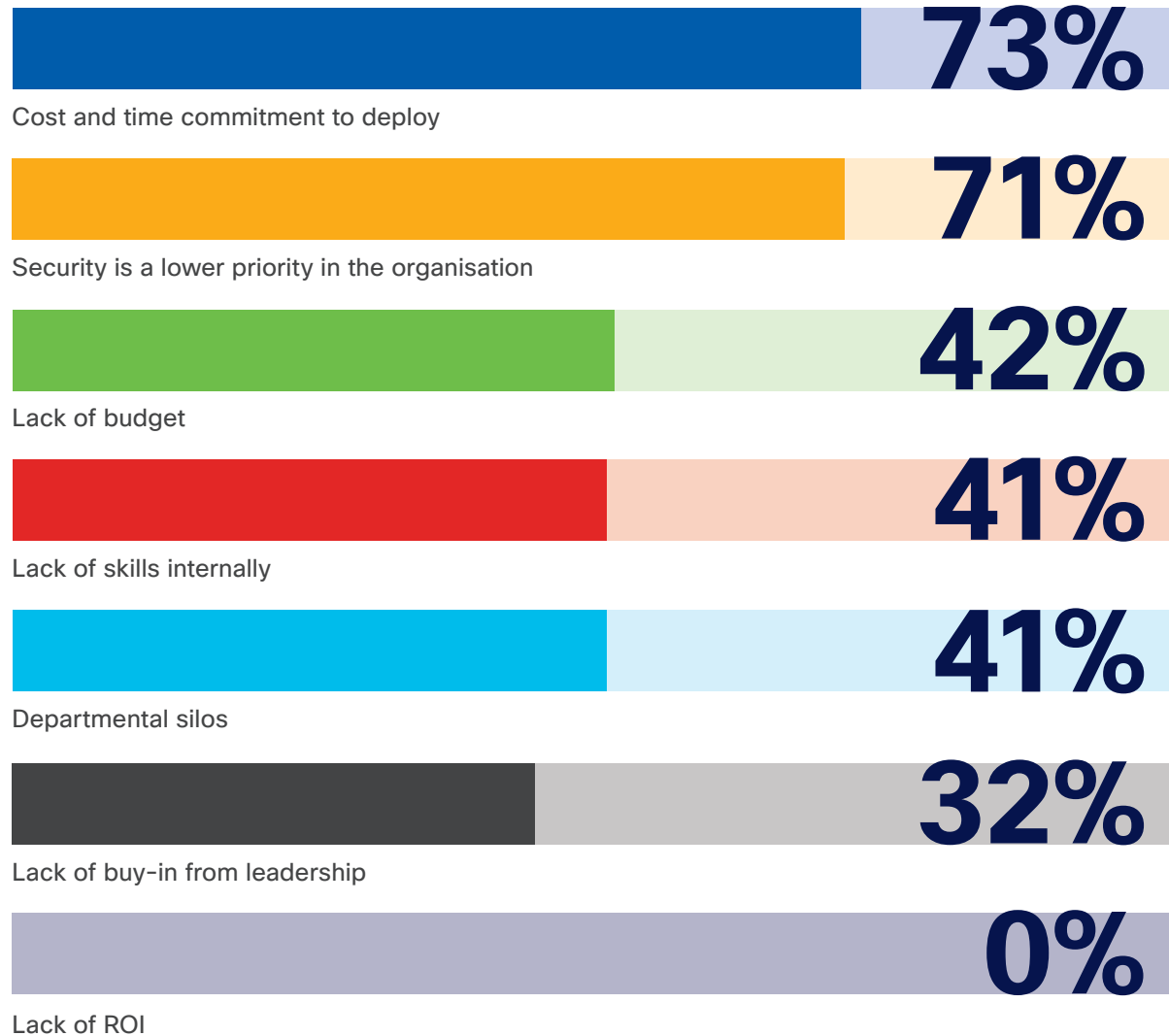
Nearly a third of retail professionals – 30 per cent – said that sustainability is an important consideration when rolling out new tech, while a further 29 per cent revealed that it is somewhat important for their organisation.

It is surprising that less than half – a combined 42 per cent – believe that sustainability is 'very important' or 'important' when it comes to implementing technologies. However, the figures do mirror results elsewhere in the report which suggest that reducing energy consumption costs and carbon footprint is only currently a challenge for 14 per cent of respondents. Given the current macroeconomic environment and inflationary pressures, other considerations such as cost and return on investment (ROI) could be higher on the agenda for retailers at the moment. Retailers also need to provide ROI from any technology investment. Sustainability and low energy consumption could become more important for retailers over the next 12-months, especially given that consumers are moving the needle and dictating the agenda based on their purchasing decisions, with sustainability being one of those influencing factors. This may also increasingly become a priority as inflation settles later in the year – and into 2024.

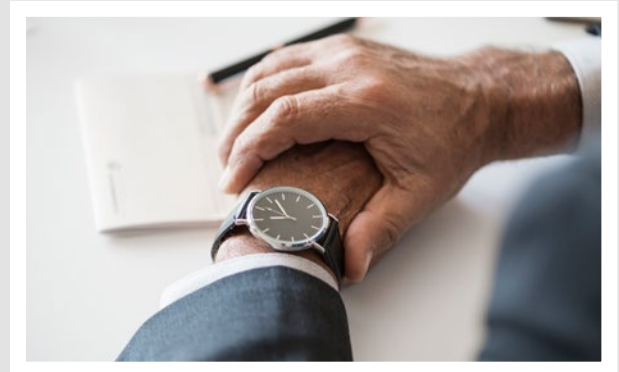
(1 – not important, 5 – very important)



Q8. What are the top barriers to rolling out new physical security technology? (select top three)



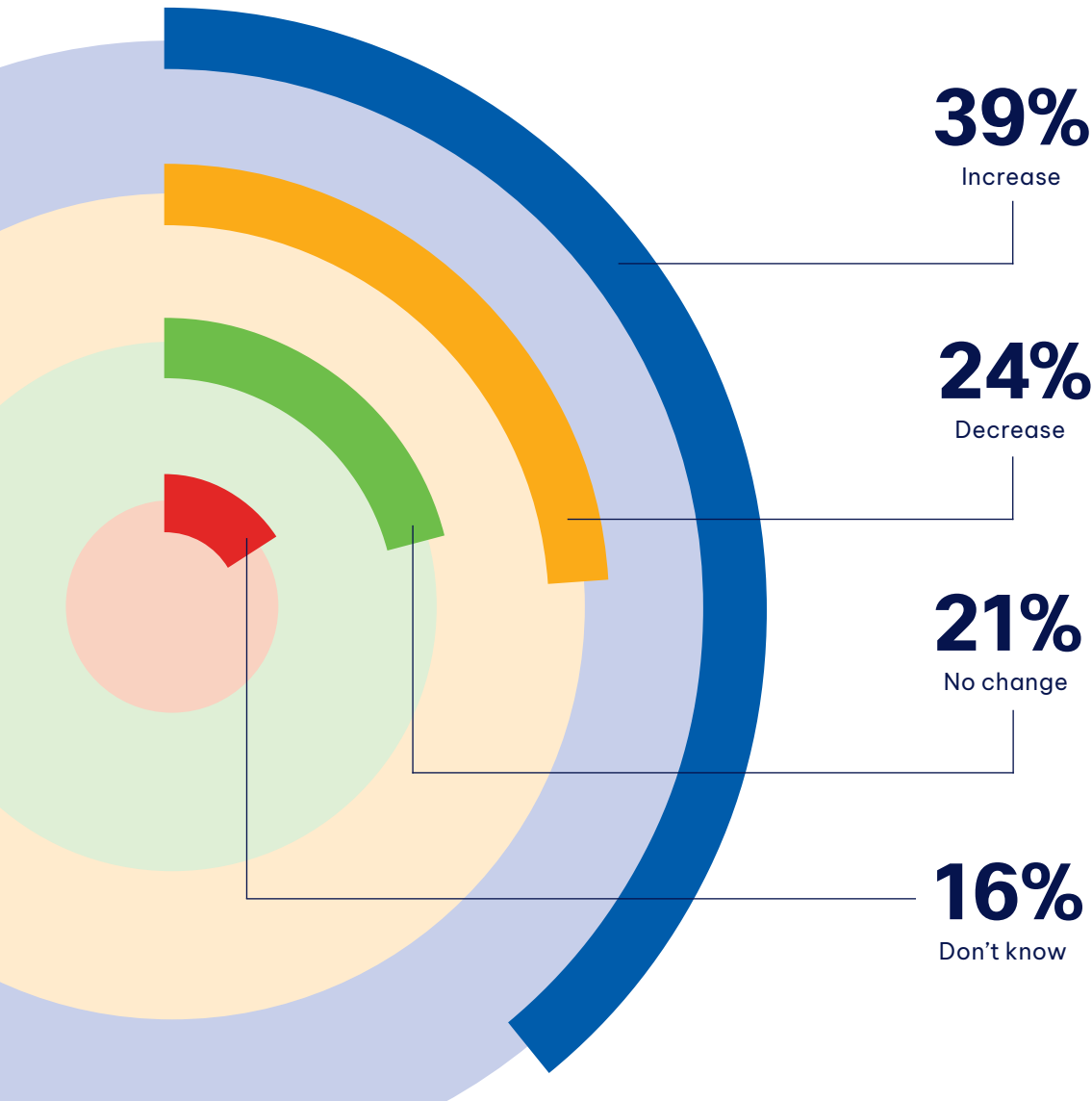
Cost and time commitment to deploy was highlighted as the most prevalent obstacle for retailers implementing a new physical security technology, with nearly three quarters choosing this as a top-three barrier. While the initial cost of new technologies can put retailers off, particularly in an uncertain economic climate where companies are trying to do more with less, the long-term savings of modern, cloud-based physical security technologies can mean retailers quickly see their ROI.



Lack of internal skills was also shown to be a significant hindrance, chosen by over two-fifths of respondents. This figure mirrors results elsewhere in the report which reveal that a lack of training and education is a challenge for half of retail professionals. Companies could avoid this issue by outsourcing to a third-party which can take the hassle out of the process.

Perhaps the most surprising result generated by this question is that over 70 per cent of retail leaders say that security is a lower priority in the organisation. Physical security should be high on the agenda for retailers - particularly given the ongoing cost-of-living crisis- as people are more likely to commit crime and fraud during times of economic hardship.

Q9. How do you expect your organisation's physical security technology budget to change over the next 12 months? (select one option)

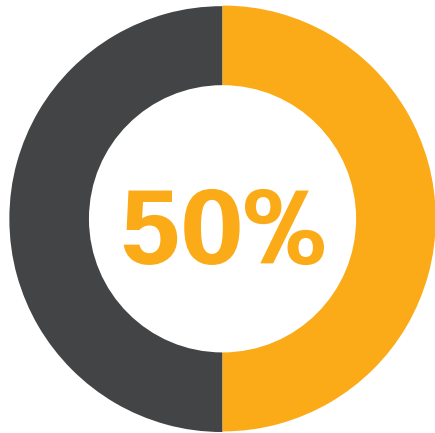


Despite earlier results suggesting that security is a lower priority for many retailers and that cost is often a barrier to rolling out the technology, it's promising to see that nearly two-fifths of respondents say that their organisation is likely to increase its physical security technology budget over the next year. With the right technology partners, firms will not only better protect their employees and customers, but also have access to data which can help in the day-to-day running of a store and create a more personalised and seamless shopping experience.

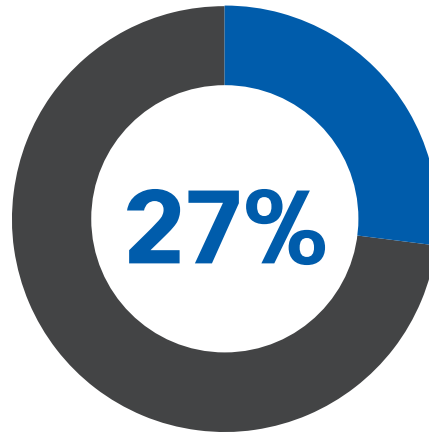
Given that nearly three quarters of respondents highlighted cost as a top-three obstacle to implementing new physical technology, it's unsurprising that some companies - just under a quarter - said they will be reducing their budget over the coming 12-months. These companies may be responding to the pressures of ongoing economic uncertainty and higher inflation by moving investments away from technology into savings for customers, or to reduce overall spending. However, these businesses could be missing out on some of the ROI opportunities of rolling out the latest physical security technologies.



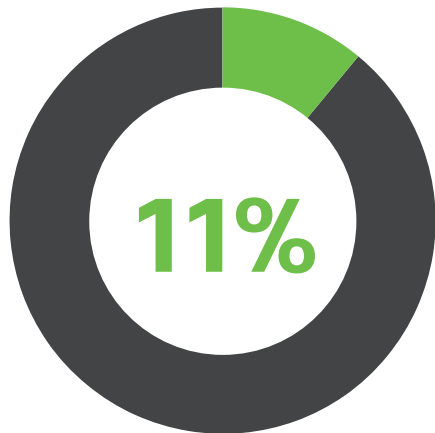
Q10. How much does ROI form your physical security investment, drive consideration? (select one option)



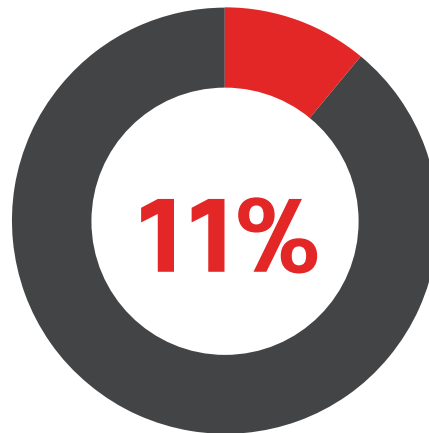
Somewhat



Very much



Not at all

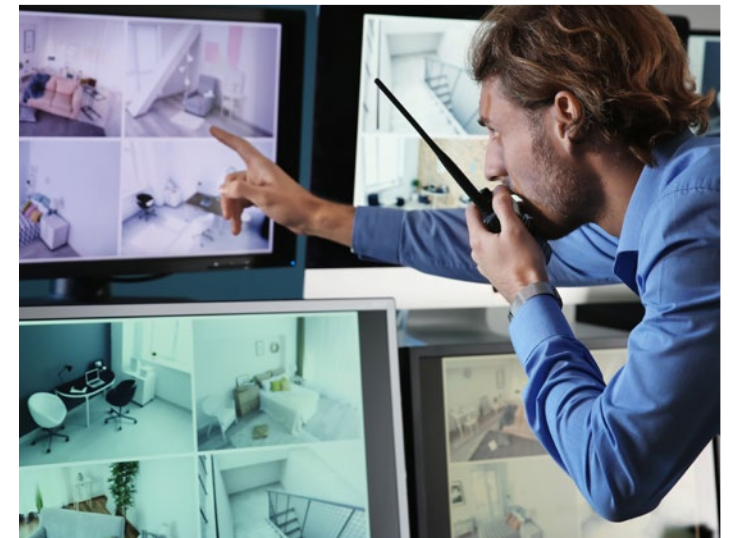


Don't know

With results elsewhere in the report suggesting that cost commitment is a key barrier to rolling out physical security, it's interesting to see that the majority of respondents see ROI as a consideration for investing in the technology.

With a combined 77 per cent of respondents saying that ROI forms physical security investment consideration to some extent, it's clear that it's important for retailers to know that the technology they buy performs well and is worth the cost.

Some 11 per cent said that ROI doesn't impact their investment consideration when it comes to physical security, while the same number were unaware if this forms part of their consideration. These companies are likely missing out on turning their physical security strategy into a competitive advantage, rather than a cost.



Conclusion

The report reveals that while retailers are taking some steps to manage the convergence of digital and physical security, there is generally a low uptake of methods necessary to successfully bridge the gap between the two.

Analysis of the results shows that the top three priorities when it comes to retailers' physical security strategies are supply chain security, utilising new technologies, and addressing labour shortages. Retailers are rolling out a wide variety of physical security technologies to support these strategies – with space monitoring and tracking the most popular – unsurprising given the many benefits this technology can have for both security and the smoother running of an organisation.

Despite retailers rolling out the technology, there are still barriers to implementing it. Nearly 75 per cent of respondents said that cost and time commitment to deploy was an obstacle and a further two-fifths highlighted lack of internal skills as a hindrance. By leveraging a technology partner that has the skills, time, and resource to get any physical security technology up and running, companies could address this pressing challenge. Most surprisingly, over 70 per cent said that security is a lower priority for the organisation. Meanwhile, just under a quarter of retailers are reducing their budget for physical security over the next 12 months.

However, nearly two-fifths of respondents say that their organisation is likely to increase its physical security technology budget over the next year. With the right technology partners, firms will not only better protect their employees and customers, but also have access to data which can help in the day-to-day running of a store and create a more personalised and seamless shopping experience.

The majority of respondents said that ROI is a consideration for investment in the technology – suggesting that it's important to companies that their spending results in lower costs, operational efficiency, and both time and money savings. Those that don't think of this when rolling out their next technology could miss out on turning their physical security strategy into a competitive advantage, rather than a cost.

When it comes to rolling out a cloud security strategy, concerns about the data governance and security implications of moving highly sensitive data to the cloud was revealed to be a major roadblock. However, retailers that deploy an integrated, cloud-based platform can help mitigate risks and protect customer data by managing workforces at scale and detecting threats quickly throughout an organisation.

Despite retailers rolling out a range of methods to meet their sustainability targets, there was hardly anything to split the companies that find sustainability

to be very important when choosing new technology and those who don't think it is important at all – with just over one in 10 respondents choosing each of these disparate options. Sustainability and low energy consumption could become more of a consideration for retailers over the next 12 months – particularly if inflation settles later in the year.

While some retailers are investing in new technologies to bolster their security strategies, it seems most have a way to go. By building a holistic strategy that bridges the gap between the physical and digital side of security through the latest technological innovations, this area of the business can be turned into a competitive advantage, rather than a burden or cost.



Interested in a free trial?

Visit our Cisco Meraki site [here](#)



Retail Systems

In association with

