



 GlobalData.

SUMMER 2022

Full visibility and real-time threat response: Helping retailers achieve proactive IT Security

AUTHORS

David Bicknell, Sarah Coop, Rupantar Guha, David George and David Williams, GlobalData

SPONSORED BY

 **TANIUM**

Contents

Executive summary	03
The complex environment facing retailers	04
Life after COVID	
A difficult 2022 follows a challenging 2021	
Closing the cybersecurity skills gap	
What are the risks?	07
Business viability and reputation	
A lack of visibility – need for a single truth	
Too many tools	
What are the solutions?	11
Take a proactive stance	
Invest to protect	
Recommendations	13
Sponsors	14

Executive summary

The cybersecurity threat landscape is worsening. 2021 was the worst year on record for cybersecurity attacks, and the threat landscape has already increased in 2022, exacerbated by geopolitical trends like COVID-19 and the Russo-Ukraine war.

The war has introduced new business risks for retailers: on inflation, for supply chains, and on cybersecurity. Retailers are under pressure to absorb additional costs and maintain stable prices for consumers, as well as to protect the IT estate from the increased cybersecurity threat the war situation brings. At the same time, with the growth of e-commerce, technology is at the core of the retailer-customer relationship.

Retailers have complex IT systems, with everything continually 'built on'. Retailers need to have a view right back into their ERP systems, from their back-end systems through to the point of sale. Although challenging, it is essential for retailers to have full visibility of the IT estate to support the customer journey and to ward off cybersecurity threats.

Cyberattacks put business viability and reputation at risk. Rather than physical goods, hackers are stealing valuable data. Such incidents could seriously damage a retailer's reputation in the eyes of regulators, investors, and general customers.

Organisations currently buy too many IT security point solutions, and then fail to effectively manage and integrate them. A typical enterprise has 43 separate IT security management tools in its infrastructure, which is far too many to manage. More does not mean secure.

The solution for retailers is to take a proactive stance on cybersecurity and to invest to protect. Preventative cybersecurity reduces the risk of a cyberattack by identifying security weak points and monitoring the network to identify threats. Reactive cybersecurity only responds to cyberattacks after they have occurred.

Investing in preventative cybersecurity can reduce costs in the long run. It is much more costly to recover from a cybersecurity attack than to prevent one. Yet despite constant warnings over the threats to business operations from cyberattacks, some organisations are seemingly not fully committed to security, and will only shut the stable gate after the horse has bolted. even if that means increased costs.

Only by adopting a converged endpoint solution with full visibility of assets can retailers mitigate and prevent the cyberattack risk. Adopting an effective platform will help reduce the impact of silos to provide retailers with a holistic view, enabling them to get their arms around the key concept of 'knowing what you know, knowing what you don't know.'

The complex environment facing retailers

Life after COVID

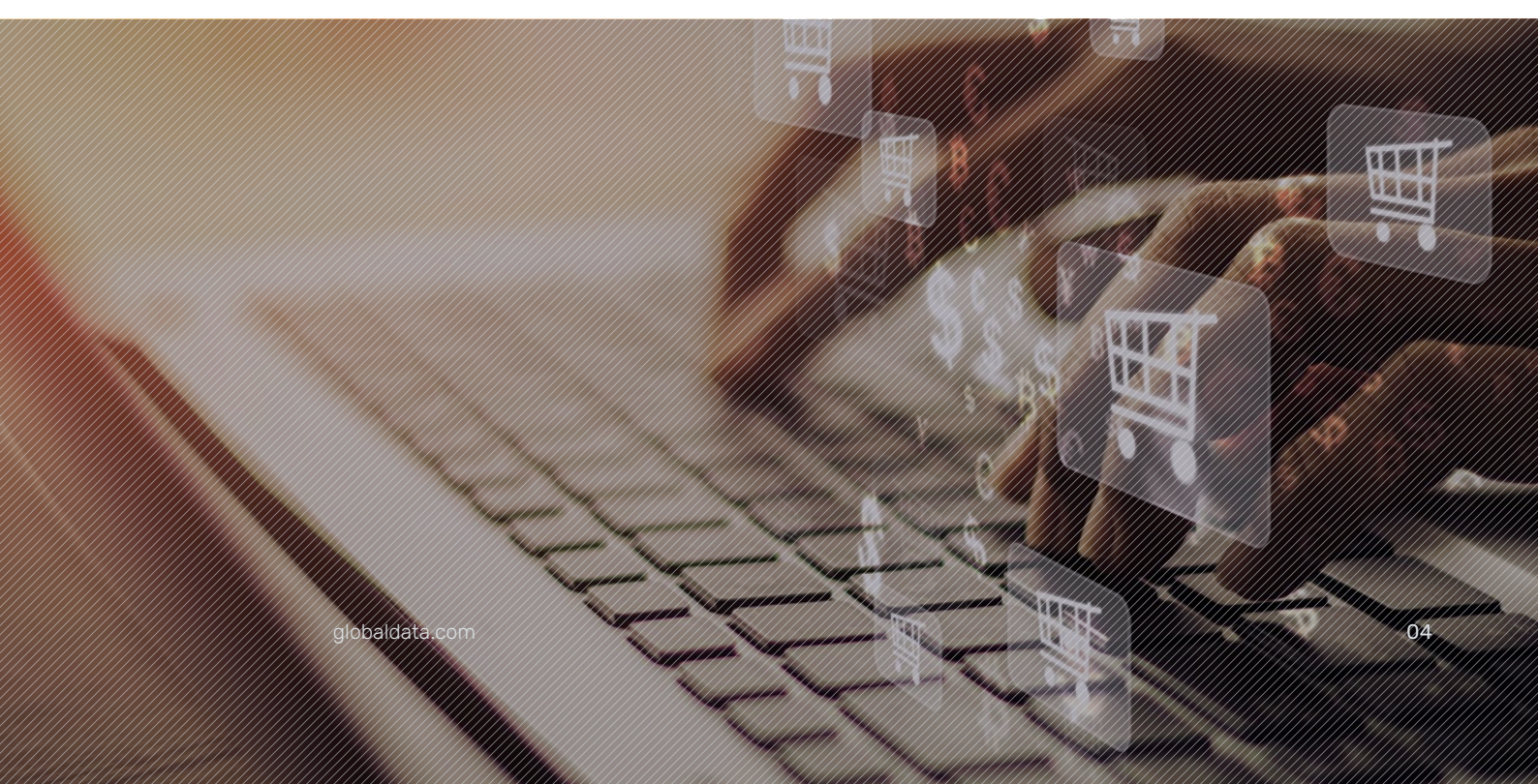
Since 2020, the picture for the retail sector has changed markedly, arguably forever, in the wake of COVID-19. The pandemic changed both shopping habits and patterns, with the weekly in-person shop being replaced by online shopping and a greater focus on e-commerce. Then just as life seemed to be returning to normal, the fallout from the Russia-Ukraine conflict introduced new business risks: on inflation, for supply chains, and on cybersecurity.

More than half of UK consumers are now shopping online, and UK online spend is forecast to increase by 29.6% between 2019 and 2024, according to GlobalData research. Retailers will seek partnerships with specialist technology vendors in order to enhance their digital capabilities, improve their online offers, and, crucially, ensure that their IT estate is secure against cyberattacks.

Whatever the outlook, the challenge is for retailers is to listen to and understand the voice of their customers. With the growth of e-commerce, technology is at the core of the retailer-customer relationship.

And yet technology itself is a major headache for retailers. One of the primary business challenges facing the retail industry worldwide is to modernise its technology architecture. The technology backdrop against which the industry is designed to operate, is now out of date. Systems cannot provide the visibility to allow retailers to flex to customers' wishes or to ever more prevalent supply chain disruptions.

Like most sectors, the retail industry has seen significant M&A activity. Not all retailers are affected, but those that have made acquisitions will need to integrate them into the business as quickly and efficiently as possible. The complexity that new acquisitions create for corporate networks can also increase the threat landscape for acquiring organisations, including retailers.



A difficult 2022 follows a challenging 2021

The cybersecurity threat landscape is worsening. 2021 was the worst year on record for cybersecurity attacks, and the threat landscape has already increased in 2022, exacerbated by geopolitical trends like COVID-19 and the Russo-Ukraine war.

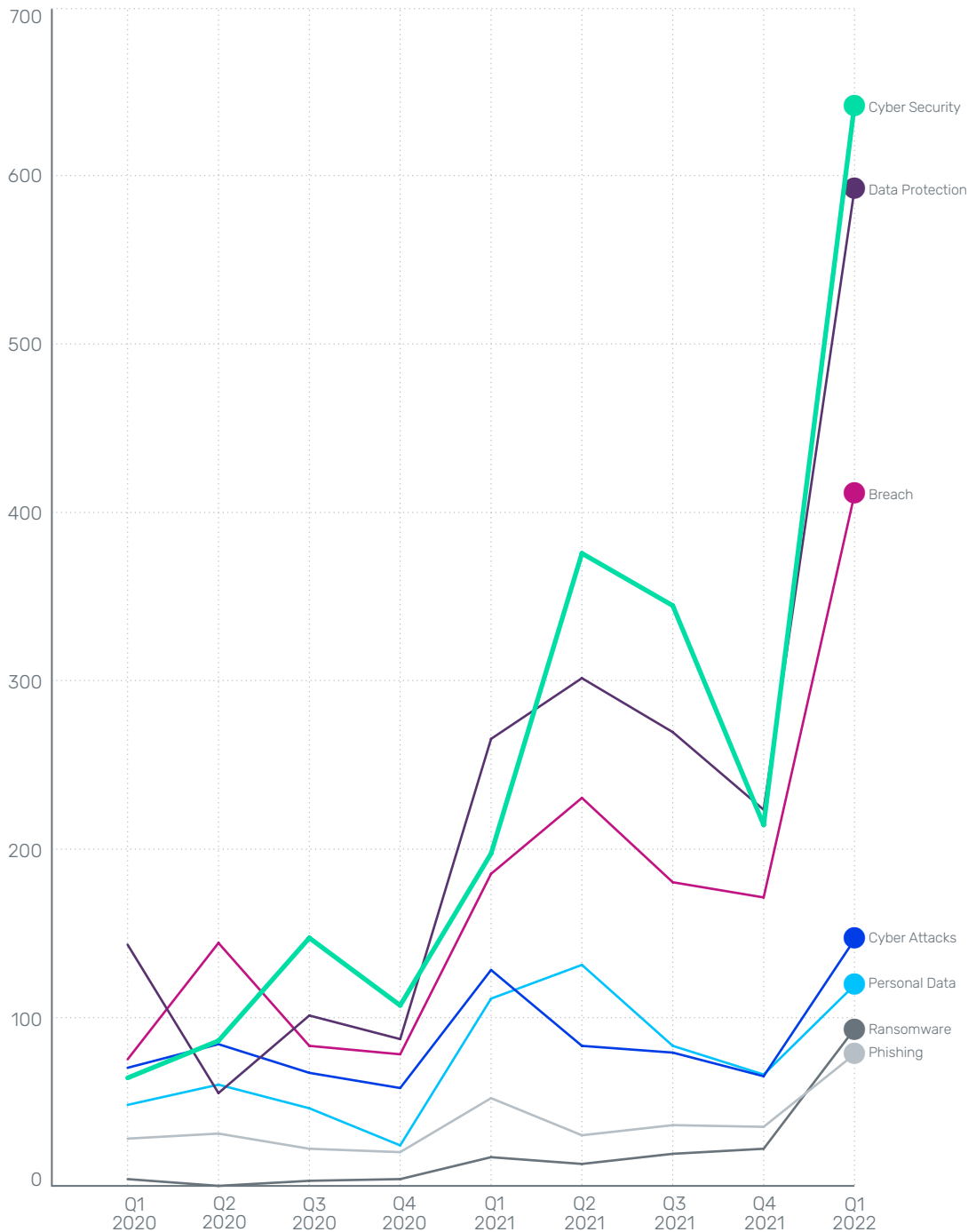
Retailers are experiencing the increasing risk. Mentions of cybersecurity breaches in global

retail company filings increased significantly in 2021, according to GlobalData's company filings analytics database. This trend will continue in 2022. It is enough to keep any retail company CEO awake at night.

Filings referencing cybersecurity breaches in retail companies show retailers are now more at risk of cyberattacks than ever before.

Figure 1

Global retail company filings, Q1 2020 to Q1 2022



Source: GlobalData

Tanium's 2022 'Prevention is Better than Cure' research confirmed the trend. 80% of C-Suite Decision-Makers believe that cyberthreats to their organisations are increasing and expect 2022 to be the worst year yet in terms of the number of attacks they will be facing.

COVID-19 accelerated trends in online shopping and remote working, distributing the workforce and increasing the number of potentially vulnerable endpoints. This will continue in 2022: a well-known online retailer expects global e-commerce sales to reach \$5.5 trillion (£4.5 trillion) by the end of 2022, increasing the amount of customer data on servers and the risk of point of sale (POS) attacks.

Cybersecurity spend will increase, despite inflationary cost pressures and a weak economic outlook. GlobalData estimates that the global cybersecurity industry will grow from \$125.5 billion (£103.6 billion) in 2020 to \$198.0 billion (£163.6 billion) in 2025 at a compound annual growth rate (CAGR) of 9.5%.

The Russo-Ukraine war has introduced new business risks for retailers: on inflation, for supply chains, and on cybersecurity. Retailers are under pressure to absorb additional costs and maintain stable prices for consumers,

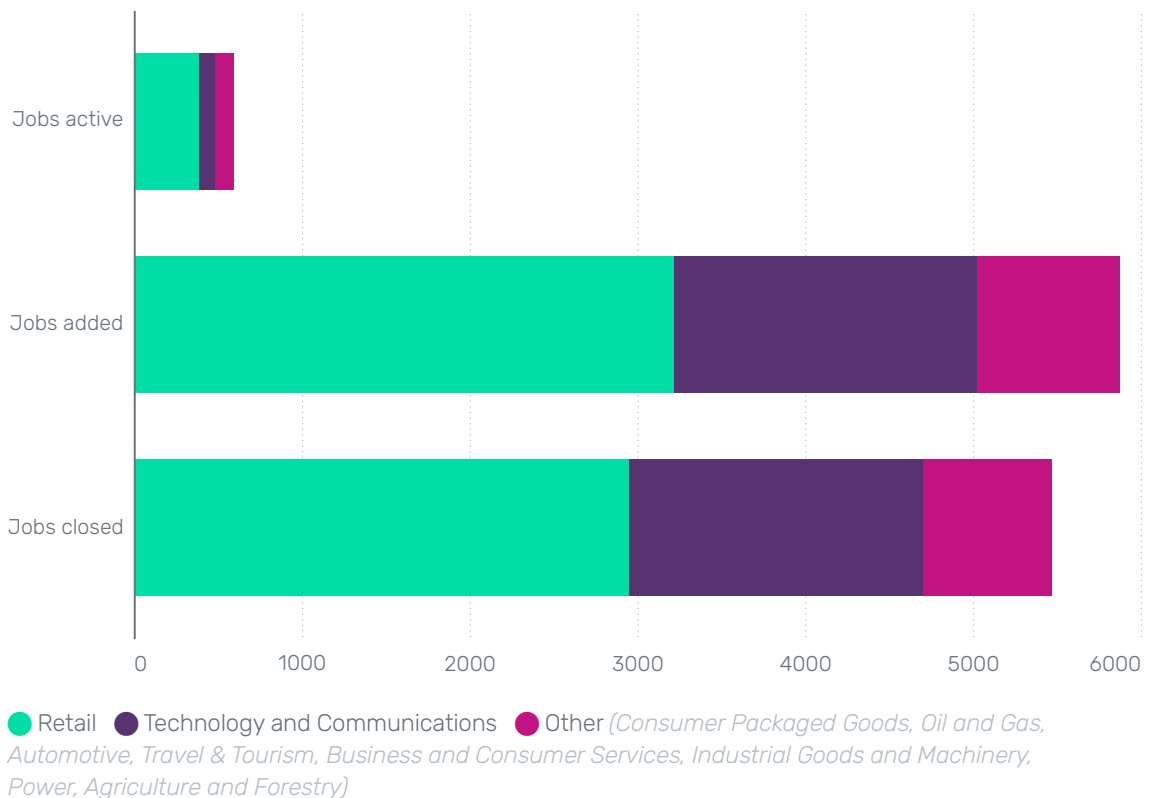
as well as to protect the IT estate from the increased cybersecurity threat the war situation brings. As well as creating difficult outlook for 2022, many of these challenges are set to persist into the medium term.

Closing the cybersecurity skills gap

Cybersecurity skills remain a thorny problem. Retailers continue to struggle to attract top cyber talent in a depleted job market. There are not enough cybersecurity professionals to satisfy demand. The problem is exacerbated by organizations' chaotic use of point solutions, which are not designed to work in concert. For retailers, the need to respond to greater adoption by their customers of e-commerce has put a premium on the business's use of skilled resources. Those tech engineers that might have spent time delving deep into cybersecurity tech dumps actually have great coding skills that can be better used within the business, which they understand well. They are best-equipped to help drive brand equity and brand awareness through technology.

Figure 2

UK cybersecurity hiring by sector, Jan 2020 to Mar 2022



What are the risks?

Business viability and reputation

Retailers are increasingly gravitating towards omnichannel experiences to attract, and retain, customers. The constant flipping between physical and online channels makes it difficult for traditional retailers to understand the value of every channel.

.....
The rise of seamless payment solutions, especially using credit cards and online banking, are prime targets for cyberattacks. As opposed to stealing physical goods, hackers are stealing valuable data from cardholders. Such incidents could hamper a retailer's reputation in the eyes of regulators, investors, and general customers.

A major retailer's recent cyber stress test shows that retailers are only too aware of the potential impact on their reputation of a data breach. The stress test concluded that a significant data breach poses a reputational risk for retailers, resulting in a decline in customer sentiment and an adverse trading impact. The company argues that the extent of the trading impact is very uncertain, both in terms of the financial impact and the period it may take to recover customer trust.

As the major retailer recognised in its annual report, the volume and nature of the customer and supplier data it holds as a business could result in 'a serious data or security breach' which it recognises could result in a significant financial penalty levied against the company, under General Data Protection Regulation (GDPR) legislation.

The emergence of the retailer's stress-test is an important development. Other retailers are likely to follow suit, leading them to reconsider what cybersecurity tools are necessary to prevent such data breaches.



A lack of visibility - Need for a single source of truth

Retailers have a large back end, or server-side, which consists of the server providing data on request, the application that channels it, and the database which organises the information. They also have complex inventory systems. It is a brittle, legacy picture, with everything continually 'built on'. Retailers need to have a view right back into their ERP systems, from their back-end systems through to the point of sale. The customer experience begins right where the supply chain starts and runs to where the retailer meets the customer, either instore, or online.

.....
Although challenging, it is essential for retailers to have full visibility of the IT estate to support the customer journey and to ward off cybersecurity threats and other network issues.

Retailers' IT infrastructure differs from other verticals in the form of retail-specific hardware and software usage, such as Point of Sale (PoS) systems, beacons, e-commerce, and supply chain management systems. These systems may require additional or different security measures than computers, tablets, and servers.

Having a better 'source of truth' from the telemetry around endpoints helps. An effective platform should provide retailers with information on how updated an endpoint is, and whether or not it is compliant or at the end of its useful life. That then provides information on the risk involved. Now, tools, using data that previously was more narrowly used to deal with threats and cybersecurity issues, can be applied to help retailers manage their operations. In the meantime, cyberthreats will cause retailers performance issues, and mean IT issues continue to grow, unless they are addressed effectively. That is an unwanted additional headache for retailers, given the business challenges they are already facing.

An effective approach allows retailers to have a better viewpoint in terms of portability, resilience, and how the customer experience will be affected all along the supply chain and at point of sale. Such an approach helps create an environment that is more secure, protecting necessary inventory systems from hackers.

Organisations are experiencing more attacks than ever before. Cybersecurity Ventures notes that ransomware attacks on businesses occur every 11 seconds. In all, businesses experienced a 50% increase in weekly cyberattacks in 2021.

But it's not just external attacks. Insider attacks are multiplying and can go unnoticed for indefinite periods of time. Key areas to focus on are reducing information silos across the supply chain and establishing strong internal knowledge of security solutions and risks.

Despite the focus from 2020 to 2022 on the growth in external attacks as a result of the Covid pandemic and changing consumer behaviour, insider attacks are a particular worry.

More than 34% of businesses around the globe are affected by insider threats yearly and 66% of organisations consider malicious insider attacks or accidental breaches more likely than external attacks. Over the last two years, the number of insider incidents has increased by 47%. Adopting the most effective analysis tools can help manage risk and reduce both insider and external threats.



“Latency is the new issue. E-commerce has become so critical to retailers that a slow network leading to online shoppers waiting around is as damaging to the corporate brand reputation as a network outage.”

Erik Gaston, VP Global Accounts and Verticals, Tanium

Too many tools

A typical retailer now has too many separate IT security management tools in its infrastructure. It needs more clarity, not more tools.

In order to meet this challenge, retailers should look to invest in modern solutions which can individually be collapsed and integrated onto a single converged platform. This generates a uniform language across disparate solutions, meaning retailers can be less reliant on expensive, highly-skilled employees to maintain their cybersecurity systems. The platform can be orchestrated to empower teams to spot slight changes and small deviations from the norm. That enables them to identify and respond to potential issues in real-time, thereby avoiding a potential negative customer experience.

.....
An effective platform will also help reduce the impact of silos to provide retailers with a holistic view, enabling them to get their arms around the key concept of 'knowing what you know, knowing what you don't know.'

But despite all these solutions, organisations are finding it harder than ever to protect their IT infrastructure. Just like the threat environment, cybersecurity solutions are continually evolving, and some might argue there is a need for the convergence of security and operations.

Cybersecurity must be a key element within a company's risk management framework. This can create top-down flows of cybersecurity awareness from the board level to the frontlines, helping to plug all touchpoints precisely. An organisation-wide approach can allow CISOs to make strategic and practical investments in order to reduce the risk of breaches. Subsequently, they can deploy multiple solutions on an as-needed basis without exposing any touchpoint.

Over four in ten organisations surveyed expect to spend more on Threat Detection, Endpoint Security, Data Recovery and Backup, Employee Awareness Training, New Endpoint Devices and Communication and Collaboration Software over the next financial year. In other words, the need for multiple solutions - but at present too many point solutions - probably means creating more data than can be managed effectively.



What are the solutions?

Take a proactive stance

Be preventative to avoid breaches. There are two possible approaches to dealing with cybersecurity. You can be proactive, taking the necessary steps to keep yourself safe by investing in the right solutions, or be reactive, responding only when a breach has occurred. Forewarned is forearmed. Those retailers who take a mainly reactive approach to cybersecurity are significantly more likely to have experienced a cyberattack or data breach in the last 24 months than those who take a mainly preventative approach.

Preventative cybersecurity reduces the risk of a cyberattack by identifying security weak points and monitoring the network to identify threats. Reactive cybersecurity only responds to cyberattacks after they have occurred, an unacceptable approach in the current landscape.

90% of industry professionals whose organisations take a mainly reactive approach have suffered a breach within the last 24 months.

Cyberattacks can be avoided or reduced with the right preventative measures, including transparency, threat detection and having a complete view of the IT estate.

86% of organisations who have experienced a cyberattack or data breach in the last six months agree that if their organisation had spent more on preventative measures to stop cyberattacks and data breaches, then the impact of 'avoidable incidents' would be minimised.

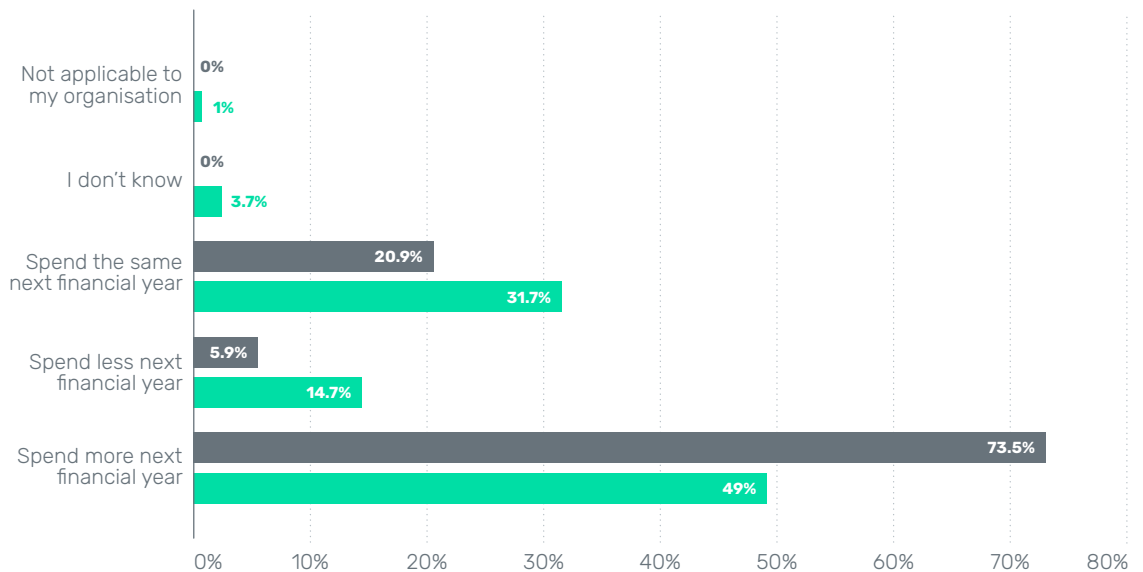
Amongst retailers, this rose to 93.5% believing the majority of cyberattacks could have been avoided by preventative measures, for example, training staff not to click on phishing links or patching vulnerable endpoints.

Preventative measures are vital, but no company is ever 100% safe from a cyberattack. Threat detection is also a prerequisite. In fact, 73.5% of retailers surveyed in the 'Prevention is Better than Cure' survey are spending more on threat detection in the next financial year, compared to 49% of all surveyed.

Figure 3

'Prevention is Better than Cure' survey results, January 2022

Is your organisation planning to spend more or less on threat detection next financial year compared to this financial year?



Source: Tanium

● Retail ● Total surveyed

Invest to protect - it costs more to recover from a cyber incident than to prevent one

Investing in preventative cybersecurity can reduce costs in the long run. It is much more costly to recover from a cybersecurity attack than to prevent one, and every company is at risk of a cyberattack. And yet, eight in 10 (79%) professionals surveyed said that more cybersecurity budget would likely be assigned following a data breach, rather than ahead of one. Despite constant warnings over the threats to business operations from cyberattacks, some organisations are seemingly not fully committed to security, and will only shut the stable gate after the horse has bolted, even if that means increased costs.

A leading technology company reported that the average total cost of a data breach in the UK increased by 20% in 2021, to £3.86 million. For retailers, the average cost of a data breach grew by 62.7%, to £2.70 million. The cost for retailers is more than doubling year on year and would be enough to put multiple retailers out of business.

Taking preventative measures to protect customer data is essential for consumer trust, especially when retailers hold extensive customer data from loyalty schemes, club cards, e-commerce transactions and mailing lists.

To counter all these threats, 90% of organisations have bought at least one new IT security point solution, and almost half (45%) have bought at least four new products, according to Foundry's 'Security Priorities Study'. A typical enterprise now has 43 separate IT security and security management tools in its infrastructure.

But 'more' doesn't mean 'secure'. Despite spending upwards of \$154 billion (£127 billion) each year from 2022 on security solutions, according to GlobalData, organisations are still finding it harder than ever to protect their IT infrastructure.

79% of industry professionals taking a mainly preventative approach to cybersecurity have experienced an attempted attack or breach in the last 24 months.

Security is changing and some might argue it is time for greater convergence between security and operations. Adopting an effective platform will help reduce the impact of silos to provide retailers with a holistic view, enabling them to get their arms around the key concept of 'knowing what you know, knowing what you don't know.'

Retailers must be on top of the overall operational picture, from the back end right through to engaging with the customer. A converged endpoint solution with full visibility of assets helps retailers mitigate and prevent the cyberattack risk.

Recommendations

1

VISIBILITY IS KEY:

Retailers must cope with the double jeopardy of growing economic uncertainty and increasing cyber challenge. To do so, they must have a clear picture of the threats facing their businesses. But that doesn't come from having more systems. More does not mean secure...

2

INVEST IN THE RIGHT TOOLS:

You cannot protect what you cannot see. Crystal-clear visibility into the corporate IT landscape is key to mitigate risks of cyberattacks. CEOs must invest in the right tools to provide their CIOs and CISOs with necessary security insight to gain a holistic view of security assets, unceasingly assess risk exposure, and deploy the right tools to avert, detect, and respond to potential threats. Most C-Suite respondents agree that the evolution of risk analysis tools is making it easier to prevent cyber threats.

3

FOCUS ON THE BIG PICTURE:

Retailers must be on top of the overall operational picture, from the back end right through to engaging with the customer. Security is changing and some might argue it is time for greater convergence between security and operations. Such a converged endpoint solution with full visibility of assets helps retailers mitigate and prevent the cyberattack risk. A judicious preventative cybersecurity approach, investing to protect, is the way forwards.

4

ADOPT AN EFFECTIVE PLATFORM:

Retailers should aim to reduce the impact of silos to gain a holistic view, enabling them to get their arms around the key concept of 'knowing what you know, knowing what you don't know.'

Sponsor



Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale.

Tanium has been named to the Forbes Cloud 100 list for six consecutive years and ranks on Fortune's list of the Best Large Workplaces in Technology. In fact, more than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit www.tanium.com

Follow us on LinkedIn: [Tanium](#)

Follow us on Twitter: [@Tanium](#)



We are the trusted gold standard intelligence provider to the world's largest industries

We have a proven track record in helping thousands of companies, government organizations, and industry professionals profit from faster, more informed decisions.


Our unique data-driven, human-led, and technology-powered approach creates the trusted, actionable, and forward-looking intelligence you need to predict the future and avoid blind-spots.

Leveraging our unique data, expert analysis, and innovative solutions, we give you access to unrivaled capabilities through one platform.

HEAD OFFICE

John Carpenter House
7 Carmelite Street
London
EC4Y 0AN
UK

Tel: +44 20 7936 6400

 [GlobalDataPlc](#)

 [GlobalDataPlc](#)

 [GlobalData.com](#)

DISCLAIMER

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, GlobalData. The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that GlobalData delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such, GlobalData can accept no liability whatsoever for actions taken based on any information that may subsequently prove to be incorrect.