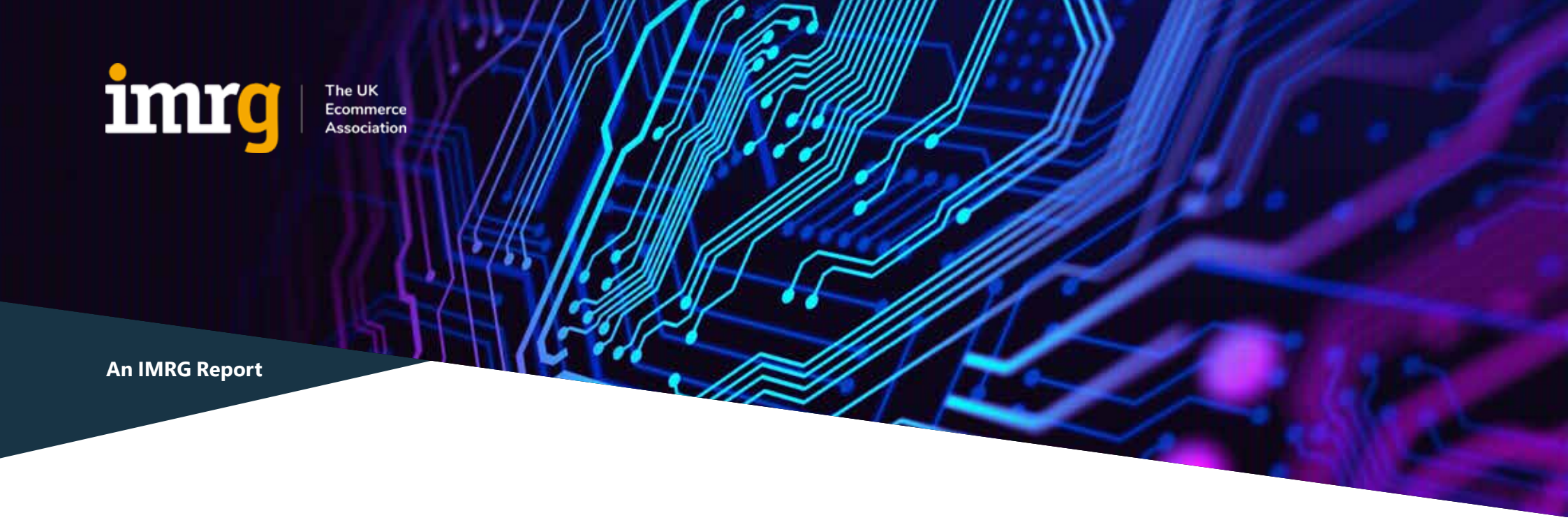


imrg | The UK Ecommerce Association

An IMRG Report

How supply chain and cyber threats are impacting digital channels

Supported by LOCKTON®

December 2021

Introduction

Major changes in consumer demands and behaviour over the last two years have triggered a transformation in the world of ecommerce. This report assesses the impact of this change on retail business models, with a particular focus on supply chains, cyber threats and profitability.

Between 2020 and mid-2021, retailers enjoyed a 40-50% growth in online revenues. While this growth has now started to slow, volumes remain strong and the current 10% contraction is now more in-line with pre-pandemic trading patterns.

While the shift to online shopping during the pandemic has been widely reported on, behind-the-scenes issues of stock availability and cyber threats are going under the radar.

Extended supply chains, shrinking delivery windows and demanding production schedules expose retailers to high levels of risk. This has been exacerbated by the massive increase in online consumer demand over the last two years.

Flexible production has allowed fast fashion retailers to turn over ranges within a few months, while stable supply chains have enabled businesses to plan and budget with increased accuracy, with little requirement for contingency planning.

Increases in demand, changes to customs procedures in Europe and staffing shortages due to the pandemic have all contributed to bottlenecks forming at ports and at sea.

A lack of container availability has also seen costs of shipping rise, and stock availability issues have had an impact on margin.

The subsequent increase in costs and lead time of shipping has led to a renewed interest in overland supply routes.

Warehousing requirements have also increased as businesses look to increase their stock-holding or to cope with changing distribution methods. This move has created nationwide warehousing and staffing shortages.

Cyber threats are on the rise too, with 75% of larger business now reporting weekly incidents. Ransomware is seeing the largest increase. This is where the perpetrator effectively threatens the ability of a business to trade, usually during peak selling periods, encouraging the business to hand over money. Often these events stem from other seemingly lower level threats such as phishing.

Recently, Ransomware attacks have seen some businesses fail and others face significant costs to rectify the damage caused. Successful attacks where personal data is exposed can also attract the attention of regulators, leading to potentially large fines and reputational damage for the company.

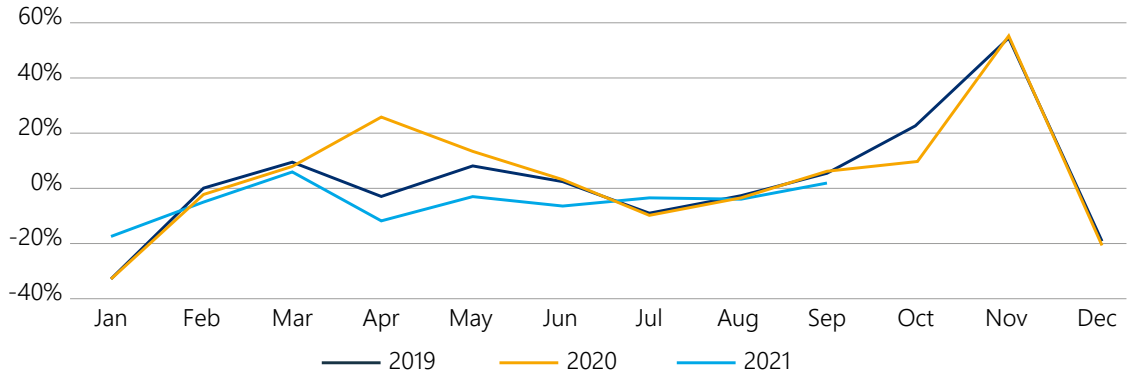
Mapping changes in online purchase behaviour

The chart on the right demonstrates month-on-month revenue from online purchases between 2019 to 2021, (this is specific to large retailers – those with online revenues of over £100m).

The line depicting 2020 shows a spike in online sales revenue between March and May, which was when the first lockdown occurred. As restrictions eased, this number fell slightly – in line with 2019 averages – before another peak in November around the Black Friday/festive period. In 2021, revenue grew at a rate consistent with 2019 levels – suggesting that demand continues to grow.

This increased level of demand, and the pace of change, has introduced some significant challenges to the retailer. Volumes have increased by such an extent that sourcing product has become more difficult, as has finding the people to pick, pack and dispatch items to the customer. The commercial success of the online retail industry has raised its profile in the eyes of criminals, putting businesses at greater risk of malevolent activities.

Graph 1: month on month revenue growth from online purchases



Supply chain risks

Mike Kay, Head of Lockton's Retail Practice says:

"Retailers are responding with characteristic vigour, adaptability and drive to transformations within their industry. It is vital that any changes retailers make to their businesses are reflected in their risk and insurance solutions. Particularly crucial areas for review are business continuity plans, business interruption insurance indemnity (time) periods, and cyber security. It is vital that retail boards understand the full extent of their exposures in these areas"

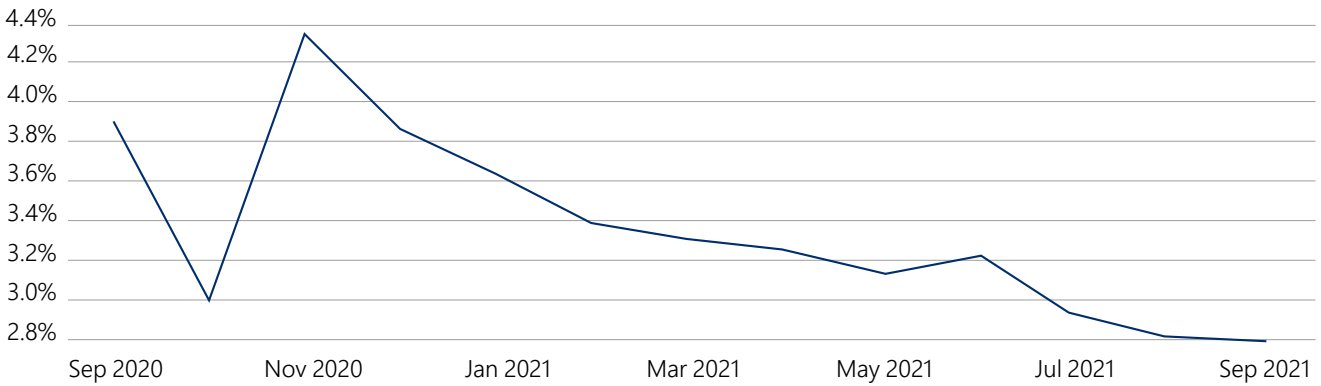
Recent events have shown the fragility of the supply chains that retailers rely on. Obstructions in key shipping channels, geo-politics interrupting finely tuned transport operations, rapidly increasing costs due to restrictions on supply chain capacity, and challenging domestic market conditions all contribute to a very fluid route to market.

Retailers often rely on long-term planning for product design, development, production, and fulfilment. Clothing retailers face the biggest challenges, as ranges change on a regular basis and are not always driven by key selling events, such as Black Friday and Christmas. With fashion collections turning over as often as six weeks, the supply chain has been developed to be flexible and responsive. This can also be a risk factor with supply being on a Just-in-Time (JIT) basis.

Other categories benefit from having a more stable promotional calendar, often set by the manufacturer / retailer themselves and built around key activities. Religious festivals and several defined sales periods are set in the calendar. Having supply issues around these times can cause significant hits on revenue and brand equity in the eyes of the customer.

The impact on stock can be seen in the chart below by the drop in conversion rate, which measures the percentage of site visitors who complete a purchase. Since April, it has been down by as much as 25% against the same months last year. For example, in September 2020 it was 3.9%, in September 2021 it had fallen to 2.8%. Small increases or decreases are not uncommon, but they are usually very marginal – a drop like this is unprecedented.

Graph 2: Monthly average conversion rate (total sessions)

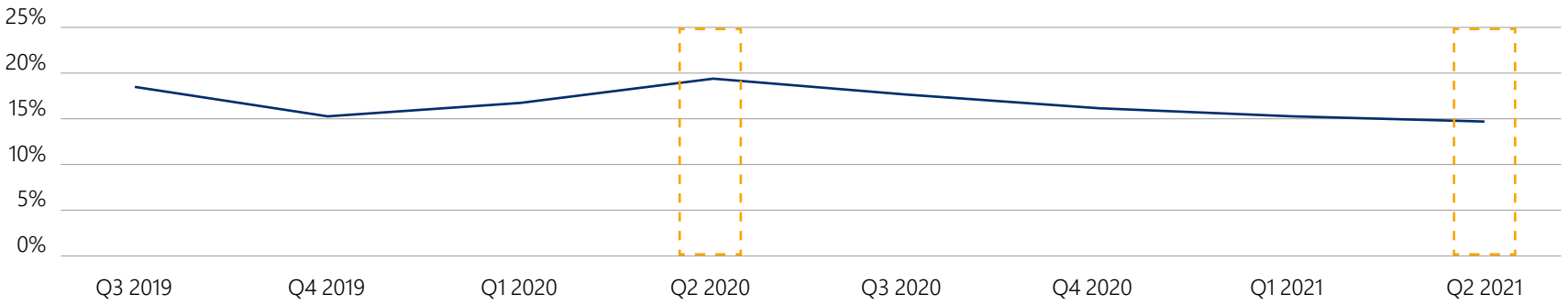


While the graph above measures overall conversion on sites, we can drill down into more detail around where exactly the drop-offs are happening. There are four stages of the 'customer funnel', which are:

- **Percentage of site visitors who view a product page**
- **Percentage of site visitors who add something to their basket**
- **Percentage of site visitors who proceed to checkout**
- **Percentage of site visitors who convert to payment.**

For three of these stages, in spite of the disruption of the pandemic, there has been very little change in the percentages between 2019 and 2020, and into 2021. For one stage, however, (the percentage of site visitors who add something to their basket) there has been a dip from around 20% in Q2 2020 to 15% in Q2 2021. This does suggest that stock availability is an issue, as the drop-off is happening on the product page.

Graph 3: percentage of sessions that convert from a product page view to add item to bag



Global risk factors

Global events may seem far-removed from the day- to-day workings of a retailer but, large or small, they can have a significant impact on the trading profitability of the business. In turn, many of these factors can influence consumer confidence and their propensity to spend.

Geo-politics – An increasingly nationalistic approach by many countries, including the US and China, is causing friction around technology, taxation and border disputes. BlackRock's Geopolitical Dashboard highlights US and China relations as a potential flashpoint, with the decoupling of technology systems increasing friction in cross-border trade and information sharing. A resurgence of Covid and its subsequent impact on supply chains is also flagged as a big risk over the next year.

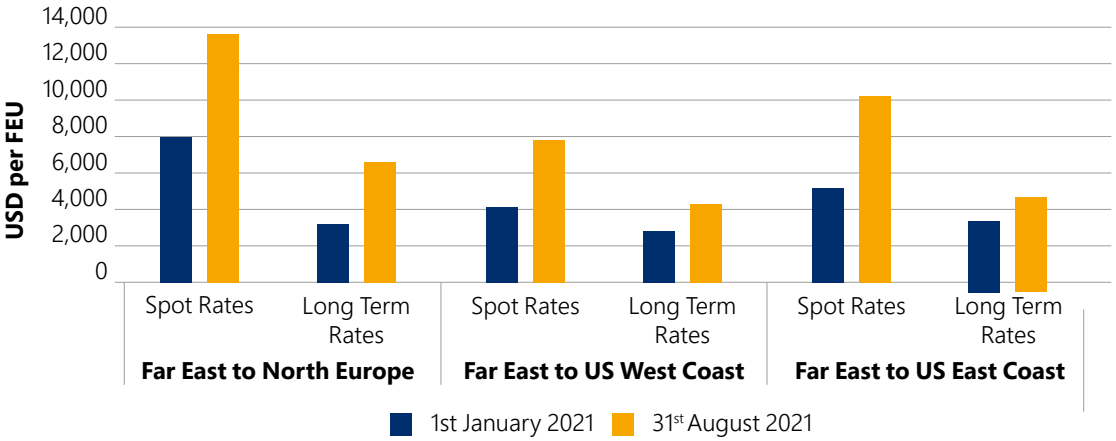
Availability of shipping capacity – Increases in consumer demand have dramatically changed the face of container shipping over the last decade. Tonnage available for shipping from the Far East to Europe has increased at a rate almost twice as high as volumes. Compared to July 2020, volumes are up by 13.8%, while they were up only 0.1% compared with July 20192. However, according to data from BIMCO3 (trade body for the shipping industry), the key bottlenecks aren't due to shipping capacity, but the shore-side ability of infrastructure to unload vessels and turn them around.

Reduced dock availability – Partially caused by the lack of staff availability due to the global pandemic and the increase in volumes, reduced dock availability is impacting how quickly vessels can be turned around. This exacerbates delays on vessels getting to the docks. Dockside backlogs are also causing a strain on customs procedures, meaning that containers are held for extended periods at the docks prior to being released.

Increased costs of containers and shipping – It has been widely reported that the lack of container availability has impacted the costs associated with their use. Data from BIMCO shows that the biggest increases have been on routes from the Far East to Northern Europe – already higher than global averages – due to political challenges and national lockdowns in Europe due to the Covid-19 pandemic.

Drewry shipping[4] – Consultants in the industry have reported that container prices are unlikely to normalise much before Q4 2022. 4 Whilst this provides a level of certainty in the near-term, it does indicate challenges for retailers in maintaining margin or price points.

Graph 4: container freight rates
Source: BIMCO, Xeneta



Changing global regulations – According to a report by CIPS, changing regulation is the fifth biggest challenge to global supply chains for 2022. 5 A sharper focus from regulators on labour conditions, due diligence and compliance requirements are likely to cause delays to the supply chain, as are increased occurrences of smuggling.

Domestic risk factors

Risks in the domestic market are often more impactful for businesses than global risks. However, recognising these and their potential influence can be challenging. Key risks that are currently impacting the UK domestic market include:

Political response to key threats – Keeping track of changes in regulations, particularly around HR, taxation, and sanctions can be difficult in a volatile political environment. Plus, changing relationships with global partners can rapidly impact the availability of product or staff – as illustrated with Brexit.

Availability of flexible staffing at peak periods – Given the difficulties retailers face in obtaining labour, retailers are likely to increase their use of robotics, particularly in warehousing. Administration roles and even remote control of automated machinery is likely to increase, thereby reducing a brand's exposure to staffing issues.[6]

Lack of capacity in warehousing – The rapid growth in of both B2B and B2C ecommerce sales, coupled with strained international supply chains necessitating increased stock holdings, means that UK warehousing facilities are close to maximum capacity. A recent report by UKWA showed that while there was a 7.5% space in a capacity of over 36 million square feet, 20% of the stock isn't fit for purpose.

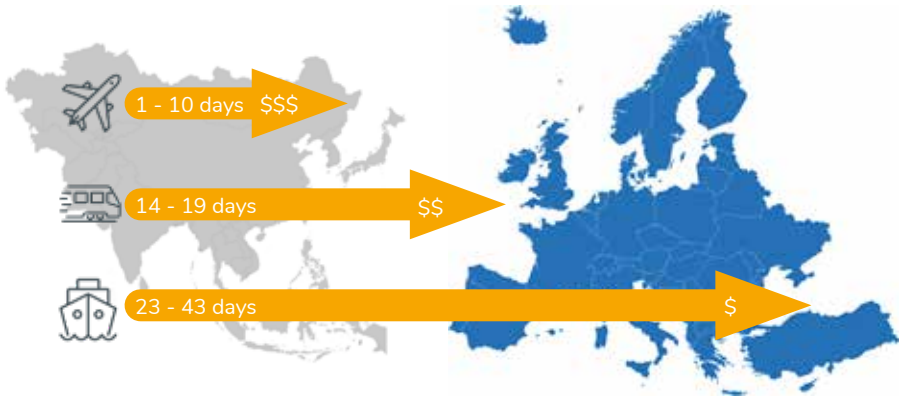
Warehouse outages – Smooth fulfilment processes are the key to all successful retail operations. Interruptions in these processes, whether caused by natural disaster or human intervention, can have a costly impact on a retailer. For example, since December 2005, ASOS has suffered three warehouse outages (Hemel Hempstead, Barnsley and Berlin) causing reported losses of over £42 million.8 These costs related to loss of stock, remedial action and lost sales where web sales were suspended.

Increased demand – Where it is unplanned, unexpected demand can provide additional stress on resources and impact the customer experience where stock is low. Recent growth in online sales, lack of trained HGV van drivers and reduced availability of spare van capacity has resulted in increased final mile fulfilment costs, which reduces margin. Staff shortages also mean those that might not have made the grade in previous years, are now being shortlisted for roles, with a potential impact on the doorstep experience that the customer has with the brand.

Mitigation activities

- **Just-in-time supply (JIT) chains** – are highly efficient when they work, but any interruption can cause lost sales, costing consumer confidence and margin.
- **Running an increased stock holding** is another possible solution. This reduces reliance on JIT but increases demand on capital expenditure (CAPEX). Balancing these two elements is key.
- **Ship earlier to ensure stock held in time for sales activity** - This increases availability of inventory but can damage cashflow.
- **Reduce reliance on shipping by investing in other means of transport.** China's Belt Road initiative is increasing train capacity from the Asian manufacturing centres. In 2018, over 6000 trains made the journey from China to Europe. Container Xchange reports that while lead times are shorter, costs are also lower, with current fees of a 40ft container at around $1,100 versus over $10,000 by sea. [9]
  Sino Shipping reports that trains from China to London are taking 16-18 days - depending on the point of origination.[10]
  UK retail brands, particularly grocers, are already increasingly using train freight as part of their supply chain mix. In October 2021, Tesco reported that it was increasing its use of trains to counter dwindling HGV driver availability and reduce its CO2 emissions.[11] It is currently running five trains per week from Spain with plans to increase services and volumes.
- **Reduce stock-keeping units (SKUs)** by focusing inventory on core product lines. By keeping stock collections limited to products that are closely aligned with the core proposition, businesses can ensure they are only keeping products that the customers expects of the brand, keeping excess stock to a minimum.
- **Ensure access to vehicles and appropriate drivers is secured ahead of peak trading periods** – This is a crucial consideration, but it is important to note that industry peers will be looking to do the same. Where deliveries are outsourced to carriers, look for guarantees around system capacity and delivery KPIs.
- **Long term planning for major disruptions.** Retailers can do this by diversifying their supplier base, not just across different manufacturers but also geographical locations. Planning for short-term shocks can be harder as the case for investment is often more marginal. However, the recent issues around fuel availability for motorists highlight the importance of this planning.

Estimated transit times from China to the EU.
Source: Sino Shipping & Freight Hub. October 2021



Mike Kay, Head of Lockton's Retail Practice says:

"Retailers should be thinking about how the fast-paced adjustments that they have been making to their business operations might impact their existing insurance arrangements. For example, they may need to review inventory/stock values to ensure policy limits are not being exceeded. In some instances, a change to supply strategy and corresponding exposure timeframes would need to be disclosed to insurers."

Cyber risks and security

Mike Kay, Head of Retail Practice at Lockton says:

"Companies that haven't yet implemented robust cyber security policies and procedures are vulnerable to cybercrime. Many organisations think they are not necessarily a target for criminals as they are not a well-known brand, but cyber criminals can and will hit anyone without discrimination."

Cybercrime and cyber-enabled crime is increasing both in terms of frequency and impact.

Cyber-crime is a term used to describe criminal activity that involves technology damaging business activities. Activities falling under this description include Distributed Denial of Service (DDoS), ransomware, hacking, and malware. Cyber-enabled crime covers actions that involve the use of technology to exploit physical weaknesses. For example, an employee using company systems to conduct fraud. The systems themselves aren't always compromised but are used to circumvent access or procedural controls.

According to the UK Governments Cyber Security Breaches Survey 2020, 75% of large businesses reported that they had experienced a cyber-attack over the last 12 months.[12] Of these, 32% were experiencing more than one incidence per week. Looking at the nature of the threats, phishing attacks rose (from 72% to 86%) whilst there was a fall in viruses or other malware (from 33% to 16%).

BlackRocks' Global Risk Dashboard shows the likelihood of cyber-attack as one of its highest risk factors for the coming 12 months, either from state actors or independent hacking groups. A recent report on CNBC highlighted a Russian speaking group that is responsible for a large proportion of Ransomware attacks, earning tens of millions of dollars per month from extortion fees.[13] Ransomware groups target businesses when they have the most to lose, during promotional or peak trading periods.

With regards to costs to the business, these include material and reputational costs. Material includes funding remedial activity, forensic investigation and loss of finances or data. Loss of finances obviously has an immediate impact. Loss of data may lead to further investigations and potential fines from the regulator. Reputational costs could include public relations, customer contact, lost sales and issues finding new customers in the future.

The direct and indirect costs of recovering from a cybercrime can be substantial. While the individual material costs may be relatively low (at an average of £13,000, according to a UK government survey), if these are happening on an increasingly regular basis, the cost to the business soon becomes more significant. Of course, this doesn't consider the unknown costs of reputational damage.

Many of the risk points include the potential for reportable data breaches. On its own, the internal and external reporting required for data breaches can add substantial cost to the underlying cyber issue. This doesn't consider the increased potential of a regulator audit and risk of fines up to 4% of global turnover. The ICO is regularly acting and fines of £20 million have been issued.[14] Even in situations where there has not been a breach but a lack of control is highlighted, fines been made in the excess of £100,000.[15]

Mike Kay, Head of Retail Practice at Lockton says:

"Insurers are looking to implement a series of minimum security standards, without which companies will not be able to obtain cyber insurance."

"As underwriter scrutiny continues to play out, cyber risk needs to be addressed by retailers at c-suite level; failure to do so will affect a business' ability to transfer cyber risk and may create exposure for directors and officers who fail to mitigate and manage cyber risk effectively."

Mitigation activities

As threats become more common, it is becoming harder to purchase insurance against certain cyber risks.

Insurers are increasingly turning to retailers to prove that they are trying to mitigate their cyber risks.

The application of standards such as ISO 277001 (framework to framework for an organisation's information security management system), GDPR and PCI DSS, help mitigate risk thereby providing more confidence to the insurers.

Popular mitigation strategies

IMRG conducted a survey amongst its retailer members to determine the most popular mitigation strategies, detailed below.

Multi-factor authentication - Of the retailers who responded to the survey, 59% had introduced multi-factor authentication for access to key systems. Email software often provides this functionality and its use is being promoted to users via online payments.

Endpoint security - About a third of the retailers have also implemented endpoint security. According to McAfee, "endpoint security is the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns."[16] Given the nationwide increase in working from remote locations through a variety of devices, the opportunities for malign actors is increased, particularly as physical security at remote locations is often lower than at business premises.

Training - 65% of the retailers surveyed also carried out regular training and awareness programs to keep colleagues abreast of requirements. With most cyber threats, the human element is often the weak link. IBM reported that human error was a major contributing factor in over 95% of all cyber-attack. [17]

NCSC (National Cyber Security Centre) recommend four key steps for businesses to protect themselves:[18]

1. Make regular backups
2. Prevent malware from being delivered and spreading to devices
3. Prevent malware from running on devices
4. Prepare for an incident

Because cyber risks affect so many operational areas, there is a need for mitigation to be coordination at board level, particularly as many cyber-attacks have the potential for significant financial impact.

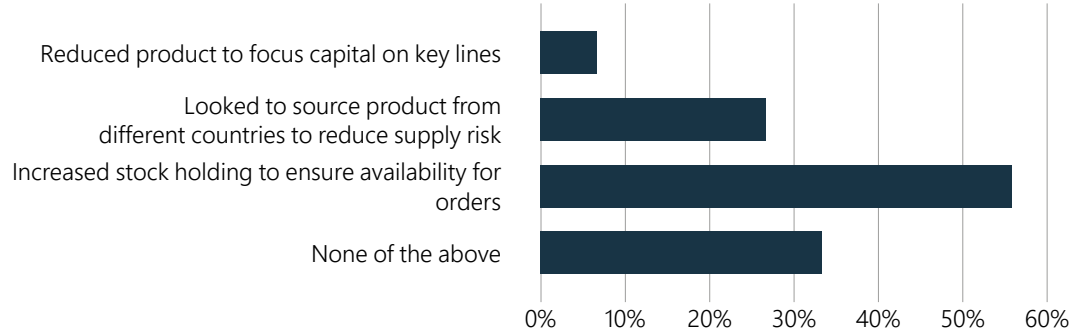
How are retailers managing threats?

To assess the ways in which venders are dealing with the current issues and threats impacting industry, we ran a poll of 42 retailers.

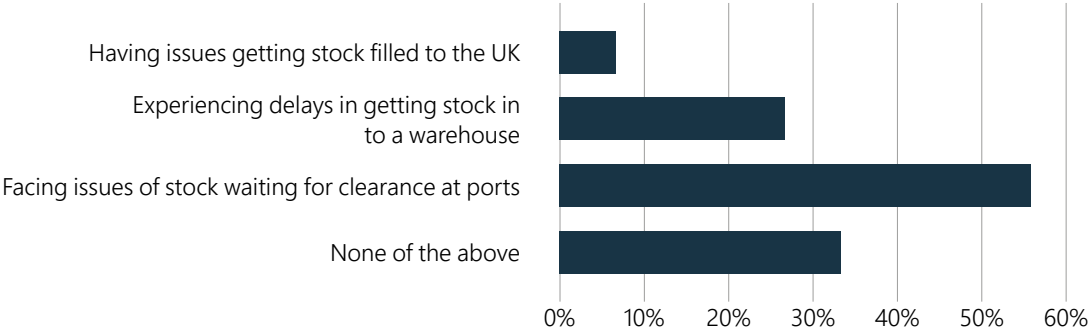
The majority of retailers said they were increasing stock holding to ensure the availability of their orders, with 55% of respondents adopting this technique. 27% were sourcing products from different countries to reduce supply risk, and under 10% of respondents said they would be reducing their product range to focus capital on key lines. 33% of respondents were not implementing any of the mitigation strategies listed.

When it came to the issues they were facing, 50% of respondents then commented that they were experiencing delays in getting stock into the warehouse, making it the most prevalent issue. A further 43% said they had stock waiting at ports, and 32% said they had issues with stock getting to the UK. The retailers experiencing none of these issues were in the minority.

Graph 5: Looking ahead to peak trading and taking into account the current supply chain issues, have you (select all that apply):



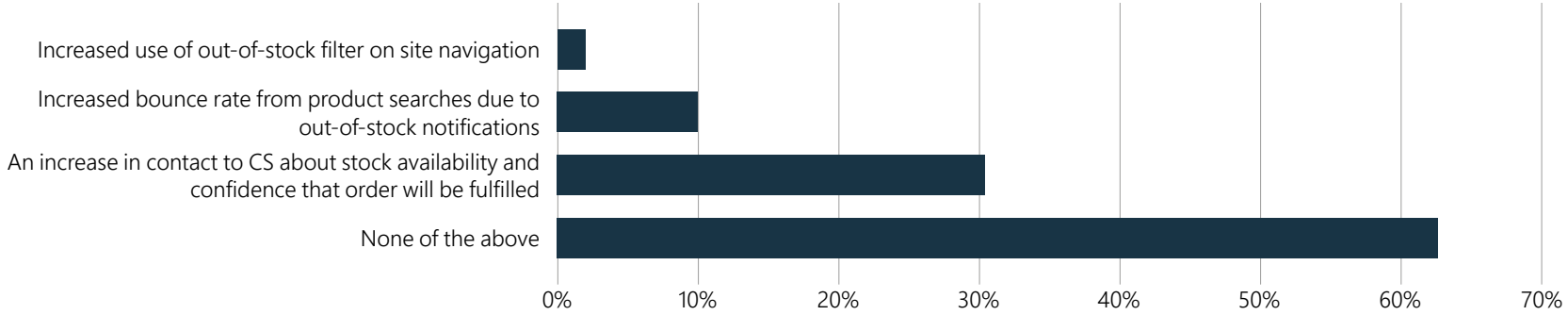
Graph 6: With regards to the current situation are you:



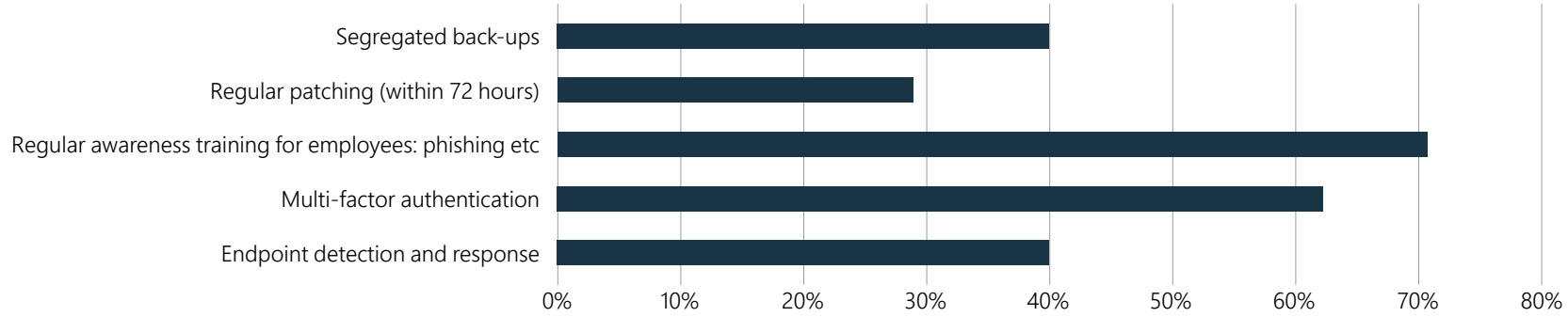
When it came to the customer funnel, we saw that retailers were experiencing fewer issues at this point in the process. However, an increase in contact with customer service around stock availability affected 31% of retailers, making it the most predominant problem.

The fourth question asked what measures retailers had in place to demonstrate minimum levels of cybersecurity. The most common were regular awareness training for employees (71%) and multi-factor authentication (62%). Regular patching was used the least, suggesting it is not as effective or popular.

Graph 7: Looking at the customer funnel, have you noticed:



The insurance market will seek to limit or withdraw ransomware coverage from xyber policies, unless you can demonstrate certain minimum levels of xybersecurity. How many of the following does your company have in place?



Conclusion

While geo-politics, global shipping disruption and catastrophic cyber-attacks might seem surreal for most UK-focused businesses, the potential impact on profitability is very real. This report has highlighted some key risk areas for businesses to look at going into 2022. The key focus should be on resilience; with shocks to global markets becoming more regular, it's crucial to for businesses to invest in effective risk management strategies in order to mitigate the effects and continue to thrive.

Executive board actions

Successful risk mitigation strategies will need to be driven by the executive team. Some key action points for consideration include:

Supply chain

1. Review impact of stock availability and increased supply chain costs on profitability
2. Increase planning and buying cycles to improve stock availaibilty
3. 3Calculate CAPEX requirements for increased stockholding and longer lead times
4. Assess supply chain for resistance to short term shocks and budget for remedial activities

Cyber risk mitigation

1. Ensure accurate and regular reporting to board on cyber threats and attacks – include impact assessments
2. Plan and invest in protection strategies, business continuity planning and the role insurance can play
3. Understand the potential regulatory impact of a successful attack. For example, an event that leads to a data breach, regulatory investigation and potential for large fines

About IMRG

We help our members understand and improve their online retail performance through a busy programme of performance benchmarking, data analysis, insight, best practice-sharing and events. We have been tracking online sales since 2000 – and now measure over 120 individual metrics in a series of indexes, providing in-depth intelligence on online and mobile sales, delivery trends, marketing ROI and channel performance.

Download more reports and view our event calendar at www.imrg.org.

About Lockton

As the world's largest privately held, independent insurance broker, Lockton provides best-in-class risk management and insurance solutions for clients.

- Over 8,500 associates
- Exceptional client retention rate (97%)
- Over $39.5 billion premiums placed
- Clients in over 125 countries
- Over 65,000 clients
- Over 100 offices worldwide
- 13.4% annual organic growth since 2000
- $2.16 billion revenues
- 90% reinvestment due to our private ownership

*Our **97% client retention** rate speaks for itself.*

To find more about Lockton's Retail Practice please click here

Further Reading

[1] Geopolitical Risk Dashboard | BlackRock Investment Institute

[2] Container shipping - onshore disruption leading to record delays and profits (bimco.org)

[3] Container shipping - onshore disruption leading to record delays and profits (bimco.org)

[4] Shipper hopes dashed with prediction of no supply chain recovery before Q4 22 - The Loadstar

[5] Five trends impacting global supply chains in 2021 - Supply Management (cips.org)

[6] 5 key trends in warehousing for 2021: from social distancing to flexible working. (replgroup.com)

[7] UKWA highlights crucial shortfall in warehousing capacity – UKWA

[8] https://news.sky.com/story/asos-warehouse-fire-cost-up-to-30m-10389648
https://www.reuters.com/article/uk-asos-fire-idUKKCN18C1DG
https://www.businessoffashion.com/articles/news-analysis/asos-warehouse-fire-destroys-stock-worth-8-million

[9] Rail Freight | Overview, Rates and Companies - Container xChange (container-xchange.com)

[10] Rail freight from China to Europe - Rates & Transit Time | Free Quote | Sino Shipping - Sino Shipping (sino-shipping.com)

[11] Tesco credits use of rail freight for keeping shelves stocked in supply crisis | Tesco | The Guardian

[12] Cyber Security Breaches Survey 2021 - GOV.UK (www.gov.uk)

[13] https://www.cnbc.com/video/2021/10/07/heres-what-to-know-about-a-ransomware-group-thats-targeting-the-healthcare-industry.html

[14] British Airways | ICO

[15] Enforcement action | ICO

[16] What is Endpoint Security? How It Works & Its Importance | McAfee

[17] Why Human Error is #1 Cyber Security Threat to Businesses in 2021 (thehackernews.com)

[18] Mitigating malware and ransomware attacks - NCSC.GOV.UK