MARSH

INSIGHTS | NOVEMBER 2019

New Retail Risks, New Strategies: 100% Confidence in Your Risk Protection?

Competition in the retail environment is brutal. Old, new, big, or small, in the fierce fight for survival, operators can be pushed out of business as is evidenced by the huge number of physical-store closings over the past year. Meanwhile, the use of technology and rapidly changing consumer habits are creating a new risk environment.

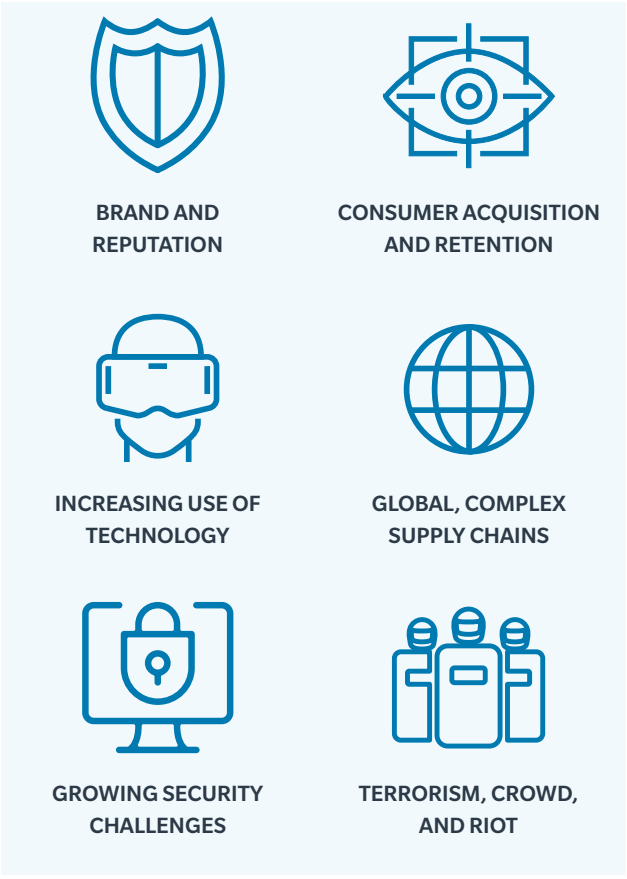
Retailing Today, Drivers of Change

Retailers today are seeking new ways of working, aligning their business models to the modern world. Successful retailers of the future will be those who position themselves to both respond to and master the highly dynamic marketplace in which they operate.

The retail environment of the future will increasingly see retailers operating smaller physical stores, with online stores being used to capture trade – this will force retailers to reconsider their virtual-physical mix.

This new mix comes with a set of modern challenges and presents yet more to consider from a risk perspective.

Old world risks such as the loss of a store or distribution centre due to fire or explosion remain, but are likely to be well managed. Goods in transit will be a well-oiled machine and employee risk will be woven into daily procedures. Those responsible for insurance have to find resolutions for new world risks previously incompatible with the traditional market. This disruptive environment creates risk implications for retailers and their trading partners, a more complex environment than ever faced before. The questions we need to ask are what impact is this evolution having on the retail landscape, and are "new" world risks, such as a malicious cyber-attack, or a knife wielding assailant considered under current arrangements?



MARSH & McLENNAN COMPANIES

CYBER ALERT

Cybercriminals have developed a wide range of methods to access data whether through web-application attacks, attacks on point-of-sale environments, denial-of-service attacks such as physical disruption to automated picking systems in distribution centres or disruption to online sales platforms and payment card skimmers. The list continues to grow. Employees are increasingly also falling victim to social engineering fraud whereby fraudsters deceive and manipulate victims into voluntarily performing actions which result in them giving out confidential information or transferring funds. Gaps in governance and control structures due to the reliance on third-party vendors also increase the risk of significant business impact of key systems not being available. Data breaches are complex concerns, often involving a combination of human factors, hardware devices, exploited configurations, or malicious software. Cybercriminals will inevitably target weaknesses in the interconnectivity between networks and processes: this has the potential to significantly disrupt operations throughout the organisation.

Reputations are regularly destroyed as a result of unexpected events.

Brand and Reputation

A firm's brand and reputation are its most valuable assets — a statement not lost in today's retail environment, given the advent of social media. Brand touches all things and is a clear driver behind growth, revenues, and the very survival of a company. As the marketplace becomes more dynamic, organisations must be able to rely on the power of their brand and reputation to attract and retain customers, business partners, employees, and shareholders.

Reputations are often destroyed as a result of unexpected events and how they are handled. Many external factors that are outside of an organisation's direct control also impact brand. Therefore, risks around brand and reputation are complex, difficult to measure, hard to predict, and often a result of strategic and operational decisions. Brand reputation is a fragile asset that is not easily fixed when compromised. Intangible damage to a company's brand could directly impact financial performance.

Adding the speed of social media into the mix creates an environment that can change at rapid pace. The erosion of trust and destruction of company value can occur in minutes and seconds.

Retailers need to be able to react at speed to brand-impacting threats. Having the right protection and crisis management plans in place is therefore imperative. Research indicates that those retailers who respond positively to threats often thrive post-crisis.

It's All About the Consumer

A core factor in this new risk environment is the consumer's evolving relationship with the retail sector. Retailers today operate in an environment where the consumer is more informed and connected than ever before. The key challenge now relates to the extent to which consumer expectations have been raised by digital retailing: 24/7 availability, online price comparison checks, personalised product suggestions/influencer and consumer reviews, and the demand for visibility into product provenance. They are increasingly snared by convenience, availability, and experience. Pop-up stores and virtual promotional sites targeting different segments and consumers will progressively become a significant part of the mix. As retailers morph into purveyors of experience rather than just a product marketplace, the future landscape will involve the navigation of increasingly complex operational, financial, and brand models in a more consumer-centric space. The need to remain agile in appreciating and acting on business model differences based on culture, distribution channel, and history, will be imperative.

Technology, Big Data, and Security

The speed and adoption of technology in the retail marketplace have increased radically in the past few decades. Evolution of the internet, smart devices, and social media has permitted new players to challenge well-established companies by utilising new ways of trading and communicating with the customer. As well as utilising technology in warehouses, for order fulfilment, and for logistics, companies are also experimenting with drones, robots, and driverless vehicles to make deliveries without human intervention.

Retailers are continuously and incrementally improving and updating legacy systems to cope with new ways of working. This often results in an inefficiency in the codebase that compounds over time. These changes leave systems open to attack, especially when outdated infrastructure is added to the mix.

The increasing use of technology means that retailers now collect, store, and leverage more consumer data than ever before across a wide-spanning range of digital platforms. Retailers now have a deeper understanding of individual preferences to make predictions and personalised product selections. This amplified data exchange creates a corresponding rise in the need to navigate new regulatory issues around data collection and the management of vast amounts of personal data. Accessibility versus security will be a trade-off to consider given the consequences to brand and reputation if that data is leaked or stolen. Data breaches have a detrimental effect on retailers[i] – heavy fines under domestic and European legislation and significant profit losses stemming from the disruption to operations and the loss of customers are becoming prevalent.

Mother Nature and Unpredictability

The recent collapse of many retailers has highlighted the current vulnerability of the UK high street. Adding Mother Nature's unpredictability and changeable climate into the mix has magnified the level of uncertainty for bricks and mortar retailers. Changeable weather can have a severe impact on shopping activity, whether it is snow preventing people from getting to the high street, an early hot summer, ash cloud, or an unseasonal wet spring. The UK has one of the most variable daily weather patterns in the world, and it is the topic of obsession for many Brits. Periods of extreme weather and events such as the "Beast from the East" in 2018 are the stuff of nightmares for the high street. IPSOS figures revealed that across the country, footfall in non-food stores was down more than 30% between Tuesday 27 February and Thursday 1 March 2018, when compared to the same period in 2017.[ii] The figures show that non-food retailers were particularly impacted as people stayed at home, rather than venturing out for non-essential items.

Retailers are becoming savvy in developing strategies to cope with unpredictable weather. A more robust focus on supply chain management and forecasting to aid stock rotation schedules will be essential, while a better merchandising and buying strategy will help to ride short-lived weather blips. Retailers with robust forward planning and risk analysis will also be able to take advantage of these weather extremities. Parametric weather solutions will utilise real-time data on weather conditions, with solutions linked to the trading environment.

Retailers require a more robust focus on supply chain management and forecasting.

The World Is Getting Smaller

Supply chains today are becoming increasingly complex as retailers operate in an ever more competitive global market. With growing inflationary pressure on raw materials, retailers need to consider how best to optimise their supply chains and sourcing agreements to meet fast-evolving consumer demand, while minimising costs to achieve profitable growth. To meet this challenge, retailers will need an innovative approach to sourcing, replenishment, and distribution. Successful retailers will be those who respond to consumers' demands for specialised products and who offer more product availability at cost-effective prices. For some, a nimble supply chain that is networked globally will become crucial, but for others that supply chain will need to be intensely local and sourced closer to the point of final distribution. Technology and the increasing use of analytics will improve tracking and traceability will help to drive efficiency throughout the supply chain. Data will be increasingly used for demand planning and to factor in volatile weather or regulatory changes.

Increased interdependency between companies will result in new risks to business. Previously a fire or explosion would have only affected one or two companies; with global supply chains, losses today increasingly impact a significant number of companies and can even threaten whole industries globally. Recent examples – such as the 2011 Japan earthquake and its effect on the semiconductor industry,[iii] and the shock to the retail supply chain following the bankruptcy of Hanjin Shipping[iv] – show how today's interwoven supply chains are creating a ripple effect on risk. Appreciating the full range of potential business income loss from property damage, disruption of the surrounding area, or closures by order of civil authority is a complex task.

Terrorism events can cause significant business interruption and denial of access costs.

Retail, Terrorism, and Crowd Riot?

The UK's intelligence services are facing an "intense" challenge from terrorism with terrorist activities more frequent than ever before, making it progressively difficult for those looking to counter them.[v] Such attacks have been classified as "lone wolf" events, which has ramifications for those with terrorism cover. Several of these attacks have taken place in the UK, including the Manchester Arena, two shopping malls in London, London Bridge, and Borough Market. These attacks have been characterised by the perpetrators using vehicles as weapons, and by the use of explosives and hand weapons. Elsewhere in Europe, a vehicle attack in Barcelona and a knife attack in Finland in August 2017 further supported the trend towards lone wolf incidents. These events caused significant business interruption and denial-of-access costs – several businesses were located in the areas cordoned off immediately following the London Bridge/Borough Market attack, for example. Organisations may also face additional costs in the wake of an attack from implementing additional security measures, counselling, and public relations, as was seen by those affected by the Salisbury poisoning incident. It has been estimated that footfall in the retail and tourism sectors of Salisbury fell 40%–50% due to a fear of contamination and the perception that businesses were difficult to access or closed.[vi]

Similarly, one of the busiest shopping days of the year, Black Friday 24 November 2017, took a dark turn following reports of gunfire at Oxford Circus. Police responded to emergency calls and social media reports of shots fired at Oxford Circus that resulted in officers evacuating nearby tube stations. Panicked shoppers and commuters were told to stay inside until further directed, and to avoid travelling to the Oxford Street area, causing an interruption to trading on one of the busiest days of the year.[vii]

Understanding Insurability Exposures

In order to properly manage these potential causes of disruption to both the physical and virtual elements of the business, it is important to understand the range of indirect events that could affect the business, particularly when absent from a traditional physical damage trigger. Risk managers will need to be more confident in understanding an organisation's business model and strategy to appreciate future ways of working. They must be able to identify not just the risks to the tangible assets of the business, but also the risks to earnings, cash flow, and reputation.

It is critical to develop workstreams that identify, assess, quantify, and treat these new risks:

- A deep dive into each of the top emerging risks is required and will provide an initial steer to prioritise next steps.
- Quantification can then be completed focusing on a forward-looking view on severity.
- Solutions to finance risks that exceed agreed tolerances can then be considered. This could lead to the creation of new-to-market risk financing products, for example, those based on parametric triggers such as footfall changes or weather patterns.

Revisit Current Risk and Insurance Arrangements

A challenge to previous insurance purchasing decisions is essential to determine if they are fit for purpose in today's new trading environment. This may unearth potential insurance coverage gaps which would include:

Brand and reputation insurance solutions now exist to cover brand-impacting events. These solutions provide crisis response and a loss of profit indemnity.

- Cyber insurance, which has evolved to cover not just data breaches but technology-driven business interruption.
- Non-physical damage business interruption policies, which can provide coverage for loss of revenue without a physical damage trigger.
- Parametric insurance solutions for pandemics and epidemics, which can be triggered by changes in public sentiment rather than direct physical losses.
- Contingent business interruption coverage, which can protect against physical damage suffered by key suppliers.
- Political risk and trade credit insurance, which can cover exposures related to government actions, instability, and insolvency.

Conclusion

The most successful retailers will be the businesses who react quickest to the dynamic marketplace. They will obtain deeper data than their competitors and use it to deliver superior products to their customers. Prepare for the unexpected. With risk profiles increasingly interconnected in today's rapidly changing world, survival will depend on how resilient organisations can be to manage disruption, no matter its source.

The right mix of traditional and advanced risk mitigation and risk transfer strategies is pivotal to protecting future enterprise value.

THREE TAKEAWAYS

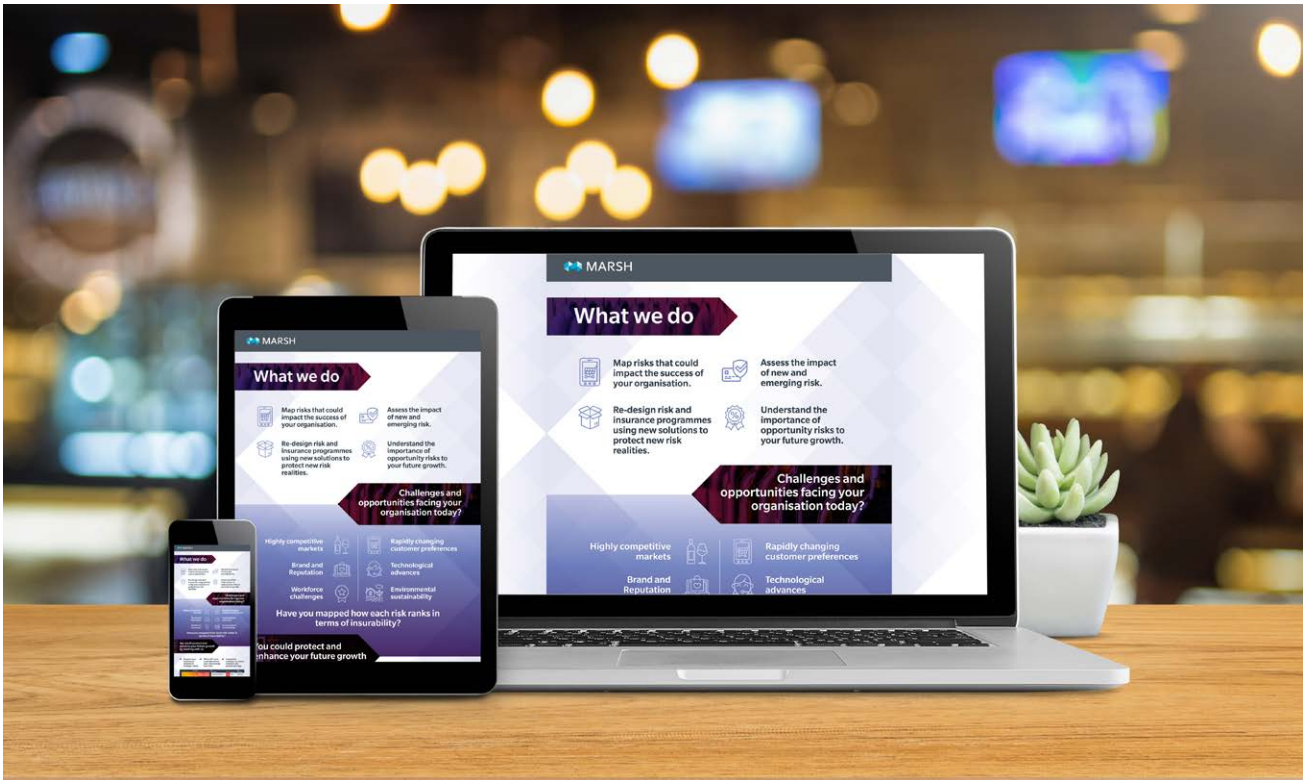
1. Establish processes to identify new and emerging risks.
2. Create and implement solutions for emerging risks that exceed risk acceptable thresholds, including those previously considered "uninsurable".
3. Ensure risk financing programmes move at pace, aligning protection to match risks created by the highly dynamic retail environment.

Next Generation Risk Protection

As companies look to dynamic futures, mapping out the road ahead to identify, quantify, and treat new risk landscapes will protect growth and reduce earnings volatility and build resiliency.

This will typically encompass evaluating how to allocate risk and insurance spend between "traditional" property and casualty solutions and "new" cyber, brand, reputation, and non-damage business interruption solutions.

TAKE A LOOK AT OUR TOOL FOR A DEMONSTRATION OF OUR APPROACH.



For further information, please contact your local Marsh office or visit our website at marsh.com.

DAVID TATE
Retail, Food, Beverage, and Leisure Industry Practice Leader
Marsh UK and Ireland
+44 20 7178 4355
david.m.tate@marsh.com

---

i. ICO. "Guide to the General Data Protection Regulation (GDPR)", available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/, accessed 29 June 2018.

ii. IPSOS. "How Can Retailers Beat a Big Freeze", available at https://www.ipsos-retailperformance.com/resources/blog/how-does-weather-affect-footfall/, accessed 29 June 2018.

iii. Lohr, S. "Stress Test for the Global Supply Chain", available at https://www.nytimes.com/2011/03/20/business/20supply.html, accessed 29 June 2018.

iv. Associated Press. "Hanjin bankruptcy filing causes global shipping crisis, retail fears", available at https://www.cbc.ca/news/business/hanjin-shipping-financial-trouble-1.3746049, accessed 29 June 2018.

v. Corera, G. "MI5 boss Andrew Parker warns of 'intense' terror threat", available at https://www.bbc.co.uk/news/uk-41655488, accessed 29 June 2018.

vi. PooleRe. "Terrorism Frequency, Q2/2018", available at https://www.poolre.co.uk/wp-content/uploads/2018/04/Terrorism-Frequency-Report-April-2018.pdf, accessed 29 June 2018.

vii. Griffin, A. "What happened at Oxford Circus? Police explain incident that was initially treated as 'terror'", available at https://www.independent.co.uk/news/uk/home-news/oxford-circus-incident-what-happened-attack-terror-police-met-latest-updates-a8074751.html, accessed 29 June 2018.

The information contained herein is based on sources we believe reliable and should be understood to be general risk management and insurance information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such.

In the United Kingdom, Marsh Ltd is authorised and regulated by the Financial Conduct Authority.

Marsh Ltd, trading as Marsh Ireland is authorised by the Financial Conduct Authority in the UK and is regulated by the Central Bank of Ireland for conduct of business rules.

Copyright © 2019 Marsh Ltd. All rights reserved. GRAPHICS NO. 19-0666