MARSH

Retail, Supply, and the Digital Revolution

CONTENTS

RETAIL, SUPPLY, AND THE DIGITAL REVOLUTION

The retail industry is currently undergoing a significant transformation, as technological innovation drives change and alters the way retailers manage their operations and interact with customers. The ability to dispatch anything from any place to any destination within a short timeframe has resulted in a high dependence on connected systems for everyday operations. This report examines the complex challenges generated by supply chain digitisation and how the cyber challenge for retailers has evolved beyond threats to customer data.

"Innovation often brings new risks; there has been an increase in information security breaches caused, or enabled by technology meant to improve productivity and increase collaboration."[2]

FROM OMNI-CHANNEL TO...?

Currently, the key challenge for many retailers is the speed of progress. Omni-channel retail, the internet of things, and contactless payment systems are all integrated features of the retail environment today, yet a few years ago these terms were not well known outside of strategy teams and technology companies. The traditional economics of retailing are shifting, with brick-and-mortar retail being increasingly replaced by online experience as consumer demand-driven shopping takes hold. The shift has created a marketplace where single-channel and multi-channel have moved to omni-channel, as consumers want to engage with the retailer across many different channels with seamless interaction.

The role of the physical store will continue to evolve as retailers adapt their services to interact with customers in new ways. Retailers are now organising and planning their businesses around the customer experience rather than the retail channel, and are bringing traditionally disparate parts of the business together in order to enable real-time trading. Retailing today, therefore, needs to be understood in the context of the major drivers of profitability, productivity, payment, and personalisation[1], which shape the strategies and policies of the business.

PROFITABILITY

With sales increasingly moving online, the economics of the retail model will be more fluid than in the past.

PRODUCTIVITY

A greater emphasis will be placed upon productivity and efficiency as people, store, and logistics costs rise. This will be a challenge due to the integration of new technologies with ageing infrastructure.

PAYMENT

Mobile payments and the growth of online channels are stimulating retailers to rethink the in-store experience and the way payments are accepted.

PERSONALISATION

Consumers have become increasingly sophisticated, demanding personalised and bespoke products and services in an instant. Innovation, quality, and speed to market are crucial to today's retailer.

1. Deloitte. *Retail Trends 2016 - Redefining convenience,* available at http://www2.deloitte.com/uk/en/pages/consumer-business/articles/retail-trends-2016.html, accessed 12 July 2016.

2. HM Government/PWC, *2015 Information Security Breaches Survey – A Technical Report*, 2015.

RETAIL IN A DIGITAL WORLD

Every change in the retail marketplace demands greater efficiency on behalf of the organisation. From stock and consumer to warehouse and store, the demands placed upon systems and interfaces are more prominent than ever. Technological advances have allowed organisations to create greater efficiency across their supply chains.

Connected supply chain technology has already been integrated for the management of the warehouse, logistics, and distribution.

The greater challenge is in establishing real-time visibility across the whole supply chain and gaining one view of stock across multiple channels.

Effective stock analysis, inventory reporting, and accurate demand forecasting is critical if retailers want to capture and retain customers, along with ensuring the development, on-shelf availability, and production of latest trends to meet customer expectations for instant satisfaction.

Some retailers have been challenged by poor visibility and ineffective use of inventory due to a lack of sophisticated supply chain systems. The need for the automation of processes while drawing on analytics and algorithms to predict and supply customer demand is leading retailers to build a collaborative, digital, and demand- and data-driven supply chain.

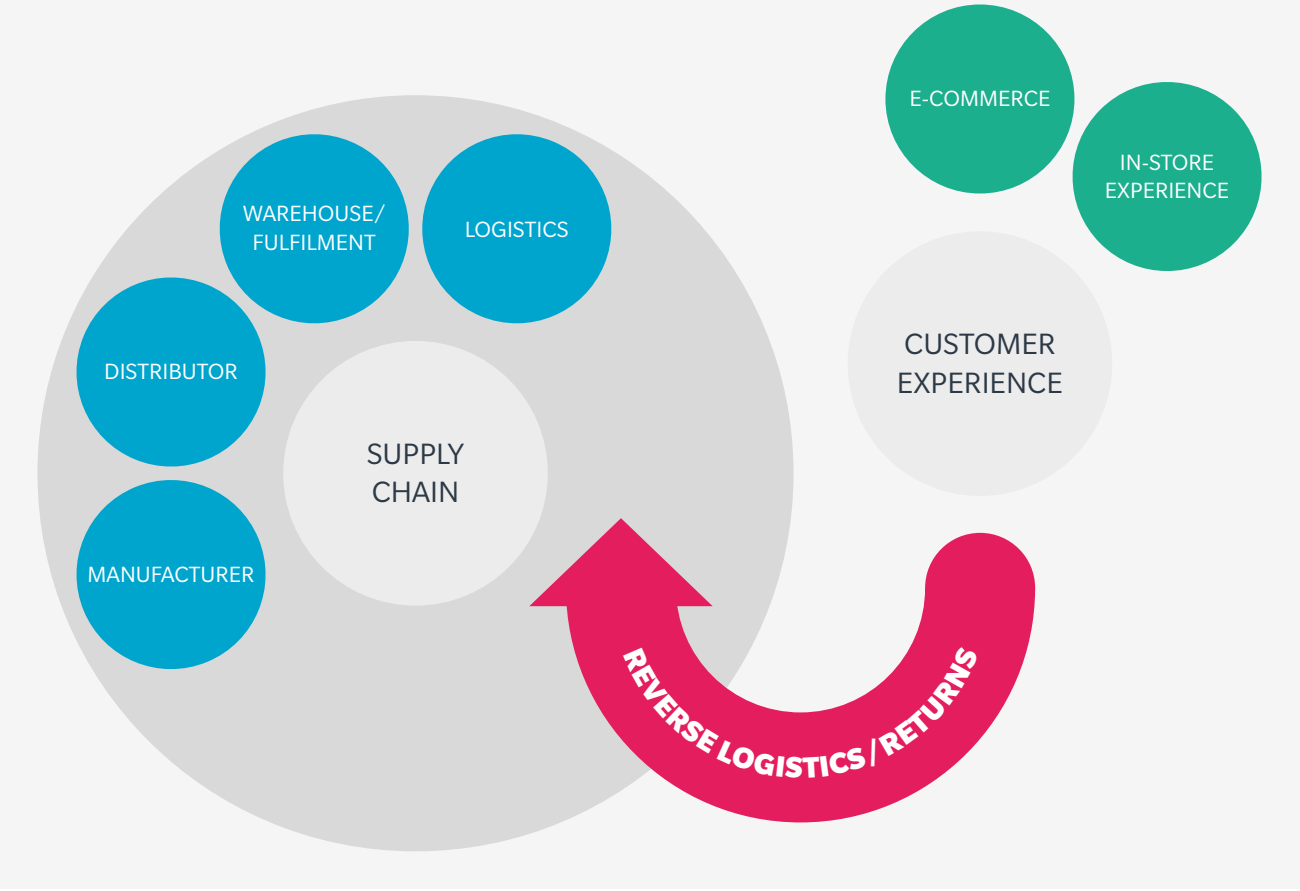
Forward-looking retailers are therefore improving inventory systems so that they can establish truly multi-channel supply chains to eliminate the need for separate online and high-street distribution centres. They are looking to focus on enhancing order fulfilment, establish inventory visibility, and ensure accurate demand planning and scheduling to cope with the control of stock across all channels.

However, as systems and processes throughout the supply chain are increasingly modified and integrated with technology to increase productivity and interconnectivity, new risks and previously unknown risks are presented, meaning retailers are increasingly vulnerable to information security breaches and other cyber-risks.

"The related risks to the supply chain is several steps removed from the analysis and decision-making centre of a given organisation."[3]

3. Chatham House, *Cyber Security and the UK's Critical National Infrastructure*, available at http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r0911cyber.pdf, accessed 12 July 2016.

FIGURE 1 **The anatomy of the retail supply chain**
Source: Marsh Analysis



SPOTLIGHT

Retail and the March of Technology

Retailers are increasingly dependent on technology for all areas of their business, including:

- Monitoring trends/browsing activity.
- Engaging with customers – social media.
- Online marketing and order management.
- Point-of-sale payment technology.
- Inventory management and stock due diligence.
- Warehouse management.
- Logistics and distribution management.
- Order fulfilment.
- People resource management.
- Administrative functions – safety, finance, compliance, and vendor suppliers.
- Returns.

RETAIL AND THE CYBER THREAT – MORE THAN JUST CUSTOMER DATA?

The phrase "data breach" has become closely associated with retailers in recent years, with incidents hitting the headlines on an almost weekly basis. Research shows that retail and consumer goods companies are more likely to report cyber-crime than businesses from any other industry except financial services.[4] October last year saw one of the UK's biggest attacks, after mobile phone provider Talk Talk was the target of hackers who stole the bank details of more than 15,000 customers.[5] Meanwhile, hotel chain Hilton was the victim of an attack that infiltrated its point of sale terminals, giving hackers access to customer credit card information.[6]

A UK Government survey highlighted that 90% of large organisations reported they had suffered an information security breach in 2015, and 74% of small and medium-sized businesses reported the same – suggesting that these incidents are the norm rather than the exception.[7] The survey noted that, as well as the number of security breaches having increased, the scale and cost has nearly doubled. While organisations of all sizes continue to experience external attack, there appears to have been a change in the character of these attacks; both large and small organisations have been subject to greater targeting by outsiders, with malicious software impacting nearly three-quarters of large organisations and three-fifths of small organisations.

4. PWC, *Global Economic Crime Survey 2014*, February 2014.

5. BBC. *TalkTalk hack 'affected 157,000 customers'*, available at http://www.bbc.com/news/business-34743185, accessed 8 August 2016.

6. AFP. *Hilton hotels hit by cyber attack*, available at https://www.yahoo.com/news/hilton-hotels-hit-cyber-attack-231206086.html?ref=gs, accessed 8 August 2016.

7. HM Government/PWC, *2015 Information Security Breaches Survey* – A Technical Report, 2015.

8. NTT Com Security, *2016 Risk:Value Report*, available at www.nttcomsecurity.com/en/riskvalue, accessed 16 May 2016.

SPOTLIGHT

Cost of Losing Information

On average, respondents to an NTT survey estimate it would cost their organisation around

GBP 1.2 Million

to recover information lost during a security breach.[8]

SPOTLIGHT

Breakdown of Interconnected Systems

In order to mitigate against losses and develop business continuity plans, retailers using interconnected systems should consider the following questions:

- What would happen if your online fulfilment system is infiltrated?
- How would you operate if your stock management and warehouse system is shut down?
- What would happen if a key supplier has a cyber-attack with the loss of thousands of orders?

INTERCONNECTED RETAIL – A CAUTIONARY TALE

Breaches involving the hacking of customer data or payment details are, of course, of serious reputational concern. Damage to the brand and subsequent loss of shareholder value and profits could significantly impact a business in today's competitive marketplace.

A failure in any of these interconnected systems could have dramatic repercussions for the whole organisation. Some examples of the potential issues include:

ORDER FULFILMENT

Any disruption to a real-time view of orders or information on product availability could be damaging. Interruption to integrated orders from supplier, customer, and transporter could result in a disastrous loss of control across the supply chain and, in turn, a loss of sales and/or reputational damage from the breakdown in stock positions.

WAREHOUSE AUTOMATED SELECTION

Retailers are increasingly utilising automation to improve efficiency and lower costs, by reducing the reliance on manual pick-and-pack of stock for shoppers. Any failure in these automated systems could have severe consequences for the fulfilment of orders or movement of goods.[9]

LOGISTICS MANAGEMENT

Logistics management is an important part of a multi-channel strategy, involving transportation management and the tracking and reporting of shipments. Modern retailing is highly competitive, and logistics optimisation can act as a key differentiator. Any breakdown or disruption of the logistics operation could cause significant losses, especially for those involved in the sale of perishable goods.

INVENTORY AND DEMAND MANAGEMENT

Stock analysis and inventory reporting is essential to optimise stock at each stage of the supply chain. This ensures quick replenishment and can help avoid future shortages or delays. Disruption to any part of this stage of the supply chain can lead to stock not being in the right place at the right time, resulting in lost sales and a possible loss of future customers.

SERVICE PROVIDERS AND VENDORS

Weak links in the supply chain leave a retailer vulnerable to attack. In 2013, 110 million customers were affected by a breach at US retailer Target Corporation, which began with attackers obtaining legitimate network access credentials that Target had provided to one of its vendors. Customers were impacted because vendor's security was compromised.[10]

9. Ocado develops new robot system to pick and pack groceries, available at https://www.theguardian.com/business/2015/may/07/ado-develops-robot-system-pick-pack-groceries, accessed on 12 July, 2016.

10. The New York Times. *For Target, the Breach Numbers Grow,* available at http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0, accessed on 8 August 2016.

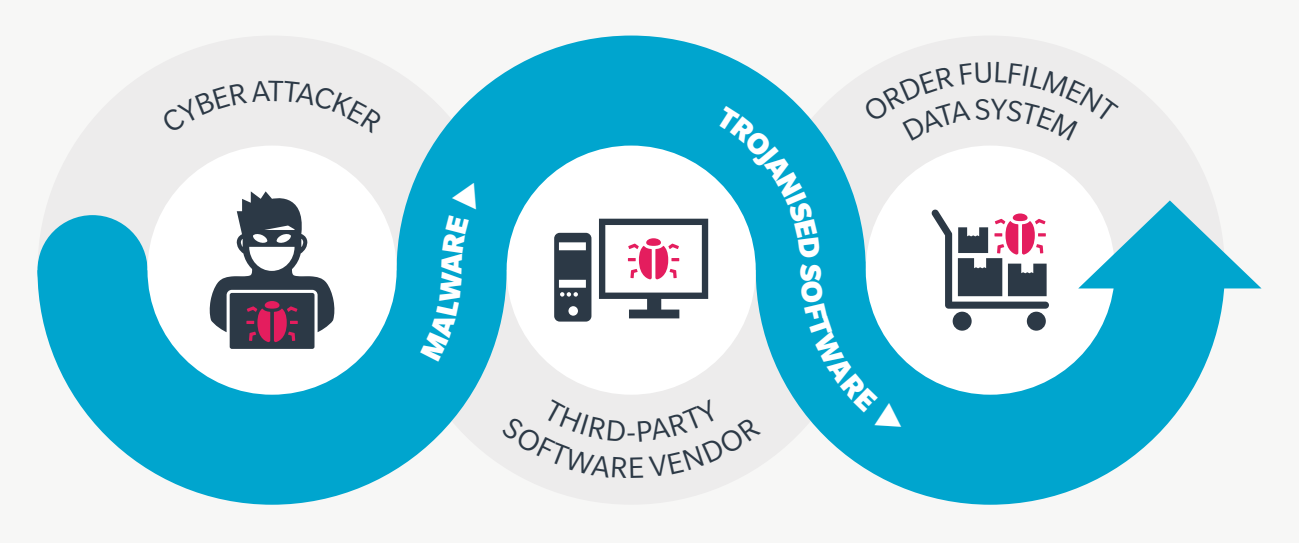
THE IMPACT – ATTACKING THE WEAKEST LINK

Increasingly complex technology and communication services are often outsourced by organisations in an attempt to reduce infrastructure costs or streamline operations. This decision immediately puts an organisation's infrastructure at risk as the threat is no longer *owned* by the organisation and its employees.

Cyber-attacks may reach an organisation through any number of vulnerable points along the supply chain, with too little overall oversight in the interconnected chain for failures to be identified. With information and security arrangements shared across a supply chain, the cyber-security of any one organisation within the chain is potentially only as strong as that of the weakest member.[11]

For example, this tactic has been used by the cyber-espionage group known as Dragonfly, which has targeted companies across Europe and North America, mainly in the energy sector, since 2011. Industry experts believe that pharmaceutical producers were the end target, as Dragonfly has a history of targeting companies through their supply chains. In its latest campaign, Dragonfly was able to "trojanise" legitimate industrial control system (ICS) software.[12]

FIGURE 2 **The weakest link – Third-party software providers**
Source: Cert-IK, *Cyber Risks and the Supply Chain*, 2015.



A cyber breach in the supply chain can have severe consequences involving:

- Disruption or a halting of business-as-usual operations.
- Damage to, or theft of, technology assets or infrastructure.
- Lost productivity.
- Loss of sales opportunities and/or loss of customers.
- Damage to stock.
- Remediation costs in the wake of a cyber-attack.
- Damage to a firm's reputation or brand and loss of shareholder value.
- Damage to competitiveness due to stolen intellectual property.
- Damage to competitiveness due to loss of commercially sensitive information.
- Loss of consumer confidence.

11. Cert-IK, *Cyber Risks and the Supply Chain*, 2015.

12. "Pharmaceuticals, Not Energy, May Have Been True Target Of Dragonfly, Energetic Bear", available at http://www.darkreading.com/pharmaceuticals-not-energy-may-have-been-true-target-of-dragonfly-energetic-bear/d/d-id/1316869, accessed on 12 July 2016.

MANAGING THE RISK – TO BE ADDRESSED BY DESIGN

The increasing sophistication of perpetrators and the interconnected nature of operations leave retailers increasingly vulnerable to advanced attacks. In an environment of operational efficiency, it is imperative that businesses change their approach to cyber-security, closely evaluating each business process. Cyber-security can no longer be the preserve of the technology department.

Recent cyber-breaches underscore the new reality in cyber-risk management; organisations now have to build a cyber-security culture. Everyone, from individual employees to risk managers, to the board of directors, now have a stake in managing cyber-risk effectively across the enterprise.

CYBER RISK – EVERYONE HAS A STAKE

While it will not always be possible to prevent every cyber-attack, it is vital that both the retailer and the organisations with which it does business have effective cyber programmes in place to better manage cyber exposure.

Retailers should consider taking the following steps:

- Understand the key cyber-risk scenarios you face.
- Consider the financial impact cyber-loss scenarios could have on your business, including third-party liability and business interruption.
- Work with risk advisers to analyse and document existing insurance coverage and identify gaps in current, and/or proposed new programme structures.
- Develop risk financing strategies for the identified and quantifiable risks, including the evaluation of cyber-risk retention – either on balance sheet or via a captive insurance vehicle and market-based risk transfer, or any combination thereof.

CONCLUSION – THE PATH TO CYBER RESILIENCE

Retail success in today's competitive marketplace is dependent on digital integration and innovation to retain and extend market share. Retailers now, however, need to consider their digital assets as more than just ways to increase online shopping as, in an increasingly interconnected world with supply chains becoming more complex, the very nature of their interconnectedness exposes companies to new cyber risks.

Addressing the issue of cyber risk must be integral throughout the organisation because, as digital becomes more pervasive, the risks will increase. The shifting cyber security landscape necessitates that cyber risk should be treated as a business issue as opposed to being the preserve of the technology department. Ownership for cyber security must now move to business leaders themselves.

Companies therefore need to take a more strategic approach to help identify, manage, and treat these new cyber threats. Being "cyber resilient" means having the ability to understand, prepare for, respond, and successfully recover from cyber breaches. Building a cyber-resilient strategy will ensure that risks are managed based on a business's individual tolerance for risk and will reposition cyber-security at the heart of an organisation, linking technologies and processes to the broader risk management activities of the organisation.

About Marsh

At Marsh, we have substantial experience in assisting retail companies to identify and evaluate the risks a company faces. Our Cyber Resilience team will work with your own cross-functional team, including members of your business, legal, IT, and risk management department. We will help you develop a clear picture of the key risks you face, understand what insurance coverage you may or may not currently have to protect you, and a plan to develop a bespoke cyber risk management programme that fits your needs.

About this report

This report examines how technological change is redefining the nature of risk in the in the ever-evolving supply chains of retailers. Marsh's UK Retail Practice believes that understanding and keeping at the forefront of technological change is key to providing the best client advice and enhancing the benefits we can deliver to clients' businesses.

MARSH

For more information, contact the colleagues below:

DAVID TATE

Retail, Food, and Beverage Practice Leader
Marsh UK & Ireland
+44 (0)20 7178 4355
david.m.tate@marsh.com

PETER JOHNSON

Senior Vice President
Marsh UK & Ireland
+44 (0)20 7357 3527
peter.a.johnson@marsh.com