The retail sector has been revolutionised by developments in the digital world, opening up a whole new way to access consumers through better quality data capture. It has also led to improved technology and efficiency both in-store and operationally. However, such changes have resulted in a high level of data retention and dependence on the internet and IT systems for everyday operations, including point of sale, stock management and supply chain — leaving retailers at the mercy of digital technology. As more retailers increase their IT capital expenditure to leverage intangible assets, many now see this as a strategic level risk which could cause major disruption, significant financial loss and lasting reputational damage, as demonstrated by recent data breaches.

Another common misconception is that most cyber incidents occur as a result of external hackers. In fact it is a combination of external hacking attacks (42%), internal negligence (such as lost laptops and files) or deliberate acts (such as insider collusion) (30%) and system glitches (28%)*. Often businesses will not know they have experienced a cyber breach until an external source notifies them, meaning that breaches reportedly take 240 days on average to detect**. This is a significant delay compared to the speed at which cyber hackers operate.

The assumption that responsibility for managing and understanding digital risks lies solely with IT departments is rapidly changing. There is growing recognition that everyone in an organisation should be accountable for cyber security, but despite this few staff tend to be trained on information security and many boards still lack a comprehensive understanding of it. This can be due to the technical language used to describe and articulate cyber exposures, as well as optionality around the disclosure of cyber breaches which can place less emphasis on actually addressing the issue.

Although investment in cyber security will not prevent against all eventualities – due to constantly evolving forms of malware and the impending threat of human error – managing digital risks effectively can significantly reduce the impact of cyber incidents.

Perception vs reality

There is a perception that IT failure and cyber crime is confined to a retailer’s trading website or the loss of data such as customers’ credit card details. The reality is that without its IT systems a retail business could cease to trade for weeks, resulting in huge financial losses due to lost revenue and the potentially extensive costs of hiring external expertise to fix technical problems.
Digital dependence
Retailers have become increasingly dependent on the internet and IT systems in all areas of their business, including:

- Office administration and general business functions (e.g. accountancy, law, marketing, sales and business strategy).
- Point of sale technology (e.g. tills, self-service check-out scanners and debit/credit card processing).
- Supply chain management.
- Stock control.
- Warehouse management.
- Distribution – including delivery to retail customers, wholesaling to other shops/businesses and to a retailer’s own outlets.
- New product design, assessment and marketing.
- Online marketing and website sales.

Who is at risk?
Due to the many types of digital risk exposures, retailers of all sizes and in all sectors are at risk, including:

- Local and international
- Department stores
- Homeware/DIY
- Food retailers
- Discount, value and luxury
- Clothing
- Motor trade
- Online
- Electrical

Legal responsibilities
There are certain laws and regulations that retailers, and those that service and supply them, must abide by and adhere to, including:

- Data Protection Act
- Law of Confidence
- Law of Contract
- Law of Tort
- Payment Card Industry Standards
- Financial Services Act
- Legal Services Act

In order to satisfy these obligations, effective cyber security measures must be implemented. Although not every law would apply to every business, all would be bound by one or more to maintain cyber security.

The risk from business partners
It is not enough for retailers to simply implement physical, technical and organisational security measures within their own businesses as the IT perimeter for cyber risk extends further than this. They must also focus on cyber security within the supply-chain and with service providers as interconnectivity between companies can pose a real threat.

The number and variety of business partners is vast and includes: suppliers, designers, marketing and PR companies, webhosting companies, cloud service providers, solicitors, accountants, surveyors, distribution and shipping companies, warehousing companies, IT supply and service companies, customers, banks/financial services.

What are the risks?

- Flawed Digital Strategy
- Loss or Theft of Confidential Business Information/Trade Secrets
- Failure of Interconnected Systems
- Loss or Theft of Personal Data
- IP Infringement
- Fraud
- Cyber Extortion
- Supply Chain
Flawed digital strategy
Retailers unsurprisingly tend to focus on the threat posed by unforeseen events, such as a hack or service downtime. However, with online trading contributing a higher proportion than ever of most retailers’ income, a badly executed strategy can have just as significant an impact.

A poorly received website revamp, for example, can have a material effect on a company resulting in a drop in sales and, in extreme circumstances, a fall in share price.

Loss or theft of confidential business information/trade secrets
Retailers handle a lot of confidential and commercially sensitive information, both their own and that of business partners. Such information could be useful to competitors as well as fraudsters, for example; details of suppliers, pricing strategies, current financial position, advertising and marketing campaigns, and any other information that is not publicly available. The risk of this information being lost, stolen and widely disseminated is exacerbated by the digital world within which retailers now operate.

Failure of interconnected systems
Computer based services are interdependent both within and outside an organisation. The failure of one organisation’s computer system can have a dramatic knock-on effect on all those with which it is connected.

The same is true of cloud service providers and webhosting companies whose services many retailers are dependent upon. Examples of such issues include:

- **Till or chip and pin machine failure** – prevents a retailer from scanning barcodes or processing credit/debit card payments.
- **Automated stock management system glitch** (software flaw or cyber-attack) – disrupts the supply-chain and can result in stock not being in the right place at the right time leading to lost sales opportunities and possible back-up of stock which can be costly, especially if goods are perishable and must be destroyed.
- **Website issues** (server down-time, denial of service and web app attacks) – results in the inability to process online sales.

Loss or theft of personal data
Retailers collect, maintain, transmit or store private information including potentially large amounts of consumer and employee data, as well as a significant amount of credit card information. This personal and confidential data may be shared between individual organisations and their supply chains, increasing the number of touch points and therefore the potential risk of a data breach.

IP infringement
IP infringement for retailers can include violation of design, copyright, trademark, domain name and copycat websites.
Supply chain
Retailers often have complex and diverse global supply chains, covering areas as varied as stock supply and credit card payments, making due diligence difficult and costly.

At the same time there may be differences in the quality of suppliers’ cyber security.

A weak link in the supply chain can leave retailers vulnerable to costly cyber attack.

Cyber extortion
Cyber extortion has become far more common in the retail sector, partly as a result of the low cost and easy availability of hacking tools which are simple for even the most technically challenged criminal to use. Denial of service (DoS) attacks can block access to essential systems and online trading platforms, leaving retailers unable to trade and at the mercy of cyber criminals. According to recent research, these actually account for 33% of cyber incidents in the retail industry***.

Fraud
Fraud is a huge concern for any company operating in the digital world but it is a particular issue for retailers thanks to their relatively high profile and online ubiquity.

It is important to bear in mind that most attacks on retailers are financially motivated. Point of sale intrusions, for example, despite falling in recent years, still account for 31% of cyber incidents in the retail industry while web app attacks account for 10% and are on the increase****.

Retail is also one of the industries particularly prone to payment card skimming, with fraudsters using stolen details from individuals’ credit cards to make purchases. This may take place in-store with cloned cards but increasingly this type of activity is happening online where a physical card is not required to make a purchase and appropriate checks are more difficult to carry out – the cost of such activity can be significant for a retailer.

What are the impacts?
The impact of any digital incident, especially if not handled correctly, can be catastrophic in terms of reputational damage and financial loss.

Some of the more obvious impacts on the balance sheet include: theft of cash; the inability to trade and associated costs of downtime; costs to repair or reinstate systems and operations; ransom payments to hackers (denial of service attacks); and regulatory fines for data breach of customer information.

There are also some less apparent costs associated with digital incidents which may include: opportunity costs following the loss of vital business and client information; non-delivery of stock or other essential supplies; and possible legal costs associated with defending issues such as IP infringement.

Other more intangible, but no less important, consequences should also be considered as these ultimately have a financial impact. Brand and consumer trust, for example, is an incredibly important part of being a successful online retailer and can be severely damaged following an incident. A retailer’s reputation can take years to build and, in the age of social medial, hours to destroy.

A significant loss of customer data or similar breach can mean that consumers lose confidence in a retailer, taking their business to a more trusted site. Damage can be exacerbated if an incident is poorly handled from a PR perspective.

Case study
Data breaches can result in a tarnished reputation, loss of customers and reduction in share price for retailers.

What happened?
The credit card and personal data of millions of shoppers at a large retailer was compromised due to a cyber-attack during peak purchasing season.

The impact
After the attack went public the company’s reputation and sales figures took a direct hit – they also experienced a decline in the share price. The CEO was dismissed as a result of the cyber-attack.

Lessons to learn
- Cyber security must be considered and implemented appropriately to reduce the potential exposure to malicious attacks as much as possible. The retailer in this instance had been warned prior to the cyber-attack that its point of sale terminals were vulnerable to cyber criminals but had not taken action to mitigate this risk quickly enough.
- The response to a breach needs to be considered with more focus on managing reputation and customer perceptions/trust, in addition to the technical and legal elements.
- Retailers should ensure there is a company-wide awareness around cyber threats and cyber risk management, right up to board and CEO level. Responsibility for this issue can no longer lie solely with the IT department or audit committees as there is a limit to what they can do to prevent incidents.
Managing digital risks

Questions to consider

Retailers who wish to effectively manage their digital exposures should begin by asking themselves some basic questions, including:

- Has the company’s key information been identified and are all digital threats to that information being effectively managed?
- Is the allocation of responsibility for digital risks clear and is this included on the risk register?
- Is there a complete and accurate prediction of what the impact would be on the company’s reputation, share price and existence if confidential business information or customer data were to be lost or stolen?
- Is there a complete and accurate prediction of what the impact would be on the business if its online services were disrupted for a short or longer period?
- Does the business have a written cyber security policy in place? Is this championed by the board and supported by management through regular staff training and monitoring?
- Is there a comprehensive incident management plan in place to be followed for each type of cyber incident that affects retailers? Does this plan include access to external expert response teams and does it contain procedures for managing customer messages, with a focus on minimising reputational damage in the wake of an incident?
- Has the cyber security of the company’s suppliers, service providers, business partners and professional advisers been checked?

Our approach

No matter how comprehensive a retailer’s cyber security regime, it is not possible to prevent every cyber incident from occurring. Therefore it is vital that both the retailer and the organisations with which it does business have effective cyber risk management programmes in place.

At Willis Towers Watson we have the capability to support retailers at each stage of their cyber journey:

- Risk identification and evaluation – our IT risk managers will guide you through a risk management process that will identify key risks and evaluate them in line with a trusted risk classification system.
- Risk transfer, contract advice & risk control – expert guidance on placement of bespoke insurance programmes, advice on IT contracts and guidance on effective mitigation and control of uninsurable risks.
- Claims support – specialist advice and support when dealing with cyber losses.

We look forward to speaking to you about how we can help you to manage your cyber exposures.
About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 39,000 employees in more than 120 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

The Willis Towers Watson Retail Practice has worked with customer-facing businesses for over 30 years and as a result we have a deep insight into the opportunities and challenges retailers face. Our team of retail-specialists are based throughout the UK and work with retailers operating within all industry sub-sectors, including large international retailers. As part of a global broking organisation, the retail team is your connection to the wealth of expertise Willis Towers Watson has to offer.

Our industry focus combined with our risk management, claims and insurance placement expertise means we are well placed to assist with both traditional and emerging business exposures.

BLM

BLM is the UK and Ireland’s leading risk and insurance law business, with over 200 partners and 800 lawyers and technical experts totally dedicated to risk and insurance.

Our strong presence in the retail sector reflects our expertise across the whole range of legal issues affecting retailers in the UK. Cases always have to be handled in a way that reflects the retailer's strategy and priorities, including customer care issues.

Everything we do is designed to reduce the time and money our clients spend managing risk, resolving disputes and managing claims. Clients' interests are at the very heart of all processes, delivering value for money at every stage to assist in controlling costs and indemnity spend, sharing knowledge and protecting brand and reputation.

Our specialist retail team is adept at building relationships at all levels to gain a better understanding of a client's organisation, business and brand. Risk management and defensibility training are also integral elements of our service, enabling us to make a real contribution to our clients' operations.
Contact

Please do not hesitate to contact us to discuss your retail risk management and insurance strategy further and find out how we can help you implement the right approach for your business.

Willis Towers Watson

Kelvyn Sampson
UK Industry Practice Leader – Retail and Leisure & Hospitality
T: 44 (0)147 322 2990
E: sampsonkp@willistowerswatson.com
www.willistowerswatson.com

BLM

Nick Gibbons
Partner and Cyber Specialist – London
T: +44 (0)207 457 3567
E: nick.gibbons@blmlaw.com
www.blmlaw.com

* Poneman Institute – 2014 Cost of Data Breach Study: Global Analysis
** Advisen’s 4th Annual Cyber Risk Insights Conference, London, 10/02/2015
*** Verizon 2014 Data Breach Investigations Report, p15
**** Verizon 2014 Data Breach Investigations Report, p15

This publication offers a general overview of its subject matter. It does not necessarily address every aspect of its subject or every product available in the market. It is not intended to be, and should not be, used to replace specific advice relating to individual situations and we do not offer, and this should not be seen as, legal, accounting or tax advice. If you intend to take any action or make any decision on the basis of the content of this publication you should first seek specific advice from an appropriate professional. Some of the information in this publication may be compiled from third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such. The information given in this publication is believed to be accurate at the date of publication shown at the bottom of this document. This information may have subsequently changed or have been superseded, and should not be relied upon to be accurate or suitable after this date. The views expressed are not necessarily those of the Willis Group. Copyright Willis Limited 2017. All rights reserved.