Stackhouse Poland

Cyber security

Why the Manufacturing and Retail sectors must rise to the cyber security challenge

The world has unquestionably changed in the last 10 years and it begs the question "where will we be in 10 years time?" Smart cities, driverless cars, increased drone usage and AI will all have a bearing on how we live our lives and run our businesses. With the advent of smart phones and tablets we are now at a point where most people who access the internet do so remotely through mobile devices and, according to Ofcom, the average adult in the UK spends over 20 hours online per week and nearly nine hours of each day on media and communication.

A more startling statistic is that in 2018 online sales will equate to almost 20% of all retail sales (source: Statista). This change in appetite has resulted in a shift in strategy from almost all businesses as online can no longer be ignored. This has been highlighted by the major retail failures of Maplin and Toy R Us, both of whom experienced significant loss of market share to online competitors.

In fact, many retail businesses are changing strategies so that their high street stores are now considered "showrooms" and developing these outlets to be experiential which, in turn, drives traffic to their websites where clever marketing and algorithms promote additional product sales.

In manufacturing, businesses are increasingly looking to any margin improving efficiency and often this is technology dependant. With an increasing amount of automation and connected devices that enable remote access and control of plant, stock control and ordering systems, what would once have been a factory where the interruption to labour would have been the biggest threat, now the loss of internet connectivity can have the same crippling effect.

Cyber issues in the Manufacturing and Retail Sectors:

48%
of manufacturers have been subject to a cyber attack.[1]

37%
of manufacturers aren't certain they could demonstrate their cyber security credentials to a customer.[1]

53%
of reported fraud in the retail industry is facilitated by cyber.[2]

43%
of retailers had experienced a data breach in the past year, a third of those reported more than one breach.[3]

With this dependency comes risk. So much so that, according to a report by Ernst & Young, 53% of UK businesses increased their spend on cyber security last year and cyber security is now viewed as their number one risk. This is surprising as it is also reported that two thirds of manufacturers in the UK have no insurance cover despite this serious cyber threat. The same report found that nearly half of UK manufacturers have suffered a cyber attack.

In another report titled 'Cyber Security for Manufacturing' - published by AIG and EEF, the Manufacturers' Organisation - manufacturing was revealed as the third most targeted sector in the UK, with only government and finance receiving more cyber attacks. The report showed that in the manufacturing sector:

- 12% had no process measures in place at all to mitigate against the threat of a cyber breach.
- 91% of businesses surveyed say they are investing in digital
- 35% consider that cyber vulnerability is inhibiting them from doing so fully.

It also reported that a quarter of those surveyed had suffered financial loss or disruption as a result of an attack, with firms being urged to reduce their cyber risk.

Attacks both targeted and untargeted are a real threat to businesses - such as that seen last year with WannaCry and NotPetya crippling many UK SME's and indeed global companies - not to mention the NHS. In addition to increased costs and loss of trading, there is the bigger issue of reputational harm and lost confidence.

With attacks becoming more sophisticated and more disruptive the potential threat from cyber crime is widespread. Imagine the impact for a major high street retailer if their online shop was targeted and the payment information and personal data of customers compromised. What would be the impact on future trade by this now crucial channel? How long would it take to repair that reputational damage? Would those customers change brand allegiance and, if so, how long would it take to win them back?

Despite the growing awareness of risk and the money being spent on IT security, the take up of cyber and Crime insurance remains relatively low with an estimated 30% of UK businesses considering purchasing this cover (PWC). Much of this appetite for cyber insurance is in the Financial Service and Professions sector where client data and IP is their bread and butter, and loss of confidence following a cyber attack or data breach is an obvious risk concern.

However, with the management of data and dependency on technology a secondary concern to retail and manufacturing the benefit of a cyber policy in helping a business respond to, and recover from, an attach or data breach could prove to be invaluable.

Find out more

If you would like to learn more about how we can help you with cyber insurance, please get in touch.

Please call us on **0207 089 2900** or email us at **commercial@stackhouse.co.uk.**

www.stackhouse.co.uk

[1]Source: EEF Cyber Report 2018.

[2]Source: 2016 Retail Crime Survey.

[3]Source: Thales Data Security Report, 2017.

Stackhouse Poland Ltd is authorised & regulated by the Financial Conduct Authority in respect of General Insurance business. Our firm's reference number is 309340, which can be checked by visiting the FCA website. SP22/18