21st Century risks – are you prepared?

Recent economic pressures heightens focus on the bottom line, and the retail industry has more challenges than most.

Troy Johnson
Director
Griffiths & Armour
Insurance Brokers

The UK retail landscape – arguably the most competitive in the globe – is evolving rapidly from shops to multichannel to omnichannel – and those retailers who are not reacting are being left behind.

So where does this leave your risk profile? Previously, when physical stores drove your revenues, insurance considerations were a little more straightforward: simply insure the store and supply chain.

In the current environment where customers shop in-store, online, or on their mobile, the focus has shifted from stores to supply chains and distribution centres (DCs). How much thought has been given to realigning your insurance programme (and not simply evolving what you already had in place)?

Terrorism – are you covered?

Terrorism is a key risk where businesses maintain cover on DCs, even though they may be located in the depths of the countryside. Now, this is understandable because of the material impact the loss would have on your bottom line, but when looking at your insurance cover have you considered how it would react should an event occur?

This is a much more complex area than you may at first think. For example, if a package enters your DC containing a biological weapon, say ricin, does the terrorism policy you have spent thousands on protect you?

It is not good enough to assume yes simply because you have terrorism cover. The reality could be starkly different, as most stand-alone terrorism policies specifically exclude biological and this cover has to be bought separately.

The reality of cyber threats

While physical assets are relatively straightforward, cyber risks can also be a challenge to understand in terms of operational and financial impact, as they may not only affect you – they could impact your customers and/or suppliers.

With this in mind, we would challenge you to consider your risk profile and question whether cyber risks are as important or more important than terrorism risks for your key assets. Do you need to insure both? If so, how? If not, do you understand the impact a loss could have?

WHILE PHYSICAL ASSETS ARE RELATIVELY STRAIGHTFORWARD, CYBER RISKS CAN BE CHALLENGING TO UNDERSTAND IN TERMS OF OPERATIONAL AND FINANCIAL IMPACT.

For further information, please contact:
Troy Johnson
07814 455760
tjohnson@griffithsandarmour.com

www.griffithsandarmour.com

Griffiths & Armour

It is clear that cyber sits as a very high priority; most stakeholders recognise the impact an incident could have, even if only from a reputational perspective. That said, innocent mistakes can happen (mis-coding or the loss of data) and equally should a hacker target your business, you will be subject to financial losses. So why do most retailers leave these risks to IT departments to manage?

Devising a cyber strategy

Focusing on plugging gaps in your IT infrastructure is prudent, although it could be argued that it is only the same as ensuring that the doors and windows are locked at your premises and the alarm is switched on.

Your building could still be flooded, burned down or even have a vehicle driven into it, resulting in a major loss. Plugging gaps alone is unlikely to be enough.

Why then are catastrophic cyber losses left uninsured? Historically, the likelihood of such losses was very low, but these risks are increasing dramatically every day.

Impending legislative changes where you could be fined a percentage of your global turnover for any breaches also add pressure. You will be increasingly in the spotlight, both operationally and financially, with stakeholders.

Understanding cyber policies

Cyber policies are generally split into two main categories; first party and third party. First party relates to direct protection for your company. Third party relates to protection for any external parties your technology interfaces with.

IT IS PRUDENT FOR ALL RETAILERS TO AT LEAST REVIEW THEIR RISKS AND CONSIDER PURCHASING CYBER AND TERRORISM POLICIES.

There can be elements of cyber/data protection in Directors and Officers, Computer and Professional Indemnity policies. However, by purchasing a dedicated cyber policy you can be sure of the protection provided and your insurance broker should confirm how this policy fits into your overall risk and insurance programme.

Insurance is a risk transfer mechanism for those risks a business does not want to be exposed to on their balance sheet – a premium is paid for specific protection outlined in the insurance policies.

The scope of cyber policies can therefore be a challenge and you need to push your insurance broker to outline the level of cover and any conditions that could either invalidate or impact the cover being provided. The most common of these is the time franchise that will apply in the policy.

A time franchise is a defined period of time – varying from six to 12 hours – that has to pass before the policy becomes active. Clearly a lot can happen in six hours, so you need to ensure your policy aligns with your operational requirements.

The cost of security

Cyber insurance policies can require a significant investment, appearing expensive when compared to equivalent levels of protection for other policies. But the premiums reflect the risks posed. By providing comprehensive detail on your IT infrastructure, protections and processes enables competitive premiums to be negotiated on your behalf.

Against a backdrop of increasing threats, more complicated IT infrastructure and Cloud usage, the premium for a cyber policy pales when compared to the cost of an uninsured loss and subsequent reputational damage, should a loss occur.

It is prudent for all companies to at least review and consider purchasing cyber and terrorism policies. While you may believe that you have necessary processes in place, or even that such issues are unlikely to affect your business, true peace of mind based in this rapidly changing environment should not be taken for granted.