‘Cyber risk requires careful handling’

By David Legassick,

Head of Life Science, Technology & Cyber, CNA Hardy

This article first appeared in Insurance Day on 12/2019

‘Cyber risk requires careful handling’

By David Legassick,

Head of Life Science,
Tech & Cyber, CNA Hardy.

This article first appeared in Insurance Day on 12 Feb 2019.

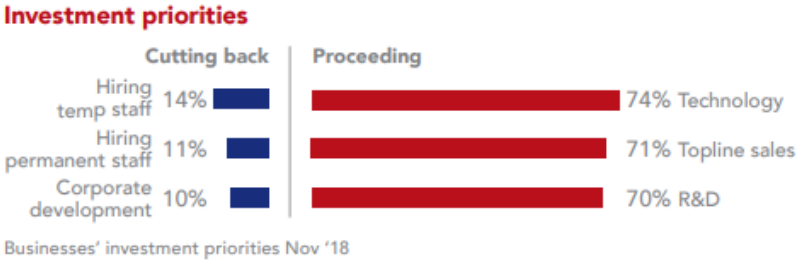
“As cyber insurance becomes a mainstream product, the insurance industry needs to consider how we avoid large losses and ensure that we are cognisant of where claims are likely to come from.”

The growing value of the cyber insurance market demonstrates that dependence on technology is becoming ever more complete. In fact, we are now well into the 4th industrial revolution, where manufacturing as the engine of industrial productivity is tech-driven. The impact of this can be seen in CNA Hardy’s latest Risk and Confidence report, where 49% of businesses predicted that cyber would become their major corporate risk by March 2019.

While no enlightened business executive would argue that this, as with previous industrial revolutions, has not delivered huge rewards; the growing popularity of cyber insurance shows that companies are beginning to recognise that their dependence on technology can be both a strength and a weakness.

‘Cyber risk requires careful handling’

On the plus side, technology does everything businesses could ask for: enabling more efficient operations, improving customer engagement – even delivering step changes in performance. Its impact can be seen in corporate investment, where the pendulum has shifted away from investing in people towards technology:



Businesses’ investment priorities Nov ‘18

In our last Risk & Confidence research - 70% of business leaders said they were prioritising investment in technology, against 24% who were planning on cutting back investment in staff.

However, if complex tech-led systems are disabled by ransomware or hacking, then the activity of a company can be heavily impacted, both financially and operationally; as we saw with attacks last year on the Marriott chain.

Cyber losses are also not just the domain of big businesses and SMEs, in particular, need to consider how they can improve their cyber risk management.

Accepting this as a reality, both businesses and insurers need to adapt their risk management to cope with the new realities of technologically-led, interconnected risk.

‘Cyber risk requires careful handling’

Adapting to the new reality

What is the new reality that cyber risk brings, and what should the insurance industry do differently?

Key to cyber underwriting success is a clear understanding of the risks we are underwriting. To really understand the true scope and scale of cyber risk, will require changes in underwriting practice across the market.

Wordings need to be more clearly understood by brokers and clients. Insurers need to do more to help brokers understand (and communicate) their wordings – like any new and complex class of insurance, an education programme is required.

We also need to understand the risk we are underwriting, but with increasing capacity driving competition and cheaper pricing and broader wordings, some insurers are failing to base their underwriting decisions on the appropriate underwriting information.

Adding on additional coverages without having a strategic overview of the total exposure is a risky game, and one that underwriters play at their own risk.

Aggregated risk

Aggregated risk across cyber clients is another significant risk – and should be considered in a similar way to national catastrophe risk. This sounds exaggerated, but if one critical service provider experiences a cyber outage (for example a major cloud service or broadband provider), it is likely that numerous clients would be hit, creating significant accumulated loss in the market. If the scale of cyber risk is underestimated there is a real risk that carriers could experience some catastrophically unprofitable years, which could impact clients and the London market.

‘Cyber risk requires careful handling’

Better data protection is required

Clients have an important role to play, as many still do not fully understand their cyber exposure or take appropriate steps to protect their business. Even basic security is often overlooked, for example, numerous firms still fail to implement two-factor authentication (requiring two separate pieces of unlinked evidence before log-in is permitted to any corporate system). While companies will employ cameras, gates and security guards to protect their physical assets (effectively 3-step authentication), it seems that they don’t apply that ‘multiple layer’ logic to protecting data.

The human factor is often overlooked

Allied to this is the human factor, sometimes referred to as social engineering. The majority of successful cyber-crime exploit human habits and weaknesses, targeting times such as lunch hours, exploiting access given to unvetted contractors, or using credible stories and fraudulent online identities to change staff behaviour (inducing sharing of passwords or access to bank accounts).

The difficulty of preventing this is graphically illustrated in the film Compliance, which tells the true story of the staff of a McDonalds in America, who were induced to ‘arrest’ and physically restrain one of their staff members by a single phone call from a fraudulent ‘police officer’. In that case the intent was to cause havoc in a non-digital environment, but the fraud could just as easily have been financial. This sort of behavioural manipulation is hard to second guess or stop.

Clients need our help in managing their people risk, both in raising awareness, and in prioritising the protections that they have in place for their non-physical assets. The principle is simple. Invisible doesn’t mean invincible, and assets that can’t be seen, still need protecting.

‘Cyber risk requires careful handling’

Augmentation

Finally, we need to use technology better as part of our cyber fightback. While technology can augment risk, it also brings the power to augment our own skills, and developments such as AI can help hold back cyber-crime, especially the huge state-sponsored attacks. It is predicted that 2019 will see big growth in AI-on-AI cyber battles, as we seek to harness technology to protect digital assets, and this is positive all round.

The cyber market offers huge potential, but there is a lot we need to do to support the maturing cyber insurance market.

Underwriters need to be mindful not to jump on the bandwagon and underwrite cyber risk carelessly, without a clear understanding of the potential size of losses. We also need to help clients to understand their policies and, what they can do to improve their own cyber risk protection, and this requires ongoing education.

Finally, employ technology of our own to fight cyber-crime, working with third parties to thwart the cyber criminals making it hard for them to access vital data and disrupt systems.

With careful management cyber insurance has the potential to become one of the most successful products, which offers great benefits to many businesses around the globe. If we abuse the potential and underwrite for short-term growth instead of creating a mature and successful market, it could end up in significant losses and disillusioned clients.

By David Legassick,
Head of Life Science, Tech & Cyber.
E: david.legassick@cnahardy.com

To download our latest Risk & Confidence Survey, visit cnahardy.com/pulse

‘Cyber risk requires careful handling’