Mactavish

CYBER RISK & INSURANCE REPORT

NOVEMBER 2018

INTRODUCTION

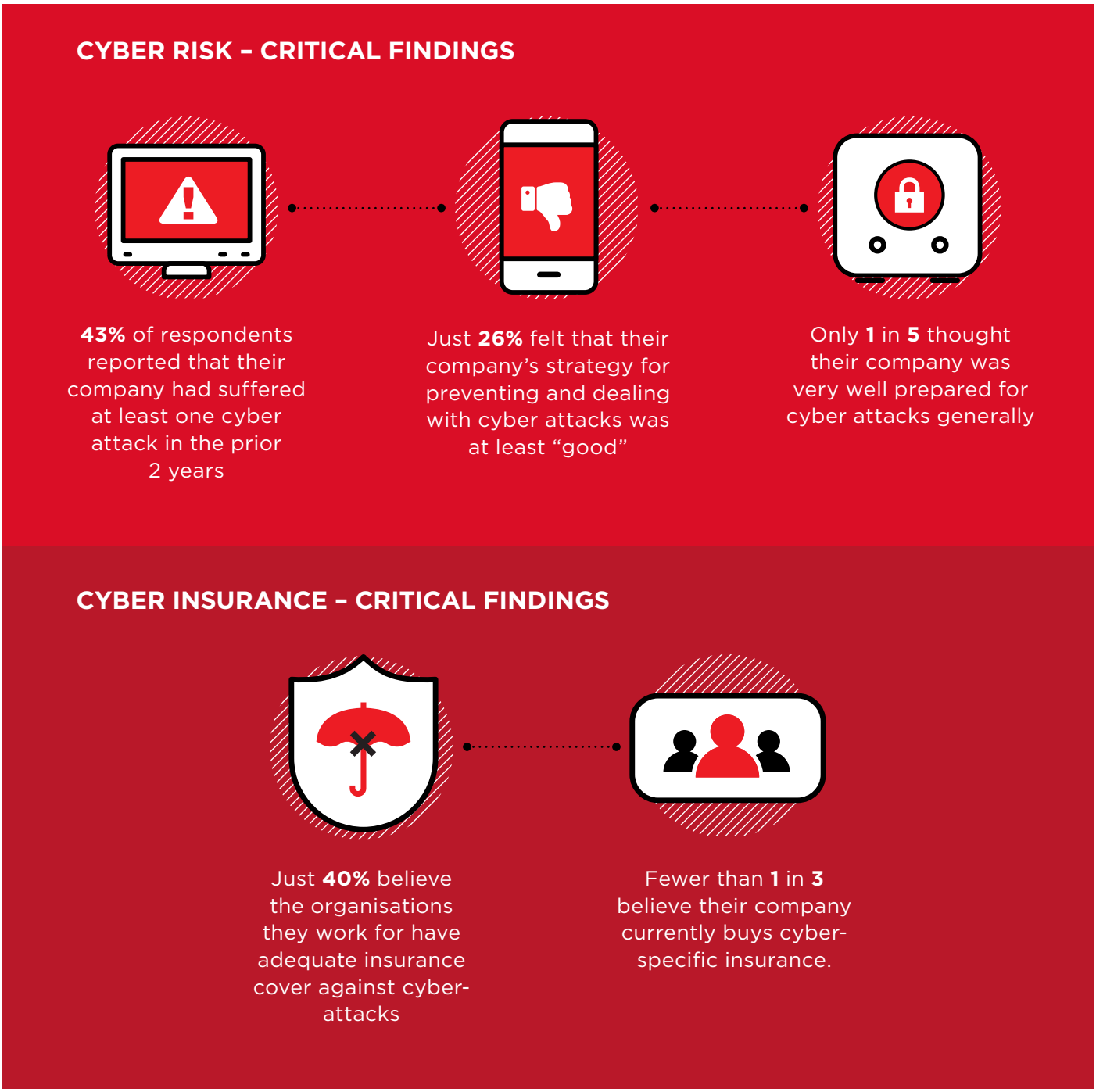
Cyber risks are rapidly escalating across the economy, with new attacks on UK companies hitting the headlines with alarming regularity throughout 2018 - but these stories are only the tip of the cyber risk iceberg. Research shows that senior managers across all sectors view ever more sophisticated attacks as increasingly commonplace, but often feel that their organisations remain under-prepared.

In this context it is not surprising that cyber insurance has been about the hottest topic in insurance for the last few years. But despite this attention, most companies still do not buy cyber insurance while many are uncertain over what it covers and do not trust it to pay out. This caution is justified as cyber insurance is a new and untested product – with many reviewed standard cyber insurance policies failing to meet the client needs for which they were sold. Most 'off the shelf' cyber policies suffer from a range of limitations and will not automatically protect against all cyber risks.

RESEARCH HIGHLIGHTS

Mactavish's October 2018 survey of around 700 UK senior managers confirms a growing level of cyber risk concern as shown below:

FIGURE 1 – *UK Senior Managers attitudes to cyber risk and insurance*



RESEARCH HIGHLIGHTS

FIGURE 2 – *Why do companies not buy cyber insurance? (% of respondents)*

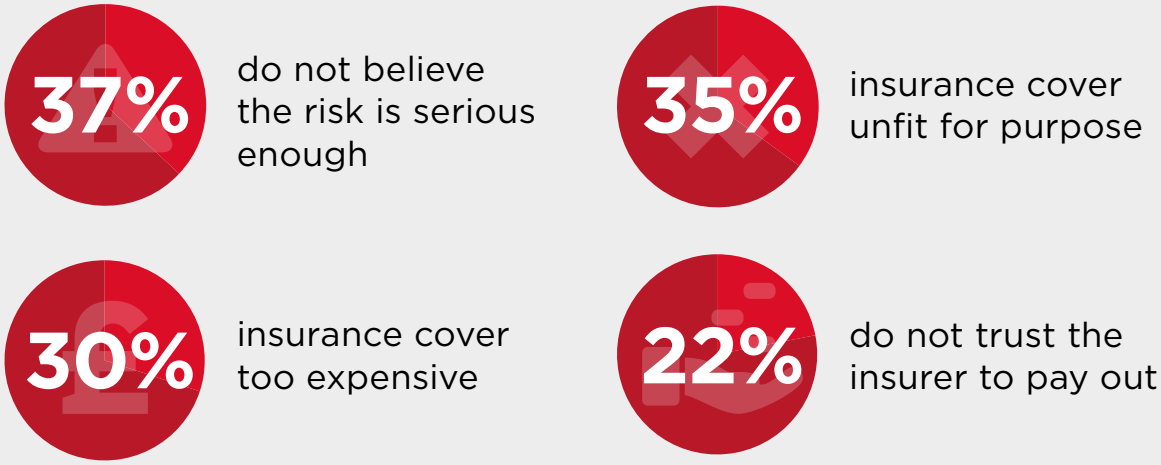
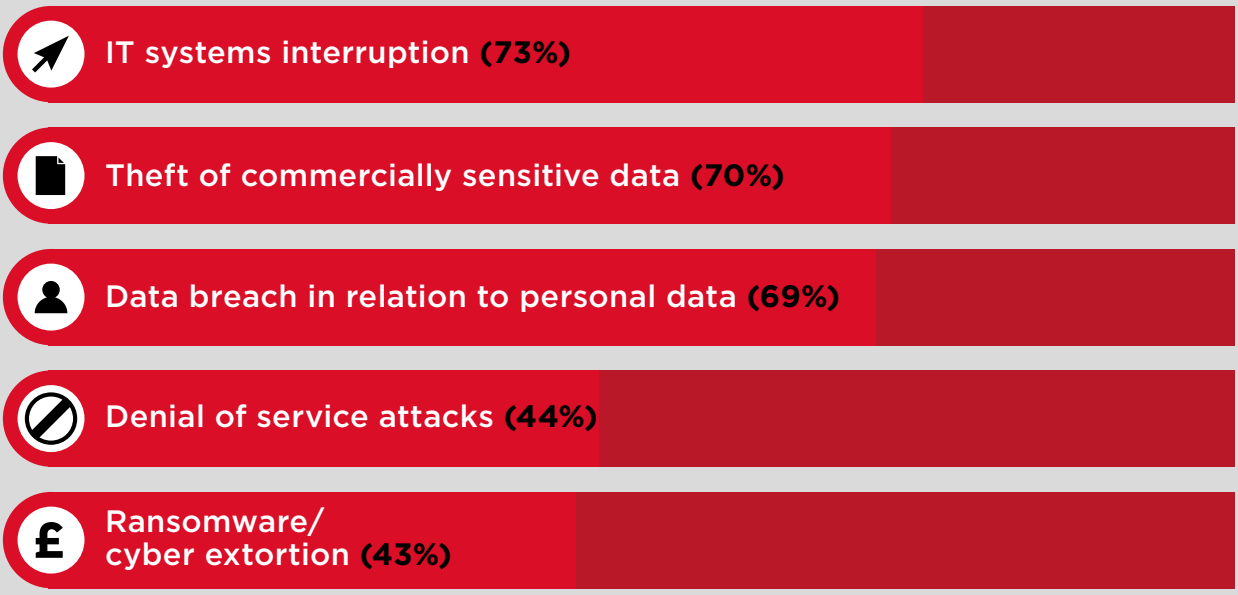


FIGURE 3 – *What are the most common cyber-risk concerns? (% of respondents)*



COMMON CYBER INSURANCE LIMITATIONS

Based on Mactavish analysis of market-leading standard cyber insurance wordings, there are at least 8 common flaws, meaning buyers need to negotiate bespoke cover:

1. Cover can be limited to events triggered by attacks or unauthorised activity – excluding cover for issues caused by accidental errors or omissions
2. Data breach costs can be limited – e.g. covering only costs that the business is strictly legally required to incur (as opposed to much greater costs which would be incurred in practice)
3. Systems interruption cover can be limited to only the brief period of actual network interruption, providing no cover for the more significant knock-on revenue impact in the period after IT systems are restored but the business is still disrupted
4. Cover for systems delivered by outsourced service providers (many businesses' most significant exposure) varies significantly and is often limited or excluded
5. Exclusions for software in development or systems being rolled out are common and can be unclear or in the worst cases exclude events relating to any recently updated systems
6. Where contractors cause issues (e.g. a data breach) but the business is legally responsible, policies will sometimes not respond
7. Notification requirements are often complex and onerous
8. During a cyber incident, businesses often have no freedom to choose their IT, PR or legal specialists, as the policy only covers insurer appointed advisors.

WHY DOES STANDARD CYBER COVER REQUIRE TAILORING?

Like many forms of business insurance, cyber losses and cyber policy wordings can be highly complex. Across the industry, insurers' approach to large claims has changed in recent years in ways which create significant challenges for policyholders.

The combination of aggressive cost cutting across the industry, increased focus on off-the-shelf solutions, and demanding new legislation creates specific challenges that the insurance industry does not have the technical capabilities to consistently overcome.

The net outcome of this is that insurance products do not reliably protect businesses. There is a high level of disputed, discounted and delayed claims settlements. For example, our seminal research showed that, across all strategically significant claims, on average: **45%** are disputed; average dispute resolution time is almost **3 years**; and disputed settlements are **60%** of the amount originally claimed. These issues affect businesses of all sizes and sectors.

MACTAVISH CYBER RISK CONSULTING PRACTICE

Mactavish has analysed and negotiated bespoke cyber cover for many FTSE 250, FTSE 100 and private companies in recent years.

Building on this knowledge, in 2018 we have launched a new Cyber Risk Consulting Practice to help companies accurately identify their cyber risks, develop business-specific loss scenarios and negotiate bespoke insurance cover – whether as part of the existing programme or via a cyber-specific policy.

> *"There are a number of new cyber insurance policies being launched, but despite a sharp increase in cyber incidents this market is very immature and in many respects untested. Perhaps some of these policies have been rushed to market by insurers eager to capitalise on the growing cyber risks facing organisations, and their desire to spend significant amounts of money to protect themselves against this. Very few claims have been made on these new cyber insurance policies, but my bet is that many will be disputed, or settlements will be much lower than clients expected. However, this can be avoided if organisations first understand the cyber risks they face, and then secure a bespoke policy to meet their needs."*

BRUCE HEPBURN, MACTAVISH CEO

CASE STUDY: RETAIL CLIENT

A retail client had recently suffered a cyber attack for which their insurance did not respond, prompting them to engage Mactavish to review and renegotiate their cyber insurance policy.

This exercise began with a programme of in-depth risk interviews to profile the key cyber risks faced by the organisation and the likely impacts of and business response to such attacks.

This analysis was then used to identify the shortcomings of the current insurance policy and a revised wording was drafted by Mactavish and negotiated with insurers. The net outcome was to drastically enhance the likelihood that the policy will respond as expected when tested by future loss event. Some key example enhancements included:

1. Extending cover far more widely across the company's critical 3rd party IT providers
2. Expanding cover to cater for defined accidental as well as malicious loss scenarios
3. Extending the type of costs which the company could incur whilst managing a cyber loss, and the duration over which such costs could be incurred
4. Amending key policy T&Cs to provide additional flexibility and remove draconian insurer rights in the event of a minor breach of policy requirements by the insured.

ABOUT MACTAVISH

Mactavish is the UK's leading expert on insurance governance and has been operating in the commercial insurance sector for over 15 years. Its focus has always been on detailed, technical analysis which does not shy away from uncovering and studying uncomfortable truths or challenging accepted wisdom.

The company is relentless in its focus on driving increased standards across the commercial insurance industry which can cope with increasing risk complexity and work fairly and reliability for all parties. This has given the business an unrivalled depth of expertise on the insurance placement process and a wide spread of clients.

Mactavish has also been closely involved with the project to reform commercial insurance law in the UK, an eight-year programme which culminated in the Insurance Act 2015.

Mactavish is licensed by the Bar Standards Board of the Bar Council to access barristers directly, for both contentious and pre-contractual legal work in the field of insurance. We believe the business is unique in the UK in this regard.

Mactavish

Mactavish Office Address: 5 Chancery Lane, London, EC4A 1BL, United Kingdom

Telephone: +44 (0) 207 046 7974 • **Email:** mail@mactavishgroup.com • **Website:** www.mactavishgroup.com

Twitter: @MactavishGroup • **LinkedIn:** Mactavish