S-RM

# CYBER SECURITY INSIGHTS REPORT

2022

# Contents

# Introduction

In the **S-RM Cyber Security Insights Report 2022** we seek to understand the specific cyber security challenges faced by C-suite leaders and senior IT decision makers. It follows on from our 2021 report, enabling us to draw out valuable trends from the past 12 months in global corporate cyber security.

We again surveyed 600 C-suite and IT budget holders from organisations with a revenue over USD 500m[1]. We analysed the year-on-year changes in the incidents experienced by large organisations and their approaches to spending on cyber security. This year, we also asked survey participants about cyber insurance. In the context of a well-publicised hard market, is cyber insurance still worth the cost?

The report discusses the cyber challenges large organisations have faced in 2022 – from pressed budgets to rising insurance premiums – and provides analysis and advice. Together we hope the findings will support business leaders as they plan their approach to cyber security in the year ahead.

[1] Survey commissioned by S-RM and conducted by market research firm Vanson Bourne in July 2022

# At a glance

## Serious cyber incidents are rising

The number of survey respondents who reported experiencing a serious cyber incident within the past three years rose by 15% in 2022. This suggests that organisations still have work to do to ensure their cyber security programmes are equipped for the modern threat landscape.

## Budgets have increased, but not enough

Cyber budgets were up 5.2% year-on-year. But this is unlikely to be sufficient to keep pace with increasing incident frequency and the prospects of future budget increases are gloomy. Without further commitment to cyber spend, it's unlikely that security teams will be able to keep pace with their adversaries.

## Insurance is critical, but the market is challenging

Cyber insurance remains a key pillar for organisations in their cyber security strategy. 97% of those surveyed currently hold a cyber insurance policy. But this form of risk transfer is increasingly challenging for companies – premiums had increased by an average of 42.1% since the last renewal. When premiums and deductibles rise, and exclusions increase, it means greater risk resides, uninsured, within the business. Preparing more thoroughly for insurance applications – and considering supplementary protection, such as incident response retainers – is recommended.

**15%**
INCREASE IN CYBER INCIDENTS

**5.2%**
Y-O-Y BUDGET INCREASE

**42.1%**
INCREASE IN INSURANCE PREMIUMS

# 01

# Steep rise in serious cyber incidents

Serious cyber incidents are on the rise and show no signs of stopping. Last year, S-RM surveyed 600 C-suite and IT budget holders from organisations with revenue over USD 500m. 60% of them told us they had experienced a serious cyber incident in the previous three years. This year, when we asked the same question, that number had increased to 75%.

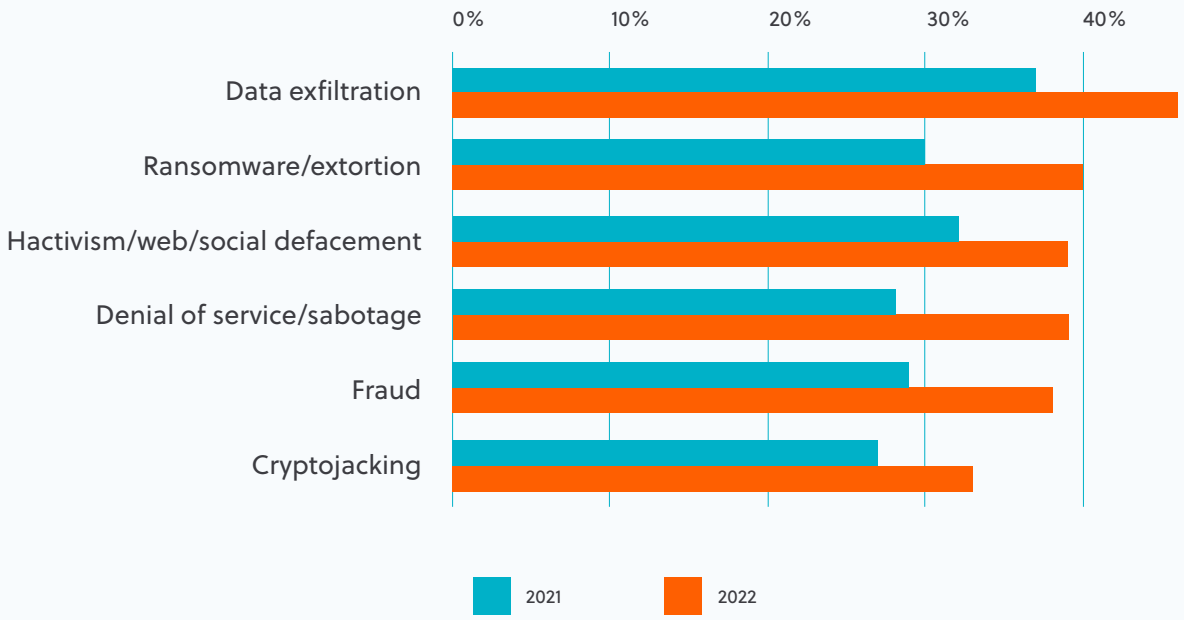
## Types of incidents

Ransomware and denial-of-service attacks increased the most year-on-year, at 10% and 11% respectively, but instances of data theft, hacktivism and fraud were all up (figure 1).

These increases are significant. As companies have spent more money on their cyber security, it might have followed that they began to experience fewer serious incidents. A better understanding of their threat profile, a well-trained workforce and more sophisticated tooling all improve a company's ability to defend against cyber threats. But the increase in incident frequency suggests that a significant number of companies have either not invested their money in the right places or have not implemented their changes properly.

There are various reasons that explain the rise in incidents. Worsening diplomatic relations between the West and countries known to sponsor malicious cyber activity, the democratisation of cyber hacking tools and services, and the enduring financial gains to be made from data theft and ransomware are all likely to be significant contributors. However, while the cyber intelligence community is constantly improving its understanding of threat groups and their capabilities, there is a level of opacity that is hard to overcome entirely.

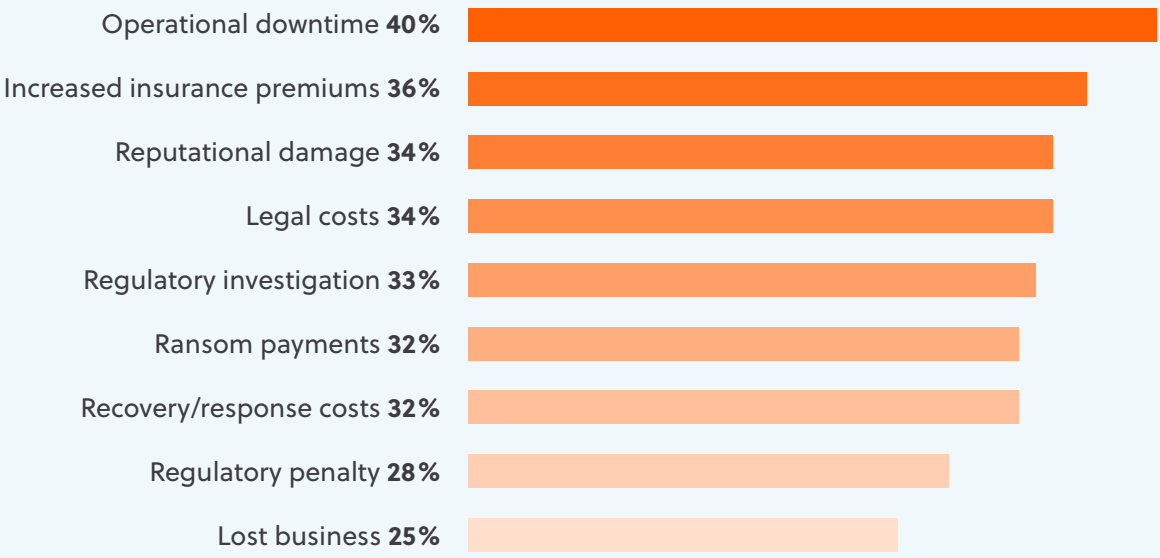
**FIGURE 1** TYPES OF CYBER INCIDENT EXPERIENCED IN PAST THREE YEARS



## Impacts are still significant

The impact of this increase in incidents is clear. This year, our respondents reported an average direct loss from a serious cyber incident of USD 1.5 million. This figure has decreased by roughly USD 300,000 from last year. When considered alongside the increase in incident frequency, this may suggest that organisations are managing the costs of cyber incidents better. However, USD 1.5 million remains significant, and this figure doesn't take into account an incident's long-term fallout. Over 30% of respondents told us their business had suffered reputational damage as the result of a cyber incident, while a quarter reported losing business altogether, meaning companies are feeling the effects of serious cyber incidents long after the hefty initial bill has been paid (figure 2).

**FIGURE 2** IMPACT OF CYBER INCIDENTS



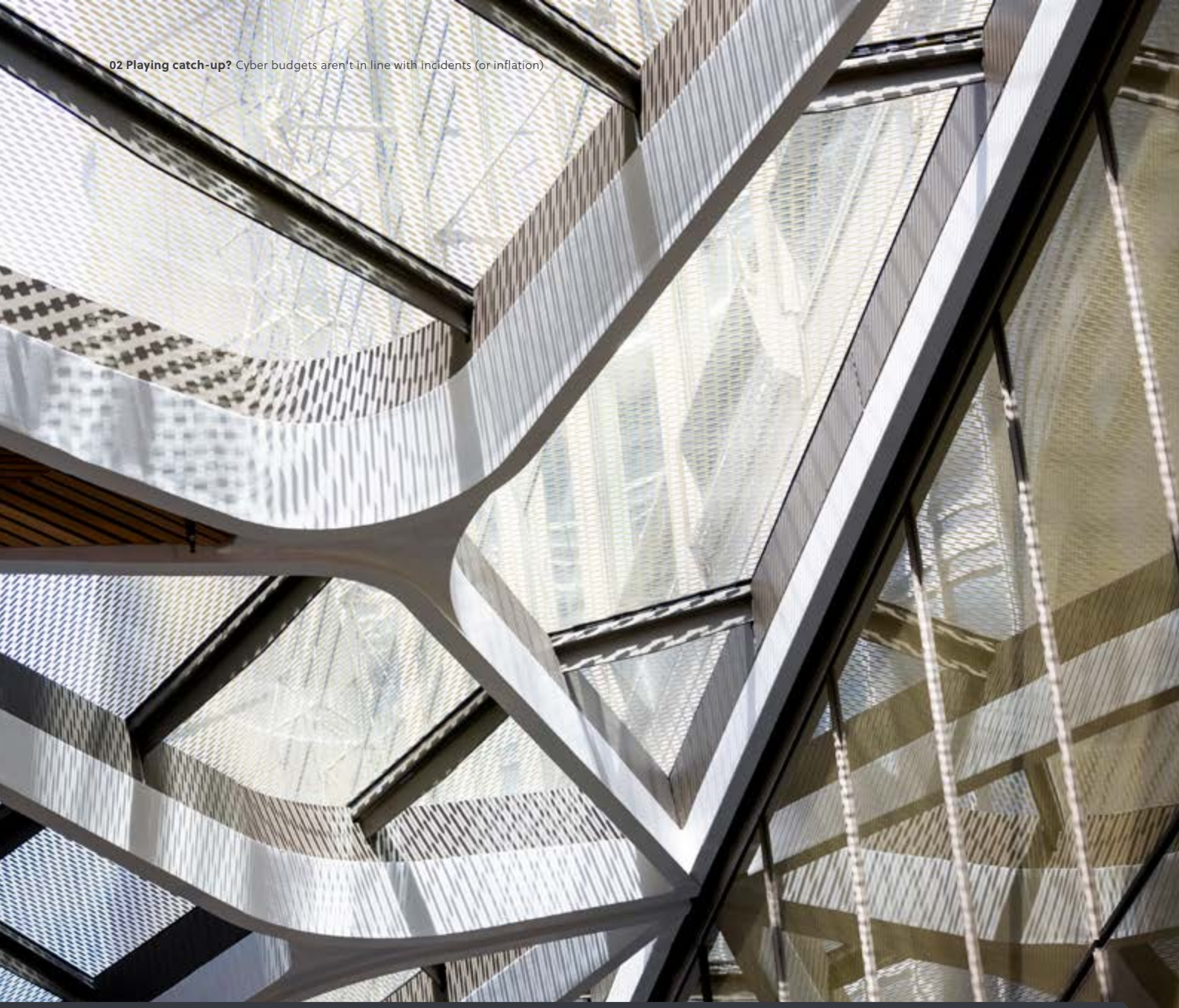
## The evolving threat landscape

CASE STUDY

# EvilProxy

In recent months, our team has observed an increase in business email compromise (BEC) attacks. Threat actors have been using an easy-to-use phishing tool known as EvilProxy to steal credentials and commit payment fraud. Critically, EvilProxy allows threat actors to bypass multi-factor authentication (MFA), one of the key methods used by security teams to prevent unauthorised access to corporate email accounts and other applications.

EvilProxy is an excellent example of how quickly the threat landscape can change. Security teams that dismissed the threat of BECs to focus on ransomware or put their faith in MFA as a fix-all solution have been caught out. As companies scramble to fine-tune their MFA solutions and alert their employees to the new threat, it is a reminder that adopting a more holistic approach to security is more likely to be effective in the long-term and that there is no room for complacency.



# 02

# Playing catch-up?
## Cyber budgets are not in line with incidents (or inflation)

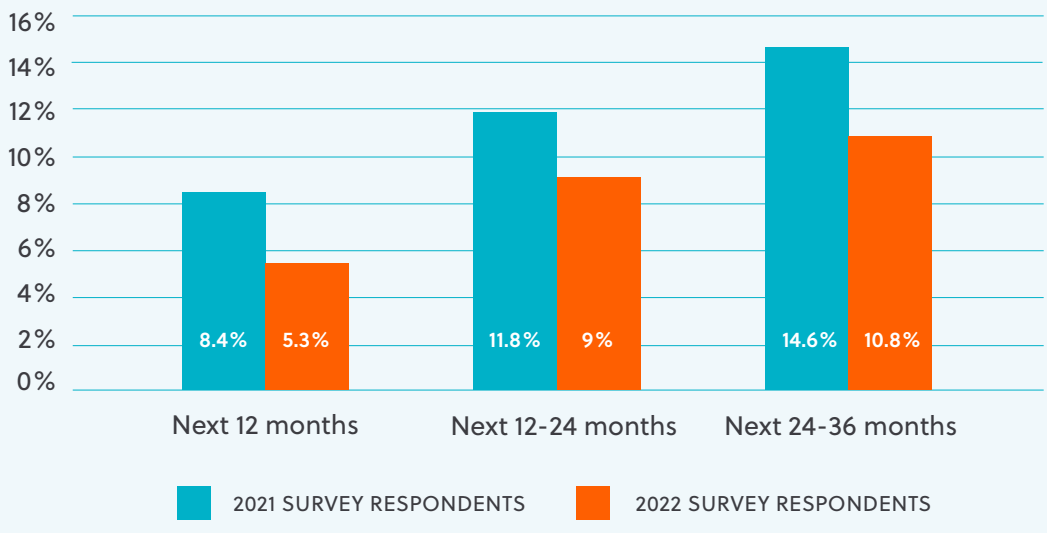
C-suite and IT leaders are struggling to find the security solutions to protect their organisations from cyber-attacks. But despite this, our data indicates that there is still a reluctance or inability to spend.

Cyber budgets increased by 5.2% in 2022, falling well short of the 15% increase in serious incident frequency. The two figures are not directly comparable – there is no guarantee that increasing a security budget will reduce the frequency of serious incidents. However, it is an excellent place to start. The relatively modest 5.2% increase suggests that even when organisations know cyber-attacks against them are rising, finding the money to protect against them is difficult.

## Organisations that are unable to keep pace with the security environment are likely to find themselves vulnerable to new, more sophisticated forms of attack.

Looking forward, the picture remains gloomy. Respondents to our 2021 survey anticipated an overall increase in cyber security budgets of 14.6% over the next three years. The past year has tempered their expectations. This year, that figure had dropped to 10.8% (figure 3), suggesting budgets are being squeezed further, barely keeping pace with inflation. In a tough macroeconomic climate it's unlikely to be just cyber security budgets that are under pressure. However, companies may regret cutting corners. Organisations that are unable to keep pace with the security environment are likely to find themselves vulnerable to new, more sophisticated forms of attack.

**FIGURE 3** ESTIMATED % CYBER BUDGET INCREASES



## Making the case for your cyber budget

With budgets under pressure, securing funds and spending them wisely is critical. We asked our respondents what the key drivers for increasing budget were to understand how to put together a compelling business case for an uplift. The need to keep pace with the evolving threat landscape was the most commonly cited, though other important factors included changing regulations and adapting to hybrid working conditions (figure 4).

The variety of responses reinforces the need for holistic thinking and the lack of 'silver bullet' solutions. Each organisation has its own cyber security challenges, and it's unlikely that restricting spend to one area will be sufficient to address them.

**FIGURE 4** DRIVERS BEHIND INCREASES IN CYBER BUDGET

## Finding the most value

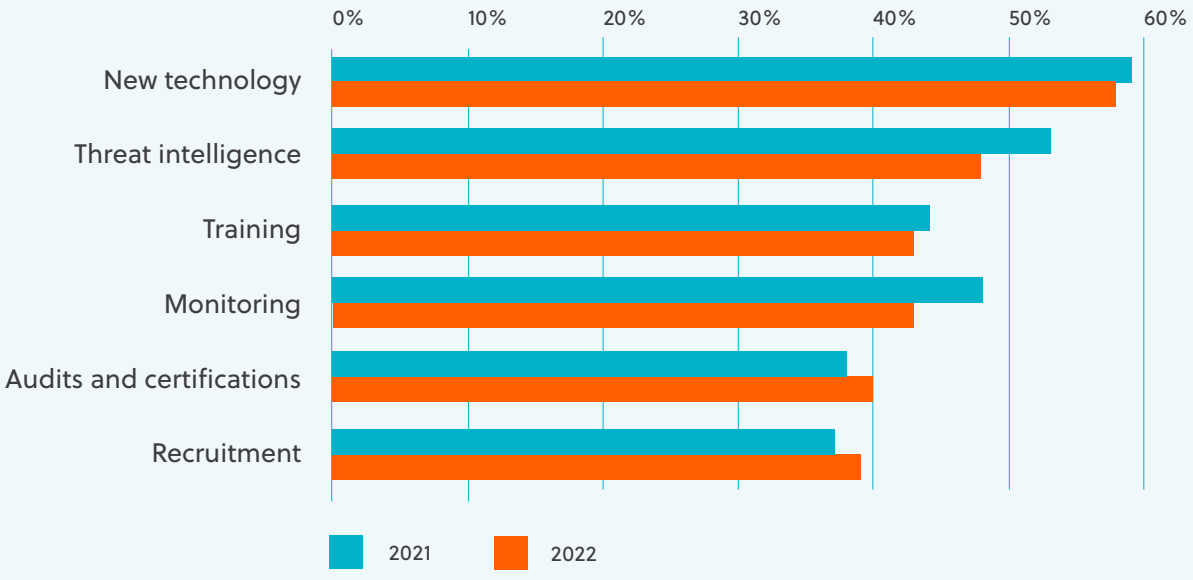
We asked respondents which areas they considered to be the best value for money when it came to investing in cyber security. New technology again came out on top, with 58% of respondents reporting that investment in this area provided 'high value for money' (figure 5).

As cyber threats evolve, it's clear that technology needs to keep pace. But enthusiasm for shiny new solutions should be matched with attention to their implementation. Technology is only effective if it is used correctly and forms part of a broader security plan.

Investment in new technology in isolation is unlikely to deliver value. For example, most large organisations now have a multi-factor authentication (MFA) solution to prevent unauthorised access to their environment. To be effective, however, the solution and its enforcement need to be managed correctly, which may require new staff or training. Similarly, endpoint, detection and response (EDR) tools drastically improve an organisation's ability to respond to a cyber-attack, but this doesn't render preventative security measures obsolete.

As cyber threats evolve, it's clear that technology needs to keep pace. But enthusiasm for shiny new solutions should be matched with attention to their implementation.

**FIGURE 5** PERCENTAGE OF RESPONDENTS REPORTING 'HIGH VALUE FOR MONEY' PER INVESTMENT AREA



PRACTICAL STEPS

# Minimising the impact of an incident

Organisations can maximise the value of their security investment by accepting that cyber incidents are inevitable and focussing on minimising their impact. Across thousands of incidents, we have first-hand experience of companies that do this well and those that don't. There are three common mistakes organisations make when responding to a cyber incident that drive the cost up significantly:

## Breakdown in communication between C-suite and IT teams

It's no secret that executive leaders and IT teams don't always see eye-to-eye when it comes to cyber security. Our survey illustrates this – we often see different responses to the same questions depending on who we ask. But a breakdown in this relationship when responding to an incident can be catastrophic. Investing in a thorough and well-rehearsed incident response plan that defines the role each stakeholder will play and the organisation's objectives goes some way to ensuring this relationship remains intact.

## Damage from attempts to contain incidents

In the heat of the moment, there is a temptation to act quickly to try to resolve an incident before it develops into something more serious. But there are times when rushing to contain an incident can do more harm than good. This might be an IT team member seeing live encryption of data and hastily unplugging a machine, or wiping business critical data before considering whether it was backed up. Training technical staff on the basics of incident containment could prevent bad decisions in the moment and significant damage further down the line.

## Poor selection or mismanagement of third parties

Even the most prepared organisation will likely need support from third parties when an incidents hits, be that external legal counsel, public relations advisors or forensic specialists. Onboarding specialists you trust ahead of time is a reliable way to ensure that companies can put their response plan into action quickly and efficiently. Our data shows that introducing unvetted third parties after the fact brings an unpredictability to the response that can send costs spiralling.

# 03

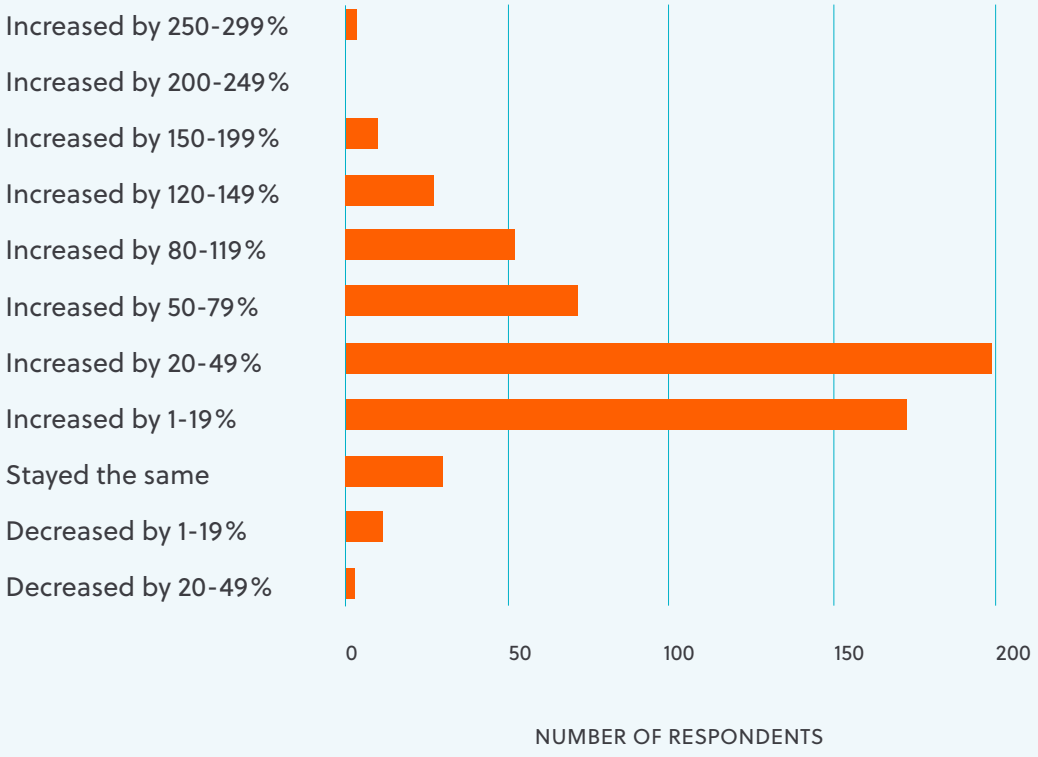
# Is insurance the answer?

With security budgets squeezed, we wanted to know whether companies were still reliant on insurance to transfer some of their cyber risk. The answer was a resounding 'yes'.

For senior IT leaders and C-suite professionals, insurance remains a key pillar of their cyber security strategy. Nearly all the respondents to our 2022 survey (97%) had held cyber insurance for at least two years, and for those who made a claim owing to a serious incident, 99% had their costs either partially or fully covered by their insurers. Organisations that held policies for longer (upwards of two years) were more likely to receive a full coverage pay-out.

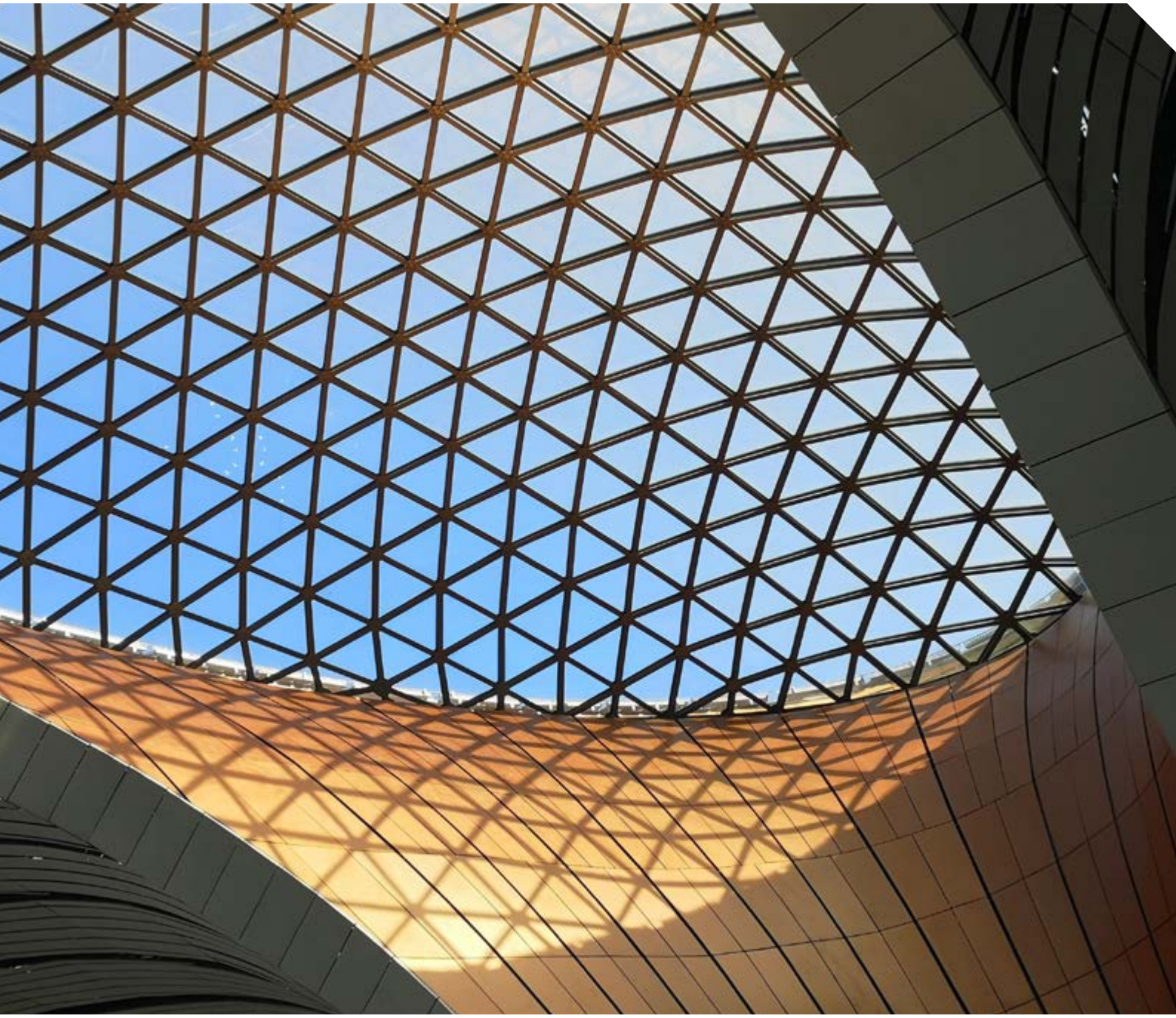
But while insurance still plays a vital role, obtaining or renewing cyber cover is increasingly challenging. There has been a hard cyber insurance market since 2020, when the loss ratio for insurers, a measure of the amount of money spent to fulfil claims against the total revenue brought in through premiums, peaked at 73%[2]. Insurers are now more cautious about who they offer coverage to, and before they do, they want better proof that organisations are taking their cyber security seriously. Those that manage to navigate this process successfully are faced with another challenge: rising premiums. 92% of organisations reported an increase in their premium since their last renewal. And as figure 6 illustrates, these increases are substantial: the average was 42.1%, with many companies seeing rises of over 100%.

**FIGURE 6** CHANGES IN INSURANCE PREMIUM SINCE LAST RENEWAL




[2] https://www.fitchratings.com/research/insurance/sharply-rising-cyber-insurance-claims-signal-further-risk-challenges-15-04-2021

Faced with higher premiums and deductibles and more exclusions in the policy, companies are looking for alternative ways to transfer their risk. 94% of respondents had an incident response firm on retainer, meaning the overwhelming majority of companies we surveyed had elected to get cyber insurance and have a response firm on retainer in parallel. Only 56% of respondents had held an incident response retainer for more than two years, suggesting that their popularity may be a direct result of the challenging insurance market. High deductibles mean that even companies with insurance could be on the hook for expensive incident costs, so there is clear motivation to keep these costs down. Retaining an expert firm that knows your network and is ready to deploy immediately is one way to do this.



PRACTICAL STEPS

# Cyber insurance business response

The difficulty for insurers is cyber security claims are multi-faceted. Business interruption costs, ransom payments, fees for technical specialists and lawyers – all of these might form part of the same claim, with costs spiralling as a result. In response, underwriters have improved their own understanding of cyber incidents and begun to ask more searching questions of insureds. Increasingly, they are seeking proof that potential insureds have implemented security controls that will directly limit the impact of a ransomware incident. When advising organisations on navigation of the insurance application process, S-RM recommends they focus on four key areas.

## 1. Back-up strategy

Top among the controls that insurers look for is a robust back-up strategy. This means having copies of critical infrastructure and data that will enable organisations to recover from a ransomware attack and continue to operate. A good back-up strategy should be coupled with a comprehensive disaster recovery plan that ensures recovery actions are practiced and will work as intended.

## 2. Operational protection

Historically, organisations neglected more operational elements of their network when considering cyber security measures. This was especially pertinent for manufacturers or utility providers, who may have a highly secure corporate network but vulnerabilities in their operational technology. Underwriters now scrutinise these environments more closely, especially when it comes to business critical or high revenue generating operational technology.

## 3. Standard controls

Controls that organisations were once advised to have in place, such as multi-factor authentication (MFA) for all forms of remote access, 24x7 security monitoring, secure management of privileged accounts and a robust vulnerability management programme, are now considered to be 'must-haves'. Organisations must ensure that these areas are considered and mature in order to secure a policy.

## 4. Communication

Insureds or prospective insureds play an important role in the underwriting process. As an applicant, the key is ensuring you have the opportunity to articulate the story of your security posture to the insurer. Whether that's providing detailed information to brokers at the proposal stage, or speaking to underwriters directly, going beyond the standard form-filling exercises increases the likelihood of a positive outcome.

## S-RM is a global intelligence and cyber security consultancy with expertise in insurance, cyber security, and cyber response.

Headquartered in London, S-RM works across seven international offices and advises companies ranging from blue-chip corporates, to large financial institutions, and beyond.

## CONTACT US

To discuss how we can help support any aspect of your cyber security, please reach out to

**JAMIE SMITH**, Board Director and Head of Cyber Security, j.smith@s-rminform.com

**PAUL CARON**, Head of Cyber Security, Americas, p.caron@s-rminform.com

Alternatively contact the **S-RM TEAM** at hello@s-rminform.com

---