CyberSmart

CYBER INSURANCE TRENDS 2023

What does the future hold for a growing industry?

cybersmart.co.uk

Contents

INTRODUCTION

Cyber insurance has never been more important

Contrary to popular belief, cyberattacks aren't only an issue for multinationals and Fortune 500 companies. Many SMEs fall into the trap of thinking their data isn't worth anything to a hacker or that they're too small to attract unwanted attention. This simply isn't true.

39% of UK SMEs reported a cyberattack in 2022, and research suggests this figure is on the rise. While most businesses have security measures and policies in place to ward off attacks, surprisingly few have a standalone **cyber insurance** policy.

What's holding them back? Let's explore the cyber insurance trends that will shape 2023.

What is cyber insurance?

Cyber insurance is a speciality insurance product that protects businesses from cyber risks, and those related to IT infrastructure and data management. It covers risks that aren't defined in or covered by standard commercial liability policies.

OBSTACLES TO ADOPTION

What stops SMEs from getting dedicated cyber insurance?

Their commercial liability policy covers (some) cyber risks

Many commercial liability policies provide some level of coverage for the most common cyber risks up to a certain value. For 43% of people in a recent Deloitte survey, this was the main reason they didn't have a standalone policy. But the level of coverage in standard liability policies isn't suitable for today's volatile cybersecurity landscape.

It's not until an SME hears about a particularly nasty cyberattack or experiences one themselves that they realise the need for more comprehensive protection. The kind that only a standalone cyber insurance policy can provide.

From accidental privacy breaches to hacking and ransomware, dedicated cyber insurance covers your business against a wide range of risks. Depending on the type of policy you have, cyber insurance can cover the costs associated with lost income due to business disruption, data recovery and restoration, post-breach investigations, and more.

In addition, a standalone policy gives you access to cybersecurity experts who can provide support and guidance on:

- Cybersecurity best practices
- Digital hygiene
- Incident response
- Business continuity & disaster recovery
- Training

Premiums are prohibitively high

For many SMEs, standalone cyber insurance premiums are unaffordable. Cyber insurance costs increased by 130% in Q4 2021 alone, driven primarily by the rise in frequency and severity of cyberattacks. And many SMEs feel the costs outweigh the risks.

Then there's inflation and the cost of living crisis. Rising energy prices are increasing overheads and, with people struggling to make ends meet, small businesses face an uphill battle attracting and retaining staff. Customers are also spending less, which is negatively impacting cashflow.

The upshot is that businesses are looking for opportunities to save money, and standalone cyber insurance policies are among the first things to go. According to Deloitte, 29% of people who cancelled their cyber insurance policy in 2021 cited the need to cut costs.

> **Even if UK SMBs do become more concerned about their business being targeted by cybercriminals, they are unlikely to be willing to pay even higher premiums to protect themselves.**
>
> BEN CAREY-EVANS,
> SENIOR INSURANCE ANALYST AT GLOBALDATA

Parallel to the high premiums is a perceived lack of value among customers. In a 2020 Deloitte survey, 34% of respondents said their policy's coverage limit was too low and 29% said the coverage terms and exclusions were too restrictive.

Qualifying requirements are too stringent

The UK cyber insurance market is still relatively young. There's limited data and standardisation across the industry, which makes it difficult for insurers to accurately assess risk. The result is higher insurance premiums and tighter qualifying requirements.

Typically, insurers require you to have a basic level of security before they'll agree to cover you. These requirements often differ from provider to provider. Some rely on the five controls of Cyber Essentials to set a minimum security standard and mitigate the risk from cyber threats, specifically:

- Firewalls
- Secure configuration
- User access control
- Malware protection
- Security update management

Be aware...

Bolstering your security beyond these minimum requirements **won't reduce your insurance premiums**, but it may protect you from more advanced threats.

Insurers typically perform comprehensive risk assessments as part of the underwriting process. The extent of this assessment depends on the size of your business. It can range from a simple questionnaire to a forensic analysis of your security that takes weeks to complete. Growing threats, like ransomware, have forced insurers to reconsider how they assess risks. Smaller businesses may struggle to meet the qualifying requirements.

The 4 biggest benefits of standalone cyber insurance

1. Enhanced cybersecurity

2. Access to expert advice & guidance

3. Business continuity & disaster recovery support

4. Peace of mind

MARKET OVERVIEW

The state of the cyber insurance market

The global cyber insurance market has enjoyed steady growth in recent years.

In 2022, the cyber insurance market was valued at $12.83bn – an increase of more than $2bn from 2021. Analysts predict this growth will continue at a CAGR of 19.52% to reach a market value of $38.7bn by 2030.

North America continues to dominate, with a market share of 89%. Analysts credit this pre-eminence to mandatory cybersecurity legislation in several US states, which has led to higher market penetration. By contrast, Europe's market share is between 5%-9%. The figure is even lower in Asia-Pacific, but analysts expect to see significant growth in this region over the coming years due to the rise in ransomware attacks.

Despite the positive outlook, sales of standalone cyber insurance remains low. For example, annual cyber insurance premiums only generate $2bn, with 42% coming from the limited coverage provided in standard policies.

Additional market stats

- 60% of finance and insurance firms have some level of cyber insurance
- 23% of finance and insurance firms have standalone cyber insurance
- High-income charities are more likely to have some form of cyber cover than others
- Only 1% of businesses and 2% of charities with a cyber insurance policy made a claim in 2021

Source

TRENDS

5 cyber insurance trends to watch in 2023

#1 Insurance premiums continue to rise

82% of cyber insurers expect premiums to increase over the next two years, driven by the market's exceptionally high loss ratio and evolving threats.

According to the National Association of Insurance Commissioners (NAIC), the US' top 20 cyber insurers reported an average loss ratio of 66.9% in 2020. Three of those companies saw losses exceed 100% of their total premiums.

Insurers look set to raise their premiums to compensate, and this is forcing customers to look for alternative options. Some experts predict larger businesses will start to self-insure. But this isn't always an option for SMEs.

82% of cyber insurers expect premiums to increase

#2 Policy adoption rates remain low

Rising premiums, stringent qualifying requirements, and a lack of understanding about the benefits of a standalone cyber insurance policy will continue to curtail adoption rates.

The latest UK government data shows that 50% of SMEs have some form of cyber insurance, but only 10% of small companies have a specific, standalone policy to protect their digital assets. Most of the businesses that do are in the financial and insurance sectors.

Insurers must adapt their models or create effective and affordable products, specifically for SMEs, to reverse this trend.

10% of small businesses have standalone cyber insurance

#3 Automated attacks become more common

Automated cyberattacks allow hackers to programmatically identify vulnerabilities in your website's defences. It requires little to no manual input, which enables hackers to scale their activities and generate profit much more efficiently. And due to a rise in bot traffic, they're becoming more frequent.

SMEs received 5.5x more website visits from bots than people in 2021. There are legitimate uses for bots, like search engine crawlers. But malicious actors can also use them to infect your website with malware, steal sensitive data, and more.

For example, recent years have seen an uptick in hackers targeting business ad accounts. Once they have control of your account, hackers can change your page name, run malicious ads, and spend thousands in a matter of hours. When hackers infiltrated Smart Marketer's Facebook ad account in 2020, they spent over $4,000 in 46 minutes.

A successful attack can cause extensive financial and reputational damage. In the coming years, insurers will need to review and update their policies to provide the most coverage for their customers.

> SMEs received **5.5x** more website visits from bots than people in 2021

#4 Hackers target supply chains

Supply chains have become a prime target for hackers, as demonstrated by the Colonial Pipeline ransomware attack of 2021. 62% of enterprise cyberattacks target vulnerabilities in customer-supplier relationships. And, given that 77% of SMEs are part of a supply chain, this poses a significant threat.

The latest government data shows that only 13% of UK businesses assess the cybersecurity risks of their immediate suppliers. Worse, only 7% consider the wider supply chain. Often this comes down to trust. SMEs automatically assume that their suppliers have taken the appropriate steps to protect themselves from cyber threats. But that isn't always the case and SMEs must be more discerning about who they work with in 2023.

13% of UK SMEs review the cybersecurity risks of their immediate suppliers

> **Supply chain attacks are a major cyber threat facing organisations and incidents can have a profound, long-lasting impact on businesses and customers. With incidents on the rise, it is vital organisations work with their suppliers to identify supply chain risks and ensure appropriate security measures are in place.**
>
> IAN MCCORMACK,
> NCSC DEPUTY DIRECTOR FOR GOVERNMENT CYBER RESILIENCE

#5 BEC and ransomware attacks intensify

Identified global losses from business email compromise (BEC) attacks rose by 65% between July 2019 and December 2021. Harnessing AI-powered deepfake technology, BEC attacks allow malicious actors to trick employees into transferring funds or sharing sensitive information over virtual meeting platforms. In one high-profile case, criminals stole $35mn by impersonating the voice of a company director and tricking an employee into transferring the funds.

Ransomware attacks are also becoming more frequent, with double and even triple extortion attacks now the norm. Ransomware attacks rose by 92.7% in 2021, and SMEs are taking the brunt of the punishment. Smaller businesses may not have the resources to afford robust cybersecurity, and this makes them a more enticing target to criminals than enterprises that typically have the best protection money can buy.

Some insurers don't include ransomware coverage in their policies and even if the victim pays the ransom, there's no guarantee they'll get their data back. Then there's the ongoing debate as to whether it's legally or morally right to agree to the hacker's demands.

> Ransomware attacks rose by **92.7%** in 2021

Prevention is better than cure

What do these cyber insurance trends tell us? For starters, cyberattacks are becoming more sophisticated and harder to ignore. And while adoption rates remain low, interest in standalone cyber insurance policies is growing, with new products entering the market to satisfy that need.

Cyber insurance won't stop a careless employee from clicking on a spurious link or keep out a determined hacker, but it will cushion the blow and get you back to business faster.

Active Protect from CyberSmart provides proactive threat protection and monitoring to secure your business against the most common cybersecurity threats. You'll also have access to expert advice, as well as 24/7 breach response and recovery support to help you get back on your feet, fast.

Get in touch