

beazley

Risk & Resilience

Spotlight on Cyber & Technology Risks for UK SMEs

Key UK SME insights, September 2023



Executive Summary

Is the ever-present threat of evolving cyber risk creating an era of cybersecurity complacency?

With indications that Russian and Ukrainian cybercrime groups are starting to regroup as they seek to recoup lost profits, having splintered when the conflict in Ukraine broke out in 2022, organisations of all sizes are likely to find themselves back on the front line in the fight against cyber-attacks. However, our research reveals that many small businesses could be being lulled into a false sense of security when it comes to cyber risk as it is dropping down their risk radar, despite saying they feel less resilient to this risk.

Our annual Risk & Resilience survey of 2000 global business leaders explores how cyber risks are increasing and cybercrime groups diversifying, how technology risk is impacting businesses, and why the emergence of AI and other innovations are demanding the attention of risk and security experts.

Small and medium sized businesses (SMEs) have often, wrongly, believed that they are not targets for cyber criminals and whilst our findings show there is growing recognition of their palpable exposure, small businesses believe their cyber risk will fall in the future. However, the reality is that smaller businesses are often targeted by cyber criminals, as their IT security is often weaker, and they can offer an easy access point into interconnected supply chains. In addition, many smaller businesses have valuable customer data that criminals can exfiltrate and sell.

Cybercrime groups are also becoming more specialised and diversified and SMEs can provide a training ground for new cyber criminals to learn their trade. Our data shows that although SMEs are concerned about cyber security and failing to keep pace with technology advancements, their perception that cyber risk is falling is contrary to reality.

Contents

01

Small businesses believing they can fly under the radar due to their size may be set for a wake-up call.

03

Are businesses becoming dulled to cyber risk despite costs reaching new highs?

02

Just under a quarter of SMEs feel acutely exposed to cyber security risks.

04

SMEs feel ill-equipped to keep pace with advancing technology.

Too small to matter?

"SME's often have weaker security systems, and they are viewed by cyber criminals as good training ground for novice hackers."

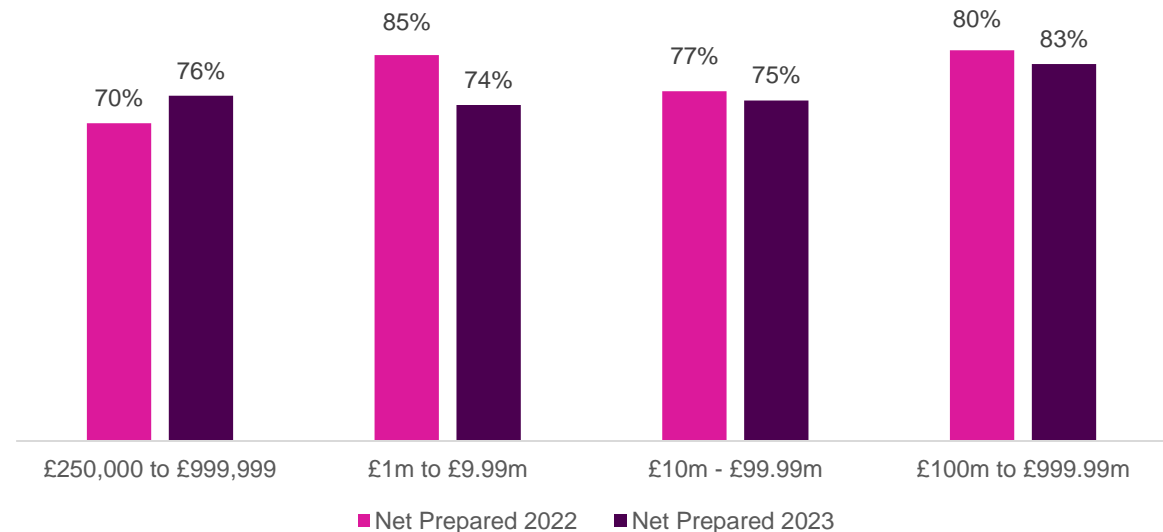


Matthew Norris

Territory Manager, Beazley Digital

Businesses that believe they can fly under the radar due to their size may be set for a wake-up call

Percentage of Business Executives Feeling Prepared to Anticipate and Respond to Cyber Risk



Our research suggests small businesses (£250,000-£999,999) feel that they are more prepared to anticipate and respond to cyber risk this year relative to last year. Additionally, small businesses believe their operating environment will become more secure in the coming months, with those projecting that they will be operating in a high-risk environment dropping from 33% now to 30% in 12 months' time. This perception of cyber risk shows that there is a danger that the ever-present threat of cyber risk could be creating cyber fatigue amongst smaller businesses as they face a myriad of other risks and issues.

Just under a quarter of small businesses believe that cyber security risk is their top threat.

“Fresh exposures to for businesses will likely occur if cyber gangs exploit AI for new criminal activity. SMEs often lack the security measures and skills to deal with cyber threats.”



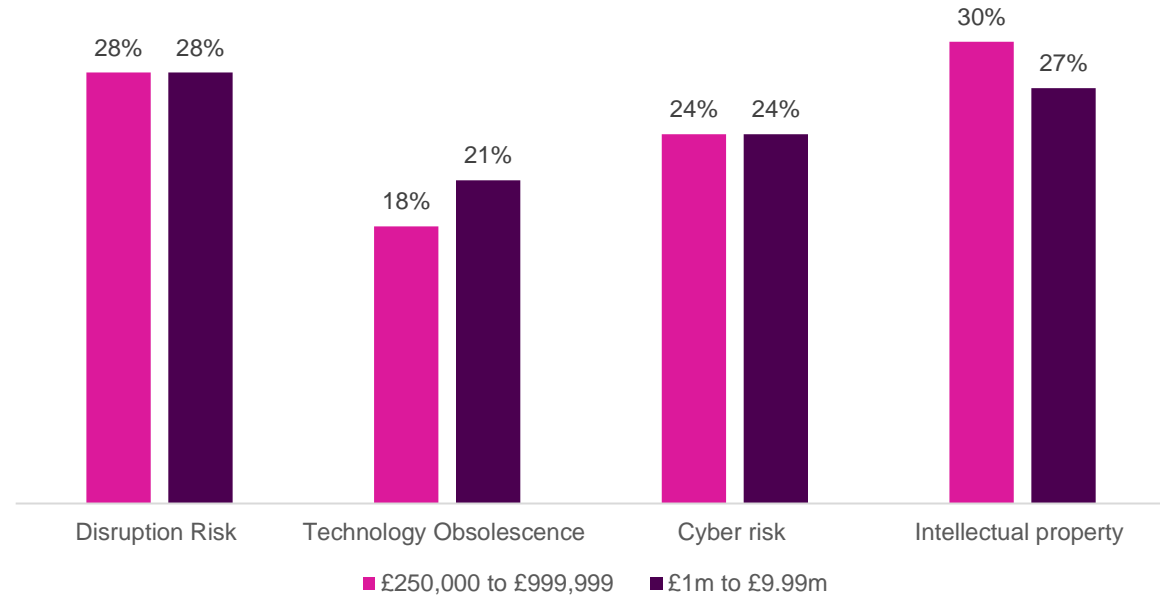
Samantha Coffin

Claims Focus Group Leader,
International Small Business
Claims

beazley

Small businesses feel unprepared to anticipate cyber risk in 2023

Percentage of UK Executives Ranking Cyber as top risk



Small businesses are realising that cyber risks are becoming more prevalent and a wider threat to operations. 24% of UK executives believe cyber security risk is their business’s top threat, falling behind disruption (28%) and intellectual property risk (27%).

Companies with an annual revenue of £250,000 to £999,999 indicated a growing recognition of their palpable exposure, stating that they now feel less prepared to deal with cyber risks in 2023 (69%) than they did last year (74%).

Businesses becoming dulled to cyber risk despite costs reaching new highs.

"While the turbulence in the Ukraine-Russia conflict has temporarily disrupted cyber gangs, leading to a decrease in the frequency and severity of cyber risks... fresh threat actors are entering the fray, driven by the need to recover lost earnings. Small businesses cannot overlook the importance of robust cyber protection; it should be of paramount concern."

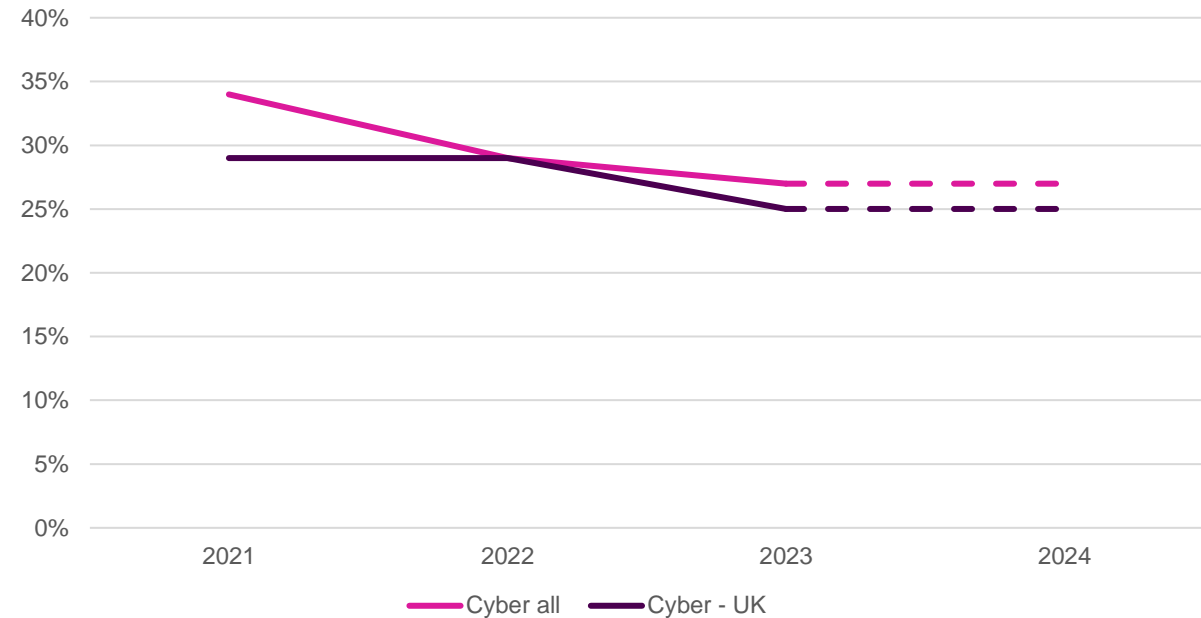


Jad Nehme

Client Experience Manager,
Cyber Risks

Small businesses mistakenly predict that their operating environment will become more secure in the coming months

UK business seems least concerned about cyber risks compared to international counterparts, as percentage ranking cyber as top risk falls



Our data shows that the perceived threat of cyber risks for businesses globally has declined since 2021 and resilience has also dropped year-on-year. The percentage of UK businesses choosing cyber risk as their top concern has been consistently lower than the rest of the world. Businesses that have invested in security should take comfort that it has improved their defence, but cyber risk is evolving. Where once cybercriminals took weeks to gain access to a network, now it is often only hours.

Limited resources to maintain momentum and update obsolete tech is hitting small businesses hard

“SMEs constrained by limited resources, tend to allocate less of their capital towards updating computer systems and modernising their IT network. This scenario is mirrored across various industries, where data-abundant yet financially challenged companies find themselves without the essential digital infrastructure, and susceptible to cyber attack.”



Carl Oliver

Cyber Underwriter

SMEs in the UK and US said they are ill-equipped to maintain their technology and systems in line with new developments

Percentage of UK & US executives feeling unprepared to anticipate and respond to technology obsolescence



Our data shows smaller businesses that lack the resources to maintain the relentless momentum of updating evolving tech feel the most exposed to tech obsolescence. Nearly three in ten (29%) UK and US businesses surveyed with an annual revenue under £1m reported feeling unprepared for the risk of their technology becoming outdated. The advent of AI represents the latest peak in technological advancement and businesses everywhere are scrambling to understand how they can benefit and where they may be at risk. However, for the moment, ensuring that they are keeping up with the more mundane patches and upgrades to existing systems is proving challenging for some businesses.

Methodology

Beazley Digital Contact Details



Matthew Norris

Territory Manager, Beazley Digital

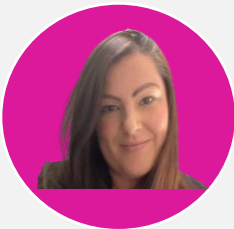
matthew.norris@beazley.com



Sam Franks

Regional Development Manager

sam.franks@beazley.com



Sarah Beckett

Broker Relations Manager

sarah.beckett@beazley.com

During January and February 2023, we commissioned research company Opinion Matters to survey the opinions of over 2,000 business leaders and insurance buyers of businesses based in the UK, US, Canada and Singapore with international operations. Survey participants were asked about their views on insurers and insurance, as well as on four categories of risk:

- **Cyber & Technology** – including the threat of disruption, failure to keep pace with changing technology, cyber risk and IP risk.
- **Environmental** – including climate change and associated catastrophic risks, environmental damage, greenhouse gas emission, pandemic, food insecurity and energy transition risk.
- **Business** – including supply chain instability, business interruption, boardroom risk, crime, reputational and employer risk and failure to comply with ESG regulations and reporting requirements.
- **Geopolitical** – including strikes and civil disruption, changes in legislation and regulation, economic uncertainty, inflation and war & terror.

Of the firms surveyed, there was an equal split of respondents across company sizes of: £250,000 - £1 million, £1,000,001 - £10 million, £10,000,001 - £100 million, £100,000,001 - £1 billion, more than £1 billion. With a minimum of 50 respondents per country per industry sector, respondents represented businesses operating in:

- Healthcare & Life Sciences
- Manufacturing, Retail, Wholesale and Food & Beverage
- Commercial Property, Real Estate and Construction
- Hospitality, Entertainment and Leisure (including Gaming)
- Financial Institutions and Professional Services
- Energy and Utilities (including Mining), Marine and Warehousing
- Public Sector and Education
- Tech, Media and Telecoms
- Transportation, Logistics, Cargo and Aviation

[Access the full Spotlight on Cyber & Technology Risk Report](#)

Discover more

[Cyber insurance for small businesses](#)

The descriptions contained in this communication are for preliminary informational purposes only. Coverages can be underwritten by Beazley syndicates at Lloyd's or Beazley Insurance dac or Lloyd's Insurance Company ("Lloyd's Brussels") and will vary depending on individual country law requirements and may be unavailable in some countries. Coverages are available in the US only on a surplus lines basis through licensed surplus lines brokers. The exact coverage afforded by the products described in this communication are subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk.

© 2023 Beazley Group

beazley



Insurance. Just different.