# Spotlight on: Cyber and technology risk

Vigilance is key to tackling ever-present cyber risk.

beazley

# The Beazley View

## It's not OK to be blasé

Vigilance is the key to tackling ever-present cyber risk, as well as growing concerns over intellectual property risk particularly as business leaders' perception of their cyber and tech resilience declines.

As the pandemic receded in the early part of 2022, instead of being able to heave a sigh of relief business has been forced to confront once in a generation geopolitical uncertainty, of which fuel and food price inflation is perhaps their most immediate concern. Which is to say nothing of the supply chain crunch that started in the pandemic and has run full steam ahead through 2022, or of February's shock ignition of a hot war between Ukraine and Russia. In this environment it comes as no surprise to us that cyber threats, which to date have not been a major feature of the Ukraine conflict, have slipped down business leaders' risk radar.

However, our belief is that this position, whilst understandable, is naïve.

It is true that efforts over the past decade to increase awareness of the cyber threat have spurred mitigation actions including enhanced risk management and the buying of insurance. However, this may have created the illusion that the issue has been dealt with and there is nothing more to worry about. This 'cyber fatigue' coupled with today's very visible geopolitical challenges make it unsurprising that business may have adopted a potentially dangerous 'out of sight, out of mind' view of cyber.

# Executive summary

## Our latest Risk & Resilience research indicates business leaders' concerns about cyber and tech risks have shifted.

While there is still general unease about cyber risks with the drop in business leaders' confidence about their resilience to the threat of cyber risk, we are detecting signs that they may have become a little blasé – even over-confident – about the cyber and technology risks faced by their businesses. This is perhaps because the overwhelming challenge that the current geopolitical and economic environment poses today is detracting their attention from the threat that cyber and tech risk may deliver tomorrow.

Fears about the threat to intangible assets from cyber criminals have also been increasing. At the same time, some businesses are wrestling with the costly challenge of replacing end-of-life systems as they try to keep pace in an increasingly tech-dependent world.

While the outbreak of war in Ukraine has created huge ripples in geopolitical terms, disrupting global trade, it remains to be seen what effect it will have on cyber exposures. The threat of a surge in state-sponsored hacking comes hard on the heels of a global move to remote working which has either validated companies' contingency planning or exposed the limitations of their IT infrastructure.

For companies with creaking legacy IT systems, the spectre of **technology obsolescence** – the failure to keep pace with changing technology developments and opportunities, or to update systems – looms ever larger as they attempt to adapt to today's operating challenges.

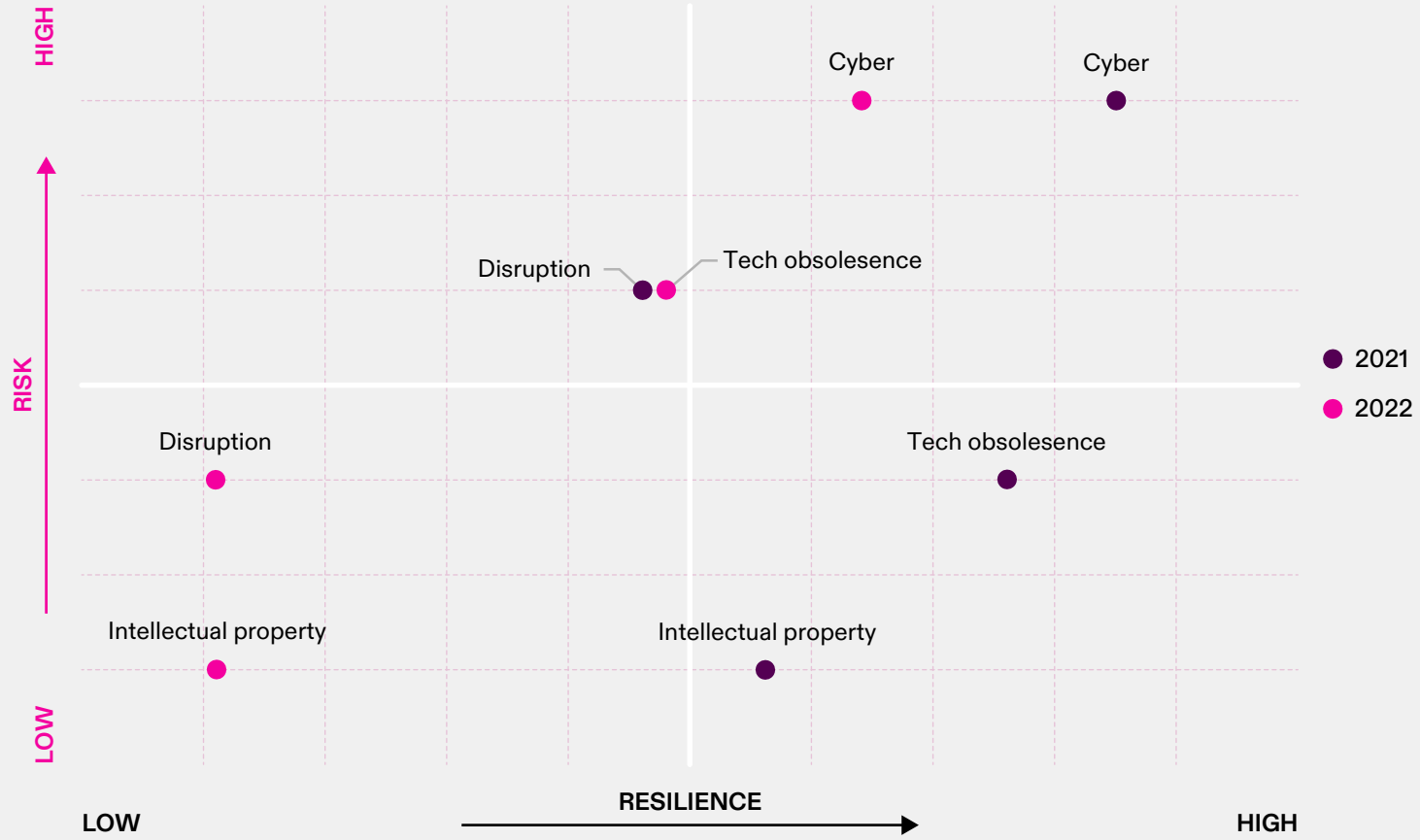
This is reflected in our survey, with technology obsolescence the **number one concern** for **27%** of UK and US business leaders, displacing **tech disruption** in the rankings and highlighting the fact that with technology is becoming an increasingly important part of economic activity, getting left behind poses an existential risk to businesses.

In the meantime, concern about **Intellectual Property (IP)** risk has also been increasing. IP disputes have become more frequent[1], so-called 'cyber-squatting' has surged[2] and there has been an alarming growth in the numbers of filings by 'patent trolls'[3], with US businesses in particular alert to the risk of IP theft from companies in China.

While IP remains low on the list of technology concerns, the proportion of companies listing it as a key issue has **grown dramatically, more than 107%, in the UK and US since last year,** while resilience has fallen, suggesting this will be a key area to watch.

# Executive summary

**Change in risk & resilience perceptions from 2021-2022 from business leaders in the UK and US**




**Not all companies are as prepared as they believe themselves to be**

"It can be easy for companies who've never experienced a cyber attack to underestimate their level of preparedness... but the fact of the matter is that cyber risk isn't going away and companies are more dependent on technology than they've ever been in the past."

**Patricia Kocsondy**
Head of US Cyber & Tech

# Key findings

## The Yin and Yang of cyber risk and resilience

**Cyber** is the leading concern within the cyber and technology risk category for all respondents in 2022, with **28%** of business leaders listing it as their number one risk. However, fewer business leaders in the UK and US cited it as a leading risk compared with last year. Resilience perceptions have fallen slightly since 2021, down 2 percentage points at **41%.** A lessening concern about cyber risk appears to be tempered by some erosion of business leaders' confidence about the readiness of their firms' cyber protection.

### Lack of investment leads to disruption and obsolescence concerns

Faced with continuing capital constraints some businesses appear reluctant to commit to the cost of transforming systems and processes potentially leaving them open to greater cyber, disruption and technology obsolescence risks going forward.

### Post-pandemic fatigue and economic woes could fuel disruption

**Tech Disruption** is less of a concern than last year, but the perception of resilience has also dropped for UK and US business leaders, down 4 points at **36%.** The double whammy of a depressed economy and the failure by some to bounce back from the pandemic as quickly as their competitors could leave them open to disruption by more agile rivals.

### Obsolescence concerns increase

**Technology obsolescence** has moved up the risk scale since last year, cited as a leading concern by around **27%** of UK and US leaders, and swapping places with disruption. Resilience has also dropped, possibly as companies struggle with the cost and effort of updating or replacing legacy systems.

### IP risk is an accident waiting to happen

The low level of preparedness for **IP** threats at the same time as concern is increasing, raises a red flag. IP still features lowest on business leaders' risk registers, with only 21% of all respondents putting it first. However, in the UK and US, the proportion of business leaders putting IP concerns top has increased by **107%** since last year.

### Cyber hygiene is key to insurability

As companies confront issues such as end-of-life technology, enhanced cyber risk linked to the geopolitical situation, and the impact of inflation on business and investment, leaders will nonetheless need to focus on **improving cyber hygiene**. With pricing for cyber insurance rising, insurers are becoming more selective about which cyber risks they write. Cyber insureds therefore need to regard **cyber resilience and risk management** as much more than a tick-box exercise, as they seek to protect intangible assets and ensure business continuity.

# Contents

# Cyber fatigue is the sting in the tail

Now that the technical demands of operating through the pandemic have eased, and businesses have adapted to a more digitally-enhanced environment it would be tempting to conclude the challenges of cyber and technology risks have dramatically reduced for many business leaders. In truth, what our Risk & Resilience research reveals is that the same concerns persist, but the picture has been re-drawn.

Cyber is still top of the list in our cyber and technology risk category, but resilience has dipped as some businesses struggle to keep pace with a continually evolving risk landscape. Meanwhile, IP continues to feature lowest on the risk list while disruption has slipped down the rankings, but as our cyber and technology experts indicate, business leaders should be cautious about taking either risk too lightly.

A recent report looking at cyber claims experience, Beazley Cyber Services Snapshot revealed that cyber risk remains a persistent threat to organisations, with no appreciable change in incidence but with an emerging sophistication in the approach taken by threat actors. Data exfiltration is now prevalent in a significant majority of incidents reported to our cyber services team, as threat actors find new ways to do business, resulting in double and even triple-extortion events.

**Fading resilience**

Cyber and technology risks might be less prominent this year, but perception of resilience across the board has dropped, hinting at underlying fatigue that belies business leaders' apparent confidence about exposure and resilience levels.

**28%**

Cyber remains the top concern in the cyber and technology risk category, with 28% of business leaders in the UK and US putting it at the top of their list for 2022

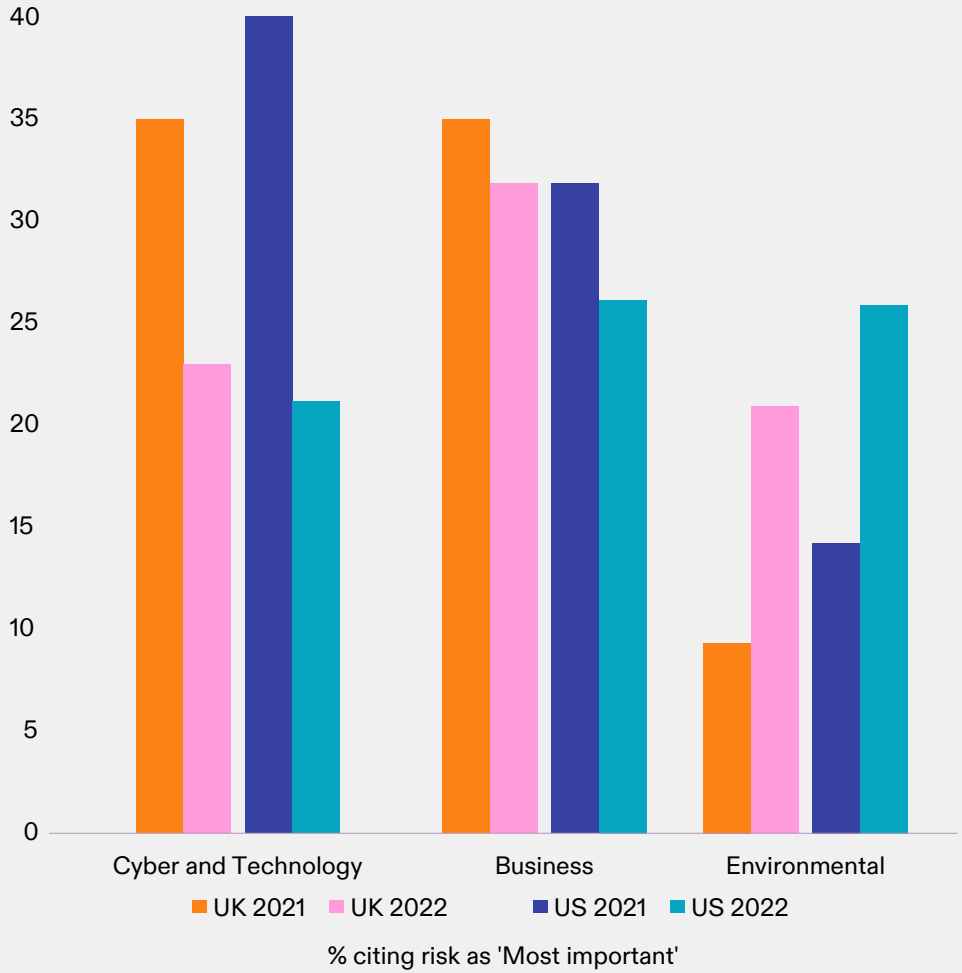
# Cyber and technology slip down the overall rankings

## But cyber is still a leading concern for many.

When we surveyed UK and US business leaders about their risk and resilience perceptions last year, the technology risk group (renamed as 'cyber and technology' for 2022) was top of their list of concerns – both at the beginning of 2021 and when business leaders looked ahead to the beginning of this year.

However, in 2022, the picture is very different. Across all survey respondents[4], business risks are now the leading concern, with cyber and technology risks predicted to ease slightly in 12 months' time – a trend that is mirrored in the response from UK business leaders. For US leaders, environmental risks dominate throughout the year, matched only by business risks as they look ahead to January 2023.

**Most important risk categories 2021-2022**



# Cyber and technology slip down the overall rankings

The push towards increased hybrid and home working has created new cyber exposures for businesses, and while many have sought to reduce the risk by deploying virtual private networks (VPNs) and multi-factor authentication (MFA) protocols on equipment used by remote-working employees, the attack surface for cyber criminals is likely to have increased. Indeed, the incidence of phishing emails and messaging surged and attacks involving ransomware doubled globally last year[6].

Indeed, cyber remains the number one technology risk for business leaders, with 29% of all respondents listing it as their number one risk in 2022, and 28% of UK and US business leaders putting it top of their list. As this year's report indicates, it is a risk which business leaders still feel well-prepared for, although perceptions of resilience have dropped since last year, from 44% of UK and US business leaders who felt 'very prepared' in 2021, to 41% this year.

The outbreak of hostilities between Russia and Ukraine - and growing Russian belligerence towards Europe and the US – has raised the additional prospect of an increase in state-sponsored cyber-crime activity. However, activity emanating from this region is more likely in the short term to be focused on the combatants, potentially lowering the risk for UK and US businesses.

**"The bad actors that Russia and Ukraine may or may not have been harbouring for quite some time became involved in a cyber war between those two countries, and so instead of directing their efforts at extorting Western companies they are looking instead at how they can take down each other's assets. That has perhaps led to a lull in cyber activity that's affecting the Western world. We do still see cyber attacks – the threat hasn't gone away, but it's tapered."**

**Patricia Kocsondy**
Head of US Cyber & Technology

# Obsolete systems could be the kiss of death

Businesses in the mid-market space in particular may be struggling to reconcile what is being asked of them by insurance and technology partners to reduce their exposure to cyber and technology risks, when faced with the cost and resources required to implement changes to legacy systems. For many businesses, the priority in the last few years may have been to simply stay afloat and keep operating, but those legacy systems are likely to be an albatross around the neck of their future competitiveness.

End-of-life systems present an existential risk to some companies, as service providers discontinue software and hardware support, interaction with third party systems becomes more difficult, and the spectre of technological obsolescence looms. Legacy systems that have a high degree of interconnectivity within a company's network also pose a greater risk of security breach and, from an underwriting standpoint, are viewed as inherently more vulnerable and therefore more difficult to insure.

Technology obsolescence also has a degree of crossover with disruption risk – the failure to innovate, or to keep pace with new developments, competitor activity, customer demand or market shifts. The prospect of a company being disrupted by a relatively new technology provider is a real threat to businesses – whether it is taxi firms being replaced by Uber and Lyft, to Amazon replacing grocery stores – there is still plenty of disruption for companies to be concerned about.

However, technology has also been an enabler as well as a disruptor of traditional business models. The reduction in perceptions of disruption risk reported by business leaders in the Hospitality, Entertainment and Leisure sector, for example, could be attributed to their leveraging of online platforms to facilitate takeaway food orders, digital streaming of live events, and remote ordering at bars and restaurants during lockdown for al fresco consumption.

In both a disruption or an obsolescence scenario there is the potential for management and boards to come under intense scrutiny with the potential for a knock-on effect on D&O cover, if they make the wrong call and fail to adapt their technology to keep up with or ahead of their competition.

# Cyber risk is still out there

## Constant cyber vigilance is essential

While cyber-crime has largely moved on from the theft of personal confidential information, and therefore the threat of large regulatory fines and class actions following the loss of client data, internal IP remains an area of concern. Since the onset of the 'great resignation' phenomenon[5], companies – particularly in the tech space – may be feeling more vulnerable about the risk of their IP moving with former employees to rival companies.

As business leaders look ahead to 2023 therefore, cyber and technology risks might have slipped below business risks in the overall rankings, but for risk managers, technology providers, and the insurance community, the risk of a black swan event from this parcel of risks is still prominent.

Physical supply chain issues have overtaken cyber as the key resiliency topic, but with society becoming ever-more dependent on technology and a growing number of tentacles in the software supply chain, underwriters and risk managers face the challenge of identifying technological interdependencies that could present a systemic risk.

Recent experiences with the SolarWinds cyber-attack and Log4J zero-day vulnerability have indicated the extent to which cyber risk can permeate an entire technology ecosystem. With an increasing number of businesses becoming entirely dependent on cloud computing, a major attack on a cloud provider could have huge repercussions.

The nature of some of the entities that have recently suffered cyber-attacks – from hospitals and healthcare systems, to the Colonial Pipeline and Australian meat-processing firm JBS[6] – indicates the potential 'real world' threats from cyber-crime. With food and energy supplies already disrupted by war in Europe, further threats to these two key commodities from hackers are a serious concern.

With the regular drumbeat of hacking events, cyber has become more of a mainstream issue. Corporations are focusing more on cyber security and resiliency than they have in the past, to the point where many perhaps believe they are ready for any attack. However, it is worth noting that unless businesses have actually experienced an attack and have come through it relatively unscathed, they run the risk of over-confidence about their exposures and resilience.

Given that many companies, particularly in the SME space, may overlook basic cyber hygiene such as enabling multi-factor authentication on all user accounts or closing unused ports it is clear that greater vigilance is needed from business leaders around their cyber and technology exposures. Constant risk management is one of the benefits that partnering with a cyber insurer can bring, to improve businesses' cyber hygiene and increase their resilience to cyber and technology risks.

### Are companies over-confident about cyber preparedness?

**"An increasing number of companies are experiencing cyber-attacks and the maturity of their control procedures is often low, meaning they are unprepared for an increase in activity. The relatively high percentage of business leaders who feel 'very prepared' for cyber risks is therefore concerning, when you consider that the threat landscape has continued to evolve."**

**Aidan Flynn**
Head of London and International Underwriting Management, Cyber

# UK-US differences

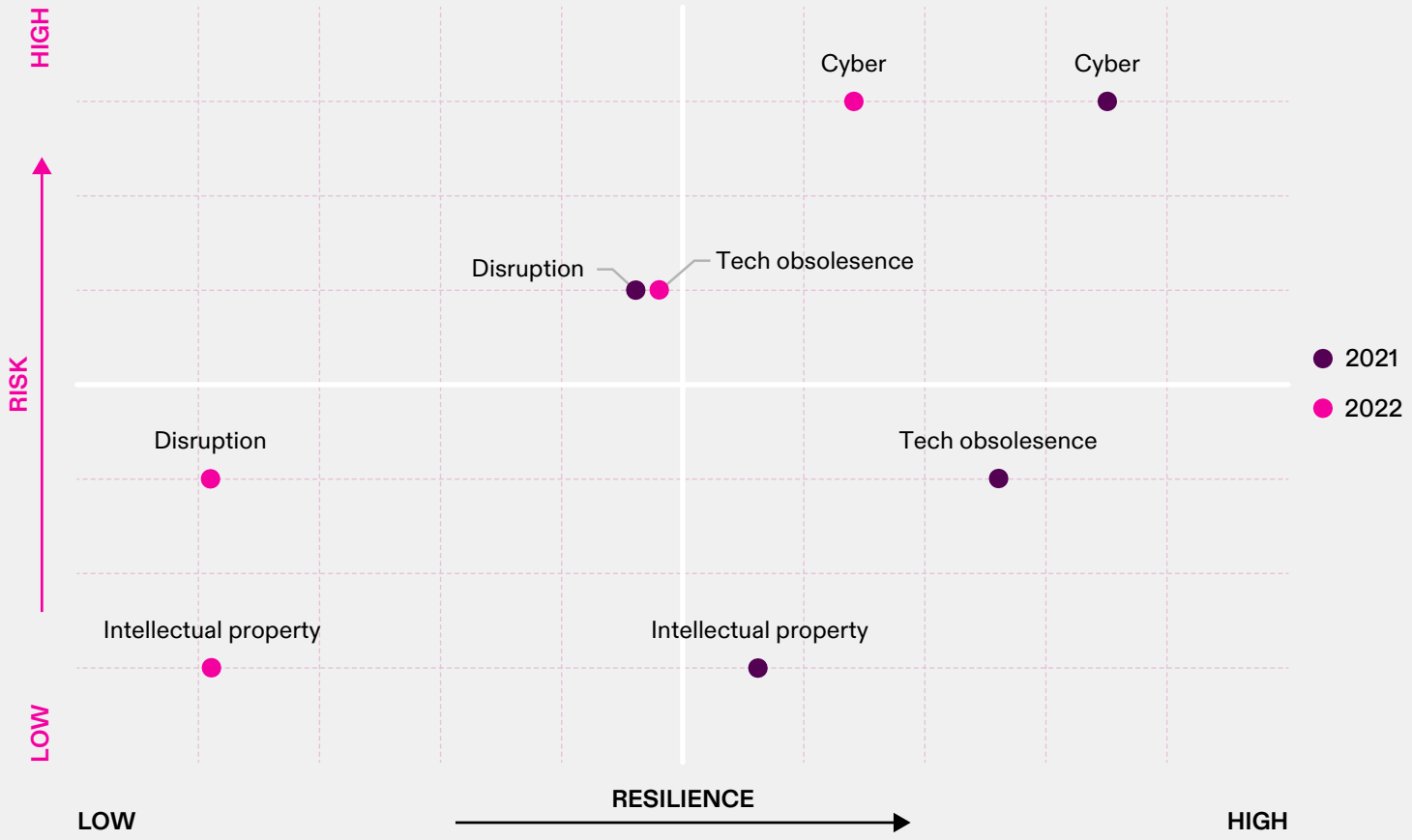
## US and UK leaders diverge on the threat of cyber and IP risk

In last year's report we found that that the cyber threat topped all other risks but was felt most strongly in the US, but this year shows a marked change in sentiment.

UK business leaders putting cyber risk top changed by less than 1 percentage point (0.3 points, roughly 1%) from 2021-2022, at around 29%, but the proportion of US leaders listing it as their leading concern dropped nearly 12 points (around 31%), to 27%.

However, the change in perception of cyber resilience tells a more interesting story. With such a dramatic change in risk perception, a surge in those claiming to be 'Very prepared' might have been expected but the proportion was down slightly – falling 0.5 points (about 1.5%) in the UK and over 3 points (around 6.5%) in the US – suggesting that companies need to get 'match fit' for the next inevitable spike in cyber-attacks if they are to justify their drop in concern.

### Change in risk and resilience perceptions from 2021-2022 from business leaders in the UK and US



# IP risk is one to watch

## IP risk is growing fast

Another notable finding last year was that survey respondents appeared to have a “blind spot” when it came to IP risks. The growth in IP disputes between companies in the US and China in recent years, and an uptick in IP litigation more generally, suggests this is an area to watch for business leaders.

Indeed, experience may explain, while IP remains the least important risk for UK businesses, the proportion of leaders putting IP risk top has increased by 8.5 points (77%), while in the US, risk perception has increased by more than 14 points (241%) compared with 2021 – taking it to third on the risk list for US leaders. While resilience hasn’t changed quite as dramatically, it has fallen for IP risks, down 5 points (13%) for UK leaders, and 4 points (9%) for US leaders.

**107%**

Against a background of increases in IP disputes, cyber-squatting and patent trolling, the proportion of UK and US leaders citing IP risk has risen, compared to 2021. This year sees a 107% year-on-year increase in it being ranked as a leading concern

# Risk perception varies by sector

## Intellectual property

Six out of the 10 industry sectors had a **10+ point increase** in leaders listing IP as their top concern. Hospitality, Entertainment and Leisure and Marine and Warehousing both saw a 16-point increase (a **rise of 366% and 152%**, respectively, in real terms) on last year, perhaps reflecting the vulnerability of both sectors to phishing and ransomware attacks.

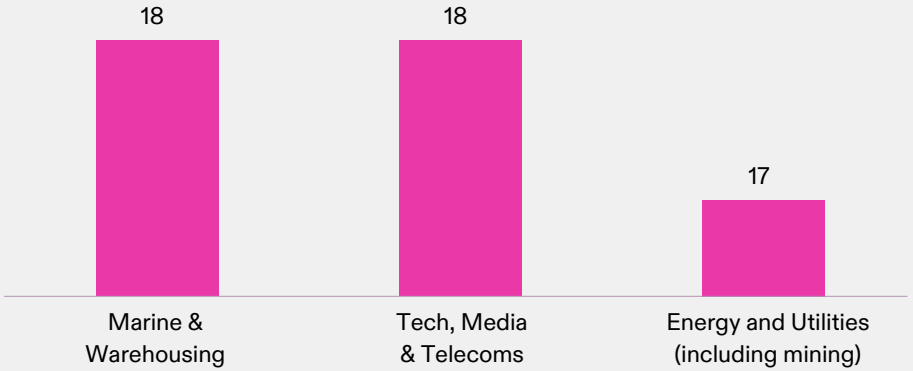
**% point increase in risk perception 2021-2022 (UK & US)**

# Risk perception varies by sector

## Cyber

For the most part there was greater optimism about **cyber** risks in 2022, with two notable exceptions. The proportion was **up 19% in Financial Services** and **5% in Manufacturing**, reflecting the findings of Beazley's Cyber Services Snapshot, where percentages of system infiltrations during just Q1 of 2022 for both sectors drew close to 2021 full-year totals.

**% point decrease in risk perception 2021-2022 (UK & US)**




% point decrease in firms listing risk as #1

# Risk perception varies by sector

## Disruption

Successful efforts to re-establish fractured supply chains appear to have buoyed up the Manufacturing sector, which registered the biggest decrease in business leaders placing **disruption** at the top of their risk list, down 13 points (or 39% on last year). Hospitality, Entertainment and Leisure similarly seems to have relaxed following pandemic challenges.

**% point decrease in risk perception 2021-2022 (UK & US)**

# Resilience drops

## Cyber

Supply chain issues still feature, while cyber lurks. Despite the drop in **cyber** concerns, there were some significant reverses in resilience, with the proportion of leaders describing their company as ‘very prepared’ down 14 points (27%) on last year in Technology, Media and Telecoms and 9 points (17.5%) in Retail, Wholesale, Food & Beverage. Both sectors appear to be prominent targets for novel approaches by threat actors.

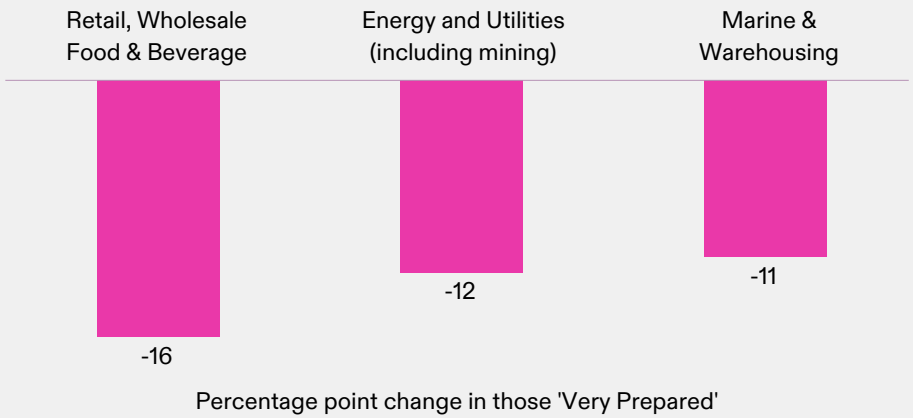
**Biggest resilience drops by sector – 2021-2022 (UK & US)**

# Resilience drops

## Intellectual Property

For **IP** risks, resilience fell most notably in Retail, Wholesale, Food & Beverage (16 points or 34%), Energy and Utilities (12 points or 27%), and Marine and Warehousing (11 points or 29%). All three sectors have experienced major supply chain difficulties in recent years, but ageing tech in some sectors could also leave them vulnerable to data theft.

**Biggest resilience drops by sector – 2021-2022 (UK & US)**

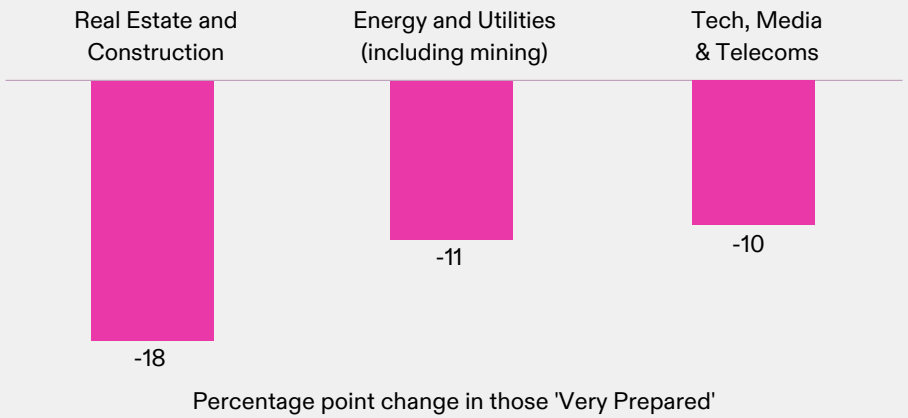


# Resilience drops

## Disruption

Significant drops in resilience to disruption risk were seen in Real Estate and Construction (down 18 points or 41%), Energy and Utilities (11 points or 24%), and Technology, Media and Telecoms (10 points or 21%). The rollercoaster ride for Energy and Utilities firms in recent years has raised concerns about longer-term supply chain issues, which is energising a growing renewables sector.

**Biggest resilience drops by sector – 2021-2022 (UK & US)**




### Why has cyber resilience dropped?

**"The key question for businesses is 'How insurable am I?' Mid-market clients are struggling to keep pace with what is being asked of them in terms of funding, budgeting for, and repairing technology to keep pace with cyber risks. We are placing more emphasis on how to handle end-of-life software and hardware issues, and industries are in catch-up mode now to budget for what their insurers require. Business leaders might not want to undertake cyber hygiene, but they need to do it."**

**Bala Larson**
Head of Cyber Client Experience

# Methodology

**About the Risk & Resilience research**

During January and February 2022 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.
- 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.
- Environmental – including climate change and associated catastrophic risks, environmental damage, greenhouse gas emission, pandemic, food insecurity and energy transition risk.

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 40 respondents per country per industry sector, respondents represented businesses operating in:**

- Healthcare & life sciences
- Manufacturing
- Retail, wholesale, food & beverage
- Real estate and construction
- Hospitality, entertainment and leisure (including gaming)
- Financial institutions & professional services
- Energy and utilities (including mining)
- Public sector & education
- Tech, media & telecoms
- Marine & warehousing

## Contributors

**Patricia Kocsondy**
Head of US Cyber and Tech
Beazley

**Aidan Flynn**
Head of London and International Underwriting Management, Cyber Risks
Beazley

**Bala Larson**
Head of Cyber Client Experience
Beazley

## Footnotes

1. Chinese courts flex intellectual property muscle across borders | Financial Times
2. WIPO Domain Name Dispute Resolution Surges | World Intellectual Property Organization
3. New Data Shows Tech Patent Troll Cases Are Rising At USITC | Forbes
4. Respondents across all countries surveyed, in the UK, US, Singapore and Canada
5. Great Resignation shows no signs of slowing down: 40% of U.S. workers are considering quitting — here's where they're going | Fortune
6. The latest cyber attack victim is the world's largest meat supplier | Fortune

**Beazley**
22 Bishopsgate
London EC2N 4BQ

**beazley.com**



beazley