

Risk & Resilience

September 2021

Spotlight on technology risk



beazley

Introduction

With Covid-19 in full force, we embarked on an exercise to understand how businesses felt about four key areas of risk: technology, business, political & economic and environmental, both now and in 12 months time.

While the impact of the pandemic has been significant across many sectors, in the UK and the US it is the technology risk category - which includes cyber risk, disruption, online intellectual property protection, and the tech risk of failing to keep pace with changing technological developments and opportunities - where concern is most keenly felt by over 1,000 business leaders in the UK and US across 10 different industry sectors that we surveyed.

In this time of seismic change, where all our known knowns have been disrupted, why does the technology risk category top the risk table now, and in 12 months' time?

The technology risk category is ranked top by some margin. Well over a third (37%) of business leaders in the UK and US perceive it to be their most pressing area of concern now. That proportion rises to 39% as we look ahead 12 months. But although these risks are challenging to manage, the good news is that executives are not in a mood to wave the white flag any time soon.

Key takeaways

- **Cyber** – is the highest ranked risk in the technology risk category, particularly by those in the US, but companies feel better prepared to manage it than any other risk.
- **Disruption risk** – the failure to innovate, and keep pace with new developments, customer demand or market shifts - runs cyber a close second, largely because among UK respondents it is the key concern, and businesses feel much less well placed to anticipate and manage this risk.
- **In terms of tech risk** – not adapting to changing technology developments and opportunities – successful companies have harnessed a combination of astute hiring and investment to ensure they manage this threat appropriately. Consequently, resilience scores are high (a median of 44% of UK and US businesses feel very prepared for tech risk challenges).
- **Intellectual property (IP)** – the failure to protect the value of IP and other intangible assets – is the outlier, a risk that businesses feel well prepared to manage, but which few rank top. Our view, given that intangible assets are the predominant source of economic value for many businesses, is that this is a blind spot that requires more forceful remediation.

Next steps

This report is packed with information on businesses' concerns about technology risks and on their perceived levels of resilience. We hope it will help open the door to useful conversations about how different risks manifest in different sectors and what we can do, as an industry, to anticipate and manage them better.

Please contact us if you want to start a conversation and find out more.



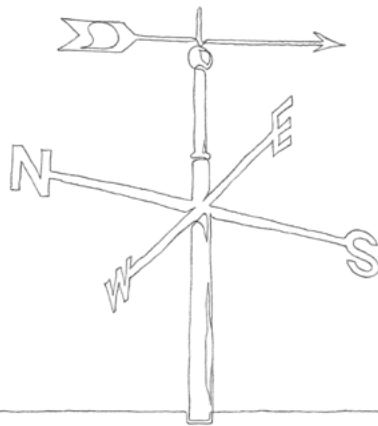
Paul Bantick
Global Head of Cyber and Technology
paul@beazley.com



Raf Sanchez
Global Head of Cyber Services
raf@beazley.com

If you are Beazley policyholder please visit www.beazleybreachsolutions.com for cyber and technology risk management information.

Contents



Why do technology risks come out on top?

As the pandemic took hold, businesses that could operate remotely were forced to adapt to new ways of operating – to comply with lockdown restrictions, and allow isolating staff to continue to work and to respond to changing customer needs. Overnight, companies had to quickly adapt existing business models to accommodate new requirements to deliver services, manage staff, provide benefits and interact with customers remotely. They were also more exposed to a greater threat of disruption by competitor organisations that were more agile and perhaps had already implemented activity-based working, permitting remote users to contribute in a hybrid environment. Many also inadvertently found they had opened the door to cyber criminals who moved fast to exploit staff, processes and networks that were suddenly exposed beyond the corporate firewall.

When we delve into the various risks within the wider technology risk category, cyber risk tops the table in terms of US-UK combined data, with 34% of respondents ranking it their top risk. However, when we disaggregate the responses, it becomes clear that US leaders are more concerned about cyber risks than their UK counterparts, who are more stressed by disruption risks – such as the failure to innovate, and keep pace with new developments, customer demand or market shifts.

Why are there regional discrepancies?

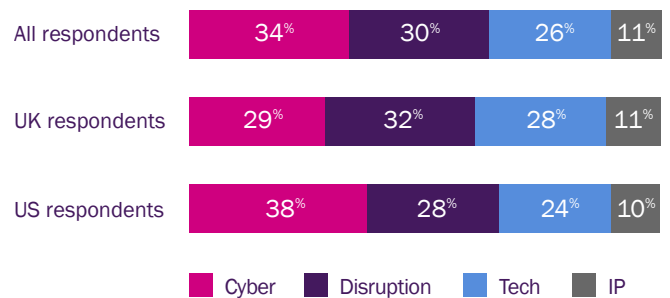
This regional discrepancy may reflect some key factors. First: longer standing concerns about the reputational and financial impacts of data breaches in the US market. Many of the most high-profile cyberattacks have been on large American companies with many millions of users or customers such as Twitter, Microsoft and Marriott, meaning cybercrime is given loud and regular media coverage. This makes the threat appear much more immediate than elsewhere. In the UK, as in the rest of the world, the risk is growing, with threat actors now increasingly using automation to scale up their attacks cheaply and enabling them to set their sights on new targets in the UK, Europe and Asia.

The second factor underpinning these statistics, and in particular the greater concern among UK business leaders regarding disruption, may simply be the relative lack of innovation in the UK compared to the US. While the US ranks second in terms of the world's most innovative countries, the UK fails to make the top ten¹. US businesses are more likely to have transformed their businesses through the use of innovative technologies like cloud computing, machine learning and AI and therefore are more exposed to certain cyber risks than businesses in the UK and Europe.

Technology risk concerns?

Overall, US business leaders feel better prepared to anticipate and respond to the risks within our technology risk category than their UK counterparts.

Which technology risk is most significant in 2021?



Percentage of companies ranking each technology risk top - US and UK, 2021

Technology risks

Cyber: IT-based threats affecting anything from national infrastructure to individual customer data and including data leak and system breach via hack, ransomware or employee error.

Disruption: failure to innovate, to keep pace with new developments, competitor activity, customer demand or market shifts.

Tech: failure to keep pace with changing technology developments and opportunities, for example Artificial Intelligence (AI), the Internet of Things and automation.

Intellectual property: failure to recognise and protect the value of intellectual property assets such as know-how, trade-marks, patents or other intangible assets.

¹ These are the 10 most innovative countries in the world | World Economic Forum (weforum.org)

How resilient are companies to technology risks?

In terms of individual risks, firms feel better prepared to manage cyber risk than any other risk in this category, particularly in the US where a median of 55% of businesses feel very prepared to anticipate and respond vs 34% in the UK. The insurance industry has provided solid support in terms of cyber risk management and mitigation which underpins business confidence. However, the rising frequency and value of claims points to the difficulty we all face in managing this risk effectively. The reality is that cyber criminals are well-funded and resourced, efficient and innovative, so can quickly leverage vulnerabilities for maximum gain.

Tech risk, and in particular keeping up with technological developments, is also something of a success story, but for different reasons. Managing this risk effectively is less of an insurance play, and more a question of business leaders getting the right talent on board and making good and timely investments. Consequently, a median of 44% of UK and US businesses feel very prepared for tech risk challenges.

Intellectual property (IP) and the failure to protect it and other intangible assets is the risk that business leaders worry about least in the technology risk category, with a median of only 12% ranking it their top risk. This is a concern given that intangible assets account for 75%² of business value globally and are the predominant source of economic value which needs protecting as we enter the economic headwinds of the post Covid-19 recovery and withdrawal of government support.

Disruption, and the failure to innovate in line with customer needs or competition, by contrast, is the risk to which business leaders feel least resilient, with a median of well under half (41%) of businesses feeling well prepared to anticipate and respond. As a result of changed working patterns post Covid-19, it is inevitable that businesses are likely to remain at heightened risk of disruption as skilled workers disperse out of city centre jobs and more new tech-enabled business models emerge.

Technology risk-resilience matrix, 2021

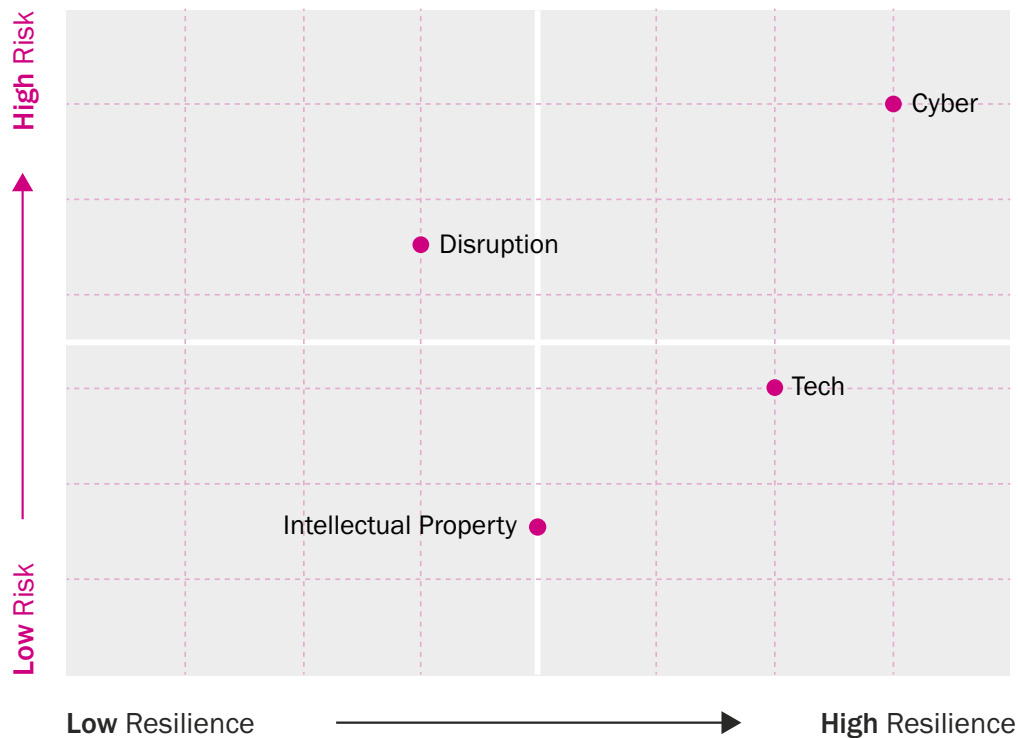


Chart scales are based on the percentage of companies ranking a selected technology risk as their leading concern and on the percentage of companies feeling 'very prepared' to anticipate and respond to the risks.

² Intangible assets make up 75% business of deal values – Burgis Bullock

Cyber: a binary issue?

Cyber threats are rising in volume and severity all round the world. As businesses of every size in every sector continue to fall foul of what is now a well-established criminal industry with attackers at every level of sophistication with varied tool-sets and motivations, our findings on cyber risk are binary: both shocking and heartening.

Shocking that according to our research, businesses see cyber as being as great a plague on business as Covid-19. Heartening that they feel well placed to anticipate and respond to the threat.

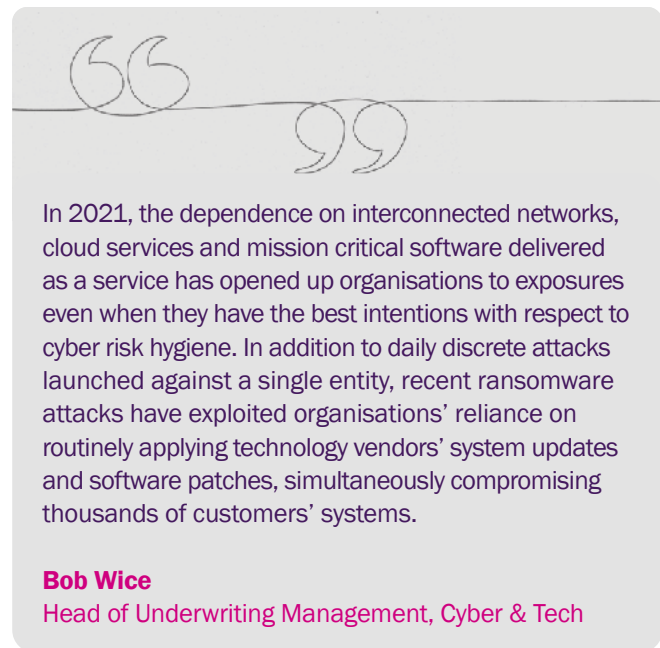
Is the risk trend our friend?

There is something of an alarming trend in cyber threats. Both the targets and the attack vectors are evolving.

Criminals' focus is shifting away from stealing customer data from retailers and healthcare providers - the dark web is awash with personal financial data and its value is diminishing. Instead, we are seeing increasing targeting via ransomware of operating systems and data belonging to economically significant industries and national infrastructure. Rather than selling personal data on, ransomware threat actors rely on companies and governments needing to buy their own data back or to reclaim autonomy over their own operations.

A more recent development over the past year has been the emergence of 'double extortion' where ransomware threat actors will blackmail their victims into paying not just to recover important data, but also to prevent the threat actor from releasing confidential company data (and even the fact that the attack has occurred) into the public domain – either for the financial gain of the threat actor or out of pure malice.

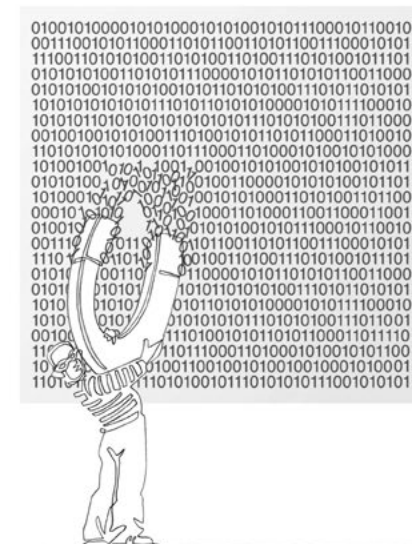
As we look ahead and consider how the world continues to grow ever more interconnected we see that where there used to be separation of systems and assets, with each company and economy operating independently of others, sharing information and data as needed; the rise of a relatively small number of global 'software as service' providers now risks exposing economies and businesses to the same threat at the same time.



In 2021, the dependence on interconnected networks, cloud services and mission critical software delivered as a service has opened up organisations to exposures even when they have the best intentions with respect to cyber risk hygiene. In addition to daily discrete attacks launched against a single entity, recent ransomware attacks have exploited organisations' reliance on routinely applying technology vendors' system updates and software patches, simultaneously compromising thousands of customers' systems.

Bob Wice
Head of Underwriting Management, Cyber & Tech

Overall, sectors which feel most exposed to cyber threats include energy and utilities, with 40% of businesses ranking this their top risk, followed by retail and technology media and telecoms (TMT), both with 38% of companies ranking this risk top.

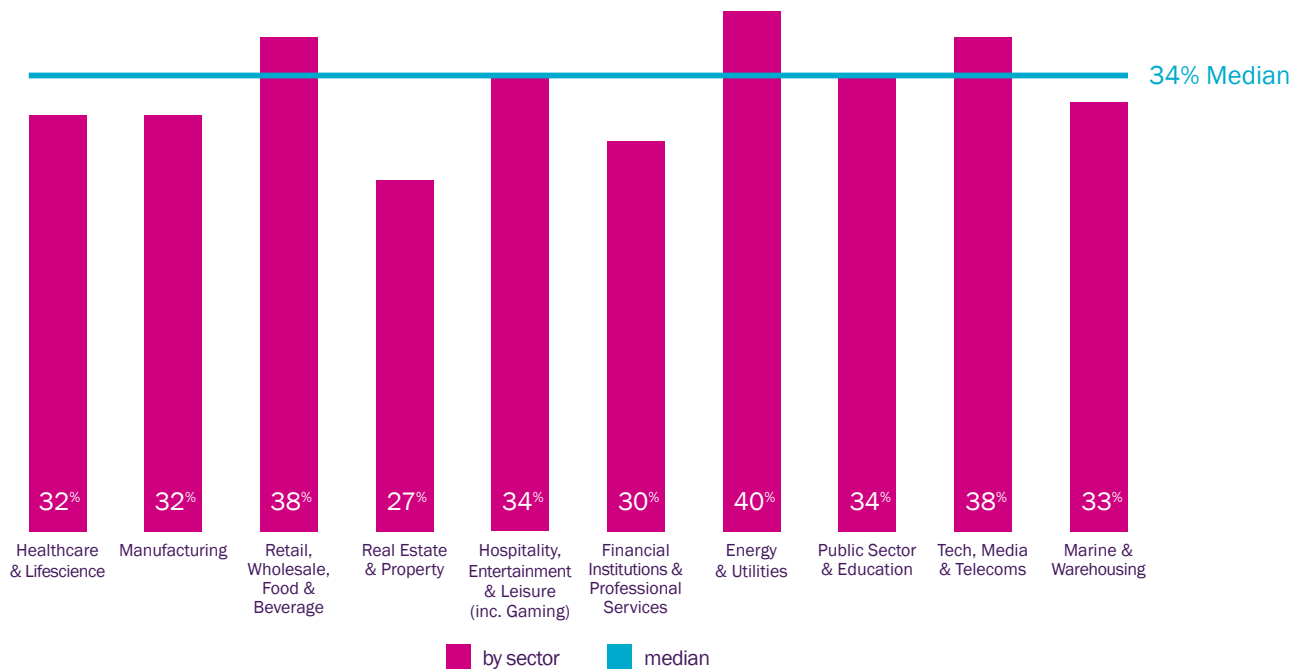


Regional and sector differences on cyber risk are striking

There is no doubt that executives in these industries are acutely aware of the risks they face. The exposure of energy and utility businesses was highlighted recently by the attack on US company Colonial Pipeline – the largest fuel pipeline business in the US - which led to fuel shortages across the East Coast of the US. While the loss of personal credit card data is troubling for retailers and consumers, failure of infrastructure is on a different scale – inhibiting economy activity and inviting civil unrest.

Shifting attack modes may explain why 53% of US energy and utility businesses rank cyber their top risk, compared with only 27% in the UK. There is a similar large discrepancy in TMT, with 50% of US businesses ranking cyber top versus just 22% in the UK.

Sector view on cyber risk



Percentage of UK and US companies ranking cyber risk top, 2021. Median line indicates the mid-point of the data set across all industries surveyed.

Experience breeds cyber resilience in retail and financial services

Despite the worsening risk picture, businesses' sense of confidence around cyber risk is notable – it is the technology threat to which businesses feel most resilient, even as attacks seem to increase in number and sophistication. As more companies rely increasingly on digital trading, so there may be a perceived safety in numbers (it won't happen to me) and high levels of confidence that security measures are effective. Time will tell if such high levels of confidence are well placed, but for the moment at least there is almost a sense that if businesses survived 2020, they can survive anything.

Industries that have the longest history of dealing with the cyber threat and associated regulatory oversight have clearly learned from hard-won experience and tend to place greater confidence in their ability to mitigate and manage the risk than others. Retail, for example, is an industry which has been in cyber criminals' sights for many years, with famous attacks on Target dating back to 2013 and TK Maxx even further to 2007. For retailers and financial services firms, a combination of experience, regulatory intervention and the threat of hefty penalties has served to ensure risk management is robust.

The road ahead

In the US, almost two thirds (65%) of retail leaders and over two thirds (69%) of financial and professional services leaders feel very prepared to anticipate and respond to cyber risk. In the UK, where data privacy regulation has been in place for a shorter period of time, these industries are notably less confident. Less than a third (28%) of financial and professional service leaders and only 32% of retail leaders feel very prepared to manage cyber risk in the UK.

Lack of funding undermines cyber confidence

Overall, sectors which are far less resilient to cyber risk include public sector and education, hospitality, and marine and warehousing. This suggests that lower budgets in the case of public entities, and wafer-thin margins for private entities in these sectors, mean they simply do not have the funding to invest in adequate cyber risk protection, even if this is as basic as regular staff training and essential software upgrades – which remain some of the most common way threat actors gain access to company systems. Companies in these sectors can also face difficulty in attracting and retaining talented information security professionals – a situation which is of concern given the growing propensity of state actors to attack these targets. In the US, only 31% of public sector and education leaders feel well prepared to manage cyber risk – five percentage points less than in the UK. In the UK, only 29% of marine and warehousing executives feel very prepared to manage cyber risk, 18 percentage points fewer than their US counterparts.



All members of the cyber security community, including regulators, network security professionals, cyber insurers, brokers and risk managers, will need to collaborate to raise awareness and be prepared to combat the next global systemic threat.

Bob Wice
Head of Underwriting Management, Cyber & Tech

In 2020, attacks just from ransomware increased by 485% according to Bitdefender's Consumer Threat Landscape report³ and the incidence of malware rose 72%.⁴

³ Ransomware Attacks Grew by 485% in 2020 - Infosecurity Magazine (infosecurity-magazine.com)

⁴ The Rise of Ransomware in the Era of Covid-19 (simplilearn.com)

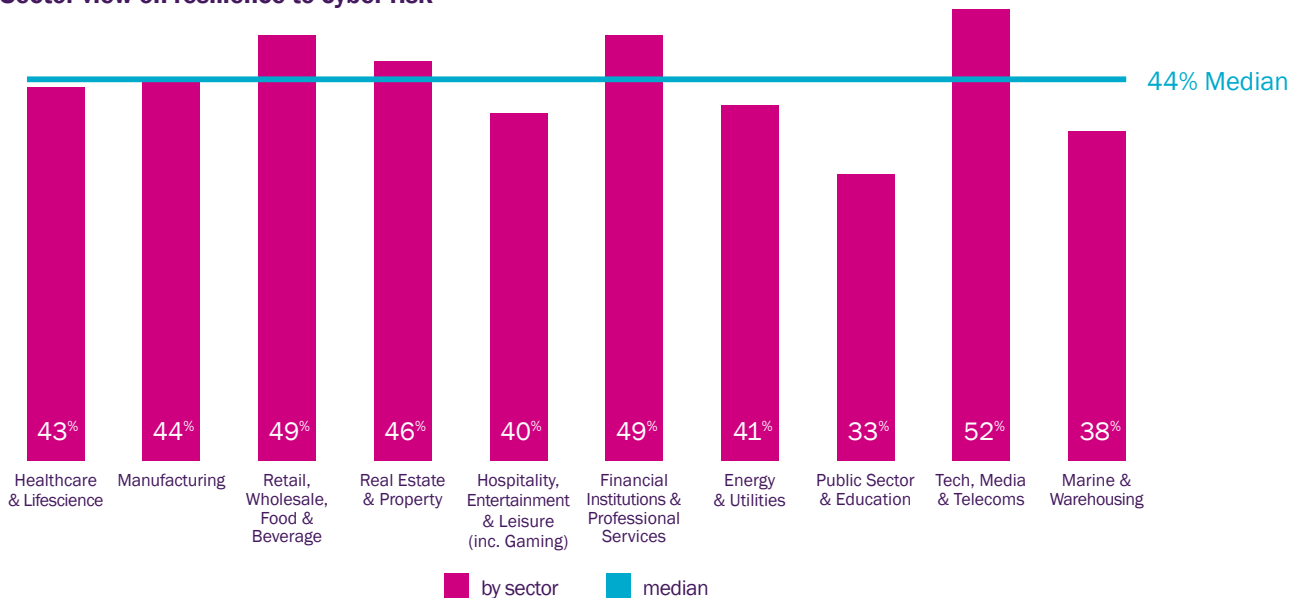


We have seen a clear increase in both the severity and complexity of ransomware events, as cybercriminals seek to maximise the value of their attacks. Increasingly, in an effort to turn up the pressure on cyberextortion demands, cybercriminals are exfiltrating data and threatening to expose the theft. With this exfiltration now occurring in approximately 80% of cyberextortion incidents, the investigation process has become lengthier and more expensive, with a deep forensic dive often necessary to ensure compliance with regulatory and notification obligations.

Moving beyond attacks on individual organisations, cybercriminals have also targeted infrastructure and supply chains. The collateral impact of such attacks is significant, particularly in attacks against technology supply chains. In March 2021, for instance, the Microsoft Hafnium vulnerability resulted in the number of incidents reported to Beazley to spike by 74% compared to the monthly average for the rest of HY 2021.

Frank Quinn
Breach Response Manager

Sector view on resilience to cyber risk



Percentage of US and UK companies feeling 'very prepared' to anticipate and respond to cyber risk in 2021. Median line indicates the mid-point of the data set across all industries surveyed.

US leaders continue to rate cyber risk and resilience more strongly than UK peers

Asked to look ahead to 2022, overall, 32% of business leaders continue to rank cyber as their top risk, two percentage points lower than in 2021, but with a far higher preponderance of US leaders ranking tech risk top. In terms of resilience to cyber, as we look ahead, overall, 44% of businesses feel very prepared to anticipate and manage the risk, but this finding is very nuanced. Just over a third (35%) of UK business leaders feel confident on cyber compared with over half (52%) in the US.

Disruption: stick or twist?

By its very nature, disruption risk – the failure to keep pace with new technological developments, competitor activity, customer demand or market shifts – challenges the status quo. These risks can hit fast or be ‘slow burn’.

Whether disruption is instant or slow burn, it can reconfigure the value chain and be difficult to recognise and respond to, particularly if businesses have extensive bureaucracy to wade through, or a poor track record of ensuring their tech firepower cannot be outgunned by others with a sharper vision or deeper pockets. Disruption risks can also materialise if businesses fail to change, even when it is clear that their strategy isn't working.

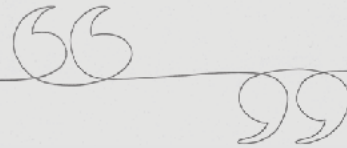
How fast can businesses respond?

So, it should be no surprise that disruption is ranked second overall in the technology category of risks behind cyber. However, it edges into the top spot for UK participants who appear to feel this risk more acutely than their US counterparts. On both sides of the Atlantic, the potential for disruptive technology to impact sectors where there is real innovative capability includes health, life science, manufacturing, financial services and real estate. Over a third (36%) of real estate companies rank disruption risk their top concern. In the US the industry which ranks disruption risk highest is healthcare and life science, in the UK this honour is won hands down by manufacturing, where 44% of business leaders rank disruption risk top.

The real dilemma for businesses is often not whether they need to change, but how fast without destabilising existing business models and revenue streams.

The impact of bricks or clicks?

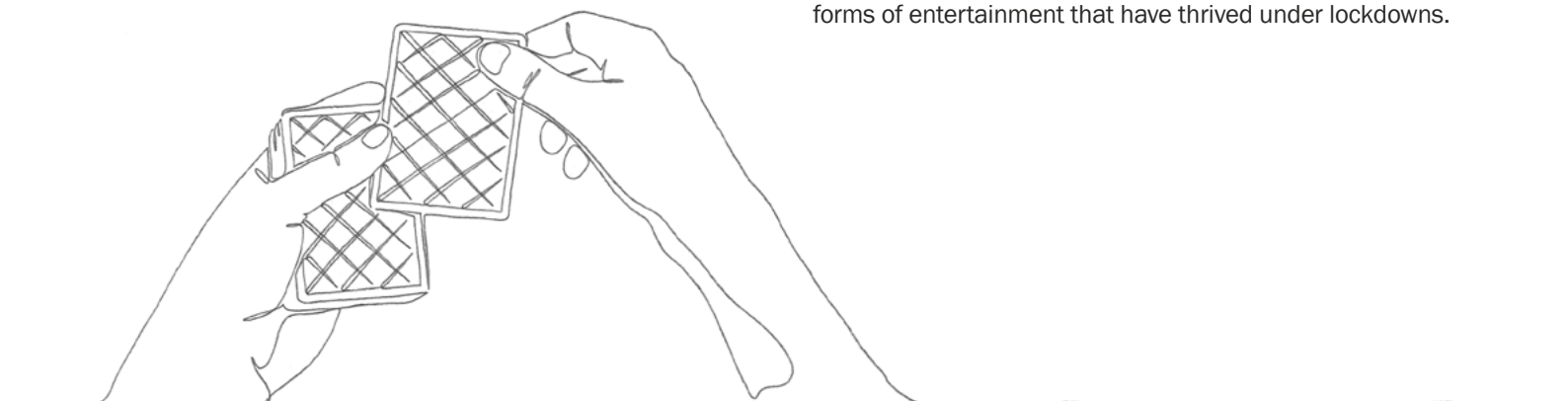
The traditional real estate model has been profoundly challenged in recent years by the advent of online sales businesses, comparison (aggregator) websites and even ‘sale by owner’ models. Manufacturing and healthcare likewise are two sectors that have been dramatically changed by the advent of new technology. While manufacturing has been transformed by automation, in healthcare we are seeing a step change in treatments based on advances in molecular biology and genomics, plus radical business model changes under the banner of digital health, telehealth and telemedicine.



Governments are keen to understand transformative technologies and to identify which have the potential to profoundly disintermediate established ways of doing business – be that 5G, low orbit satellites, CRISPR gene editing, genomics, quantum computing, AI, or machine learning. They are thinking how to hedge their economies against profound disruption plays.

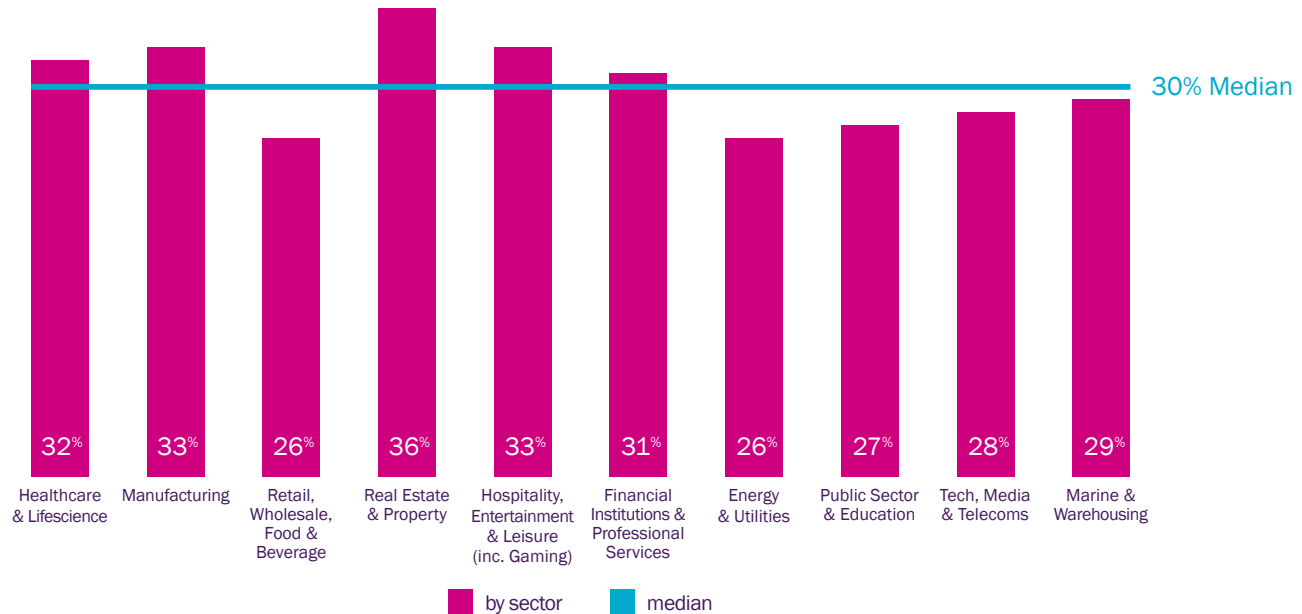
Alex Creswell, OBE
Strategic Adviser

33% of hospitality companies in the US, which traditionally have relied on physical proximity to customers also rank disruption risk top, and interestingly this view is broadly consistent in the UK where 32% do the same. It is likely that this reflects two factors – high levels of disturbance through the pandemic and the threat from alternative forms of entertainment that have thrived under lockdowns.



Spotlight on technology risk

Sector view on disruption risk



Percentage of US and UK companies ranking disruption risk top, 2021. Median line indicates the mid-point of the data set across all industries surveyed.

TMT needs a closer look

We are surprised that technology, media and telecoms (TMT) executives do not rate the threat of disruption more highly, particularly in the US, where only 19% rank it top compared with 38% in the UK.

This significant difference may reflect the broad spread of businesses within this category and their representation within our sample data, or the difficulty in anticipating the risks of disruptive technologies, business model, and external market factors. While media companies may feel less exposed to disruption, for example, telecoms businesses are at undoubted high risk both due to the rollout of new technology (5G) and uncertainty over key players.

“

”

Political rhetoric on both sides of the Atlantic indicates that governments will be more proactive in defending critical national infrastructure – including the commercial elements of this such as 5G mobile internet infrastructure. It is still unclear which companies will dominate provision of 5G. It is possible that large internet companies such as Facebook and Amazon will build dominant roles as 5G carriers.

Alex Creswell, OBE
Strategic Adviser

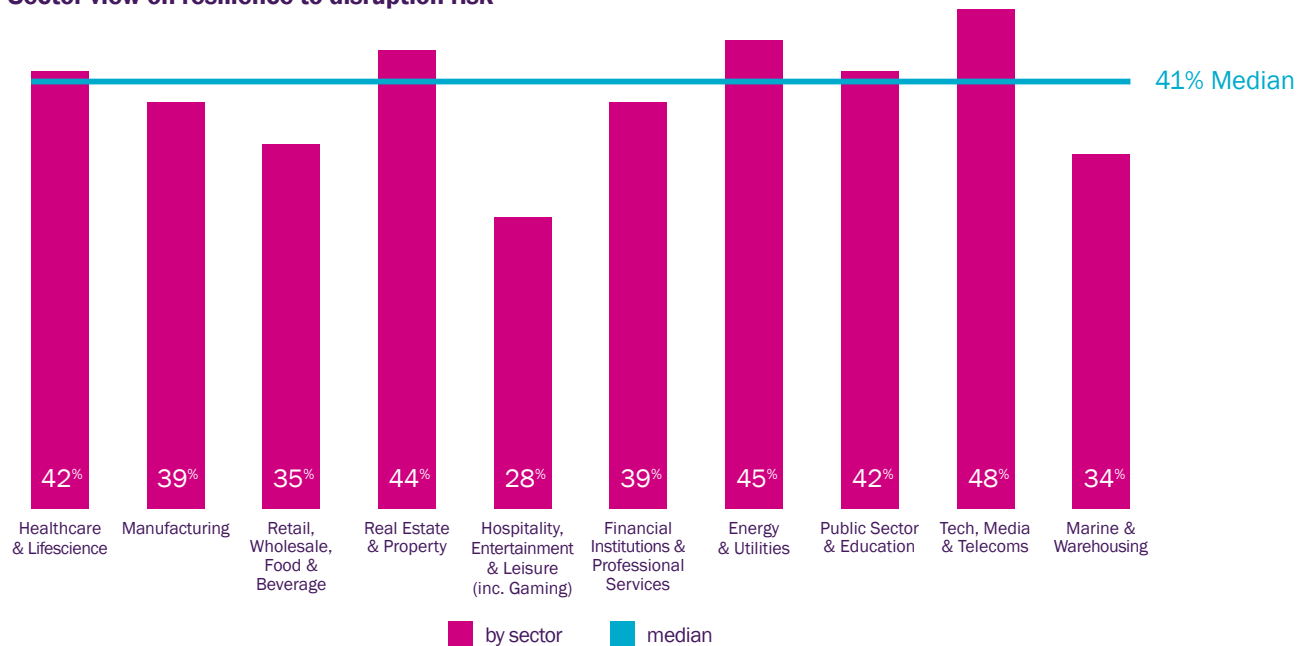
A sense of resilience in regulated sectors

Real estate is clearly a sector where business leaders feel they have weathered the storm and are now well positioned for growth post-pandemic. 44% of real estate leaders across the US and UK feel 'very prepared' to anticipate and respond to disruption risk, with comfort levels 12 percentage points higher than in the UK.

Another sector where executives feel more resilient to this risk is energy and utilities, where businesses have become adept at dealing with disruption more generally – for example from new energy sources, new producers, new models of distribution and not least from the regulators. Business leaders in the UK are notably positive in this regard – 51% feeling 'very prepared' to manage disruption compared to 39% in the US.

In general, highly regulated businesses have to be good at risk management, which may also help explain the relatively strong resilience scores by TMT, financial and professional services firms and from public sector and education.

Sector view on resilience to disruption risk



Percentage of US and UK companies feeling 'very prepared' to anticipate and respond to disruption risk in 2021. Median line indicates the mid-point of the data set across all industries surveyed.

Disruption risk set to stay second fiddle to cyber

When asked to look ahead to 2022, business leaders continue to rank disruption risk as the second most significant risk in the technology category. Overall, 29% of business leaders ranked it as their top risk in 12 months' time, a single percentage point lower than in 2021.

Tech risk: the gateway to disruption?

In many ways, the risk of failure to keep up with technological developments and opportunities, and disruption risk are two sides of the same coin. Failure to invest and to keep up with the competition paves the way for disruption by others who are nimbler, smarter and have business models that are more fit for purpose.

Financial institutions and professional services firms are more likely to rank what we have termed 'tech risk' higher than any other sector. In the US in particular, 37% of companies in this sector rank this risk their top risk – a much higher proportion than any other industry. In the UK, it is marine and warehousing that has the highest proportion (31%) that ranks tech risk top.

Why are financial institutions particularly exposed?

Financial institutions face risk from misalignment between business and IT strategies, management decisions that increase the cost and complexity of the IT environment, and insufficient or mismatched talent. What's more, mergers and acquisitions can hopelessly complicate the organisation's IT environment, something that many management teams often fail to anticipate. Meanwhile, technology-driven start-ups and disruptive financial technology ("FinTech") solutions are challenging the business models and processes at the core of many institutions, suggesting that technology risk holds strategic, financial, operational, regulatory, and reputational implications for the sector.

Marine and warehousing is similarly challenged – technology may become obsolete, disrupted, or uncompetitive, with legacy systems hindering agility – even as the pressures on supply chain management and rapid delivery have been exposed and exacerbated by the pandemic. UK companies may highlight this risk specifically because Brexit has placed even greater pressure on IT and documentation systems.

“

”

Legal and regulatory risk is inherent to investing in potentially disruptive technology research, development, and products.

Kenneth K. Suh

Focus Group Leader – Cyber & Technology Claim

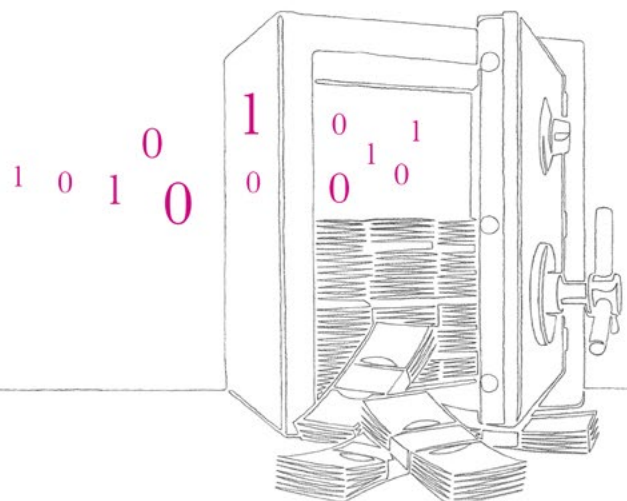
“

”

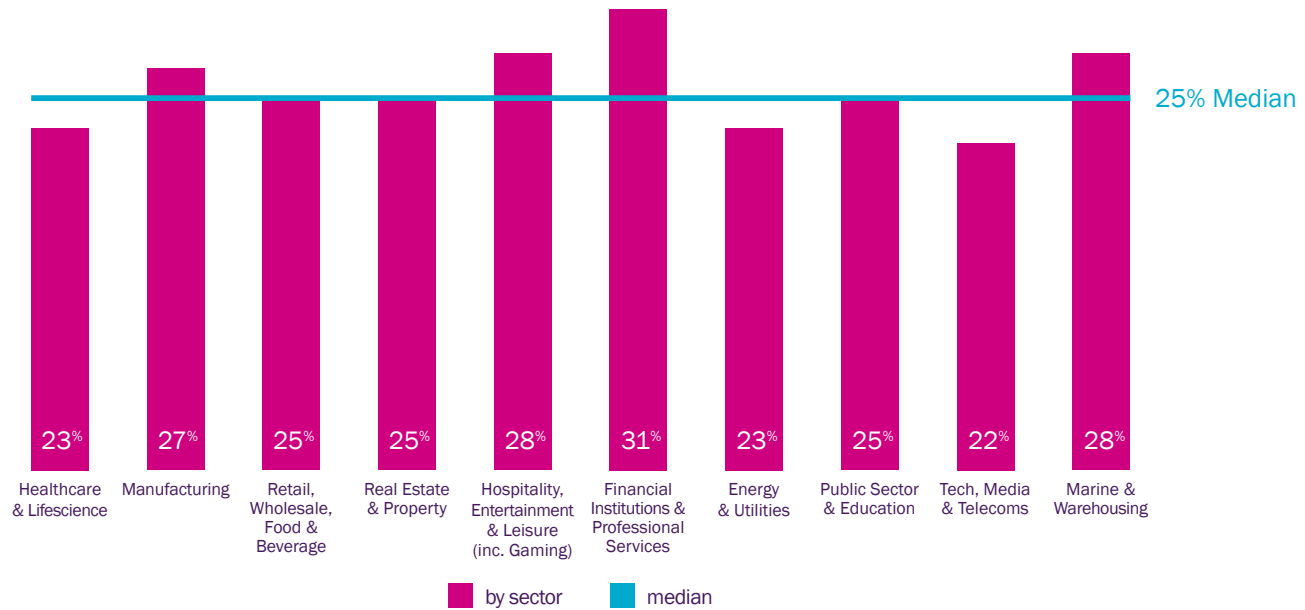
Insurance is one industry that has yet to be massively disrupted by FinTech – but we can expect it to be. On the cyber front, you could imagine that Cloud providers with a good understanding of the data flows of their customers would be in a good position to enrich the data analytics around cyber security.

Alex Creswell, OBE

Strategic Adviser



Sector view on tech risk



Percentage of US and UK companies ranking disruption risk top, 2021. Median line indicates the mid-point of the data set across all industries surveyed.

Tech risk resilience is variable

In terms of resilience to the risk of failure to keep pace with technology, financial institutions feel well prepared to face the threat. Some 56% of US businesses feel very prepared for this risk, contrasting with only 37% in the UK. Real estate is a solid 50% feeling very prepared in both territories. In the US fully 60% of technology, media and telecoms businesses are confident on about their ability to deal with this risk – a much stronger showing than in the UK where just over a third (36%) feel equally bullish – in part reflecting a broader pattern of greater conservatism in UK vs US responses.

66

99

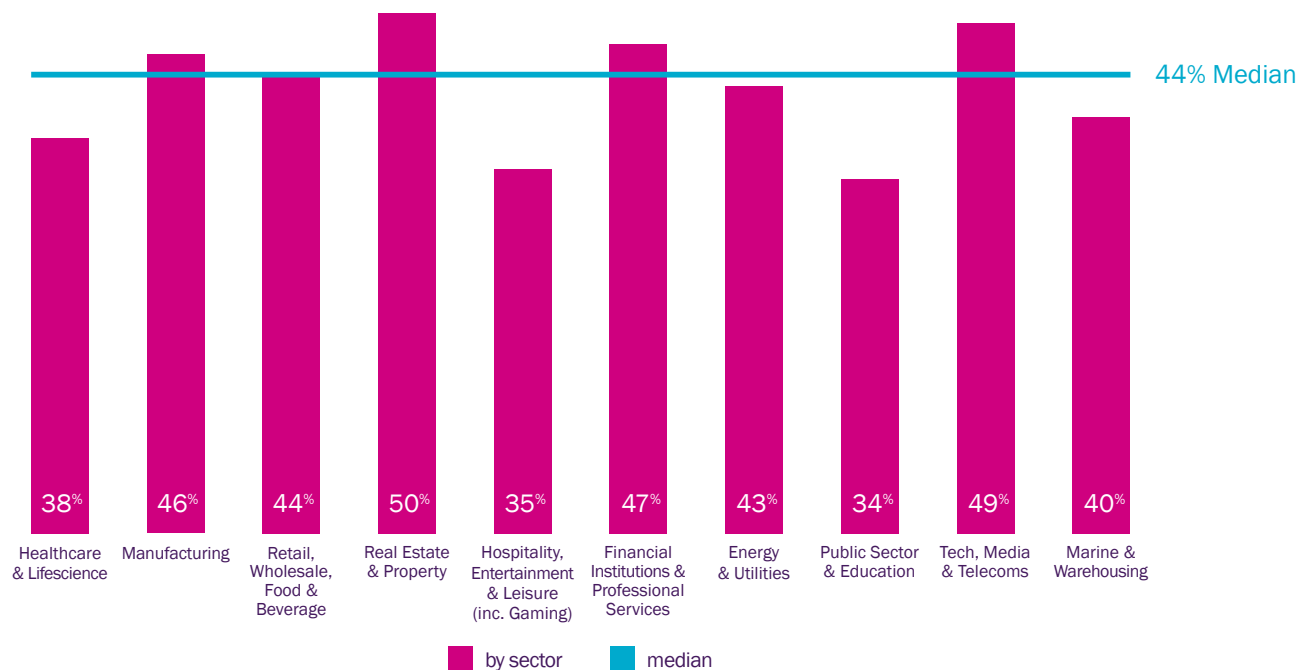
In large part, resilience to tech risk is bolstered through recognition that it takes money and talent to identify disruption before it happens so organisations are not left behind.

Bob Wice

Head of Underwriting Management, Cyber & Tech

Spotlight on technology risk

Sector view on resilience to tech risk



Percentage of US and UK companies feeling 'very prepared' to anticipate and respond to tech risk in 2021. Median line indicates the mid-point of the data set across all industries surveyed.

Money and talent underpin resilience

In both markets, those with lowest levels of confidence include public sector and education (30% in the UK feel very prepared to manage this risk, rising to 39% in the US) and hospitality (32% in the UK and 37% in the US).

Public sector and education may be long on talent but are generally poorly-funded compared to the private sector – particularly financial services and technology media and telecoms which have thrived through the pandemic and report relatively high levels of resilience. This may explain the substantial lag for public sector and educational institutions.

Shipping and warehousing firms likewise may lack the essential financial firepower to combat this risk. They operate on thin margins, yet their future relies on technology – including, robotics, RFID (radio frequency identification) and IOT (internet of things) for the efficient movement and tracing of goods in transit.

Healthcare and life science executives' relative lack of confidence in their resilience to this risk may simply reflect the harsh reality that this is a sector which is transforming at warp speed. No matter how good the cashflow or how bright the PhDs, there is no guarantee that someone else won't beat you to the punch.

Tech risk set to increase slightly

As we look ahead to 2022, tech risk, as we class it, becomes marginally more significant – ranked top by 27% of business leaders overall rather than 26% in 2021 as US businesses in particular become slightly more concerned.

IP: a business blind spot?

Of all the risks in the technology risk category, the failure to recognise and protect the value of intellectual property assets such as technological know-how, trade-marks, patents or other intangible assets (IP risk) is ranked the lowest, with a median of just 12% of business leaders rating it their top risk.

But while IP risk may be less concerning to executives than say cyber, for example, we are nevertheless experiencing a significant uptick in enquiries regarding this exposure.

Why are IP enquiries increasing?

IP is the life blood of businesses that rely on their unique ideas, insight, technology and designs to deliver services and create goods, and it is what gives many firms their competitive advantage. However, in the modern, global, economy, any business that utilises interconnected technology, or uses digital, social or traditional channels to promote its goods and services has an IP risk exposure, as these intangible assets can be deliberately stolen, copied and re-purposed, or used inadvertently in an inappropriate or unauthorised manner.

Sector responses are concerning

It is not surprising that hospitality and entertainment business leaders rank IP risk low (8% of business leaders rank IP their top technology risk; only 4% in the US). These sectors rely on creating experiences rather than content or assets. But we are concerned that it is not registering more strongly with manufacturers in our survey. Just 6% of UK business leaders put IP risk first, 8% in the US.

Financial services companies also appear to under-rate this risk, with 10% ranking this top in the UK, falling to 7% in the US. Companies in this sector do at least have much stronger resilience scores, however, suggesting perhaps that effective mitigation has neutralised the threat.

The lower prioritisation of IP risk may reflect a disconnect between business leaders' IP risk recognition and desire to leverage and monetise their own IP through litigation. While business leaders rank IP risk relatively lower than other technology risks, businesses are enforcing their IP rights, for example through demand letters and the courts.

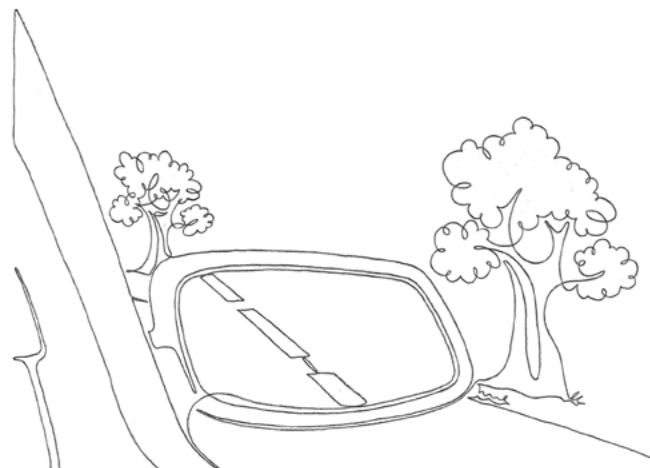
Kenneth K. Suh

Focus Group Leader – Cyber & Technology Claim

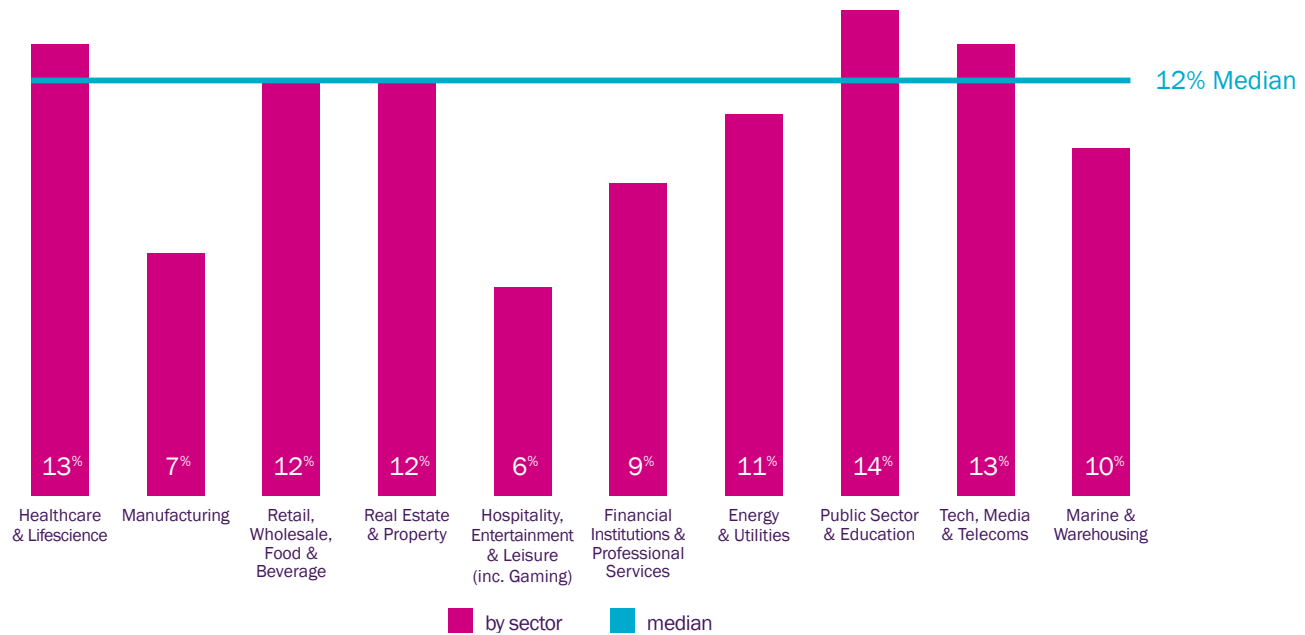
Our clients operate in a global economy, and we are seeing a rising flow of enquiries on IP risk. Any business in any sector that researches, designs, develops, manufactures, distributes or sells a product or service, faces significant exposure to IP risk, both on a first and third party basis.

Sarah Lamberg

Technology and cyber liability underwriter



Sector view on IP risk



Percentage of US and UK companies ranking IP risk top, 2021. Median line indicates the mid-point of the data set across all industries surveyed.

Resilience is variable

It is heartening to see that those with significant value at stake, for example technology, media and telecoms (TMT) companies feel 'very prepared' (38% UK, 44% US) to anticipate and respond to the risk. Financial institutions likewise show strong resilience scores with over half (57%) in the US and well over a third (39%) in the UK feeling confident. Overall, a median of 40% of companies believe they are 'very prepared' to 'anticipate and respond' to IP risk.

It is notable however that public sector and educational institutions, which exist to develop and share intellectual property, feel much less resilient, with just 30% of UK business leaders and 44% of US business leaders feeling very prepared. Although they understand the risk, unlike companies in TMT or finance, they often lack the human capital and financial resources to invest in responding to IP risks.

“

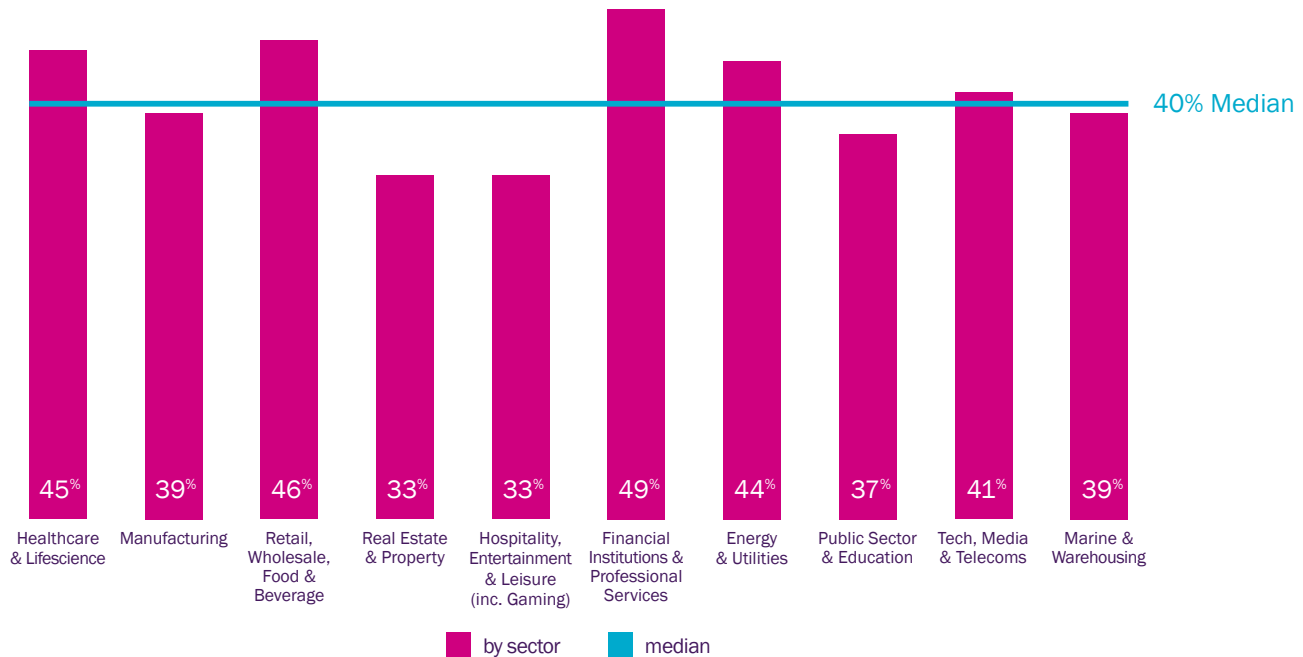
”

Companies that specialise in content and technology are in a much better position to understand IP risk – it is their core exposure. The bigger the risk, the more targeted the legal advice they receive. The less exposure companies face, like for example those in hospitality or real estate, the less they pay attention, the less resilient they are.

Sarah Lamberg

Technology & Cyber Liability Underwriter

Sector view on resilience to IP risk



Percentage of US and UK companies feeling 'very prepared' to anticipate and respond to IP risk in 2021. Median line indicates the mid-point of the data set across all industries surveyed.

IP concern set to stay low

As we look ahead to 2022, IP risk remains the least highly ranked risk in this category. There is a moderate uptick among UK business leaders, however, with 14% ranking this risk top as they look ahead compared to only 11% in 2021.

Growth in recognition of the significance of this risk is timely when we consider that intangible assets account for 75% of business value globally⁵, and are the predominant source of economic value for many businesses large and small. Although businesses may think that a patent is sufficient protection for intellectual property, the sad reality is that a patent is only effective if a business has the means (often only accessible via an insurance policy) to enforce and defend it in court. In the recession which followed 2008–2009's financial crisis, there was a boom in patent infringement filings as companies sought to protect value in their business. We may expect the same as economies rebuild post Covid-19.

⁵ Intangible assets make up 75% business of deal values – Burgis Bullock

About our Risk & Resilience research

During January and February 2021 we commissioned research company Opinion Matters to survey the opinions of over 1,000 business leaders and insurance buyers of businesses based in the UK and US with international operations. 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 & leisure (including gaming)
- Financial institutions & professional services
- Energy and utilities (including mining)
- Public sector & education
- Tech, media & telecoms
- Marine & warehousing.

Survey participants were asked about their views on insurers and insurance, as well as on four categories of risk:

- **Technology** – including the threat of disruption, failure to keep pace with changing technology, cyber risk and intellectual property risk.
- **Business** – including supply chain instability, business interruption, boardroom risk, crime, reputational and employer risk.
- **Political & economic** – including strikes and civil disruption, changes in legislation and regulation (including ESG), economic uncertainty and war & terror.
- **Environmental** – including climate change and associated catastrophic risks, environmental damage, pandemic risk, food insecurity and energy transition risk.

Of the firms surveyed in both the US and the UK there was an equal split of respondents across company sizes of: \$250,000 - \$1 million, \$1,000,001 - \$10 million, \$10,000,001 - \$100million, \$100,000,001 - \$1 billion, more than \$1 billion.

Our panel of contributors

We would like to thank our panel of insurance and risk management experts whose insight about our quantitative research has informed our findings throughout this report.



Bob Wice
Head of Underwriting
Management, Cyber & Tech



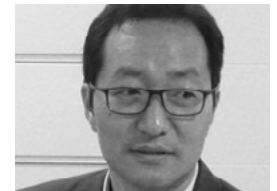
Frank Quinn
Beazley Breach Response
Manager Claims



Sarah Lamberg
Technology & Cyber Liability
Underwriter



Alex Creswell, OBE
Strategic Adviser



Kenneth K. Suh
Focus Group Leader –
Cyber & Technology Claims

Beazley Group

22 Bishopsgate
London EC2N 4BQ

T +44 (0)20 7667 0623

info@beazley.com
www.beazley.com

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.

For more information, visit www.beazley.com

© 2021 Beazley Group

This is the third in our series of Risk & Resilience reports, which explore business leaders attitudes to risk and their perceived resilience to these risks both now and in 12 months' time. To view our other Risk & Resilience reports please visit: www.beazley.com/risk-resilience

The Beazley logo is rendered in a white, elegant, serif typeface. The letters are closely spaced, and the 'y' has a distinctive, flowing tail that extends downwards. The logo is positioned at the bottom left of the page, above a thin white horizontal line that spans the width of the page.