beazley

Spotlight On Cyber & Technology Risk 2023

Executive Summary

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 business leaders could be being lulled into a false sense of security when it comes to cyber risk as it is dropping down their radar, despite saying they feel less resilient to this risk.

The next few years will reshape risk mitigation as businesses grapple with a fast changing cyber and tech world. Technological developments, such as the rise of generative artificial intelligence (AI), that have been promised or threatened for years, are now a reality and evolving at an extraordinary pace. For today's business leaders, this presents a number of potentially transformative opportunities. But they also create new and unfamiliar risks. These risks may alter business decision-making for decades to come.

Our annual Risk & Resilience survey of global business leaders found that concern about the threat of cyber risk has decreased since the "ransomware pandemic" in 2021 and 2022. However, the perception that the worst is over, that businesses are immune, or have at least built up a tolerance to the most extreme effects does not match the reality. Cybercrime, particularly ransomware, is a high growth industry and a lucrative business, and the barriers to entry are getting lower. The advent of new technology has also provided further opportunities for cyber criminals' growth models and, as they hone their techniques and attack methods, they are becoming increasingly sophisticated and efficient.

This Spotlight On Cyber & Technology Risk report explores how cyber risks are increasing and cybercrime groups diversifying, how technology risk is impacting different sized businesses, and why the emergence of AI and other innovations are demanding the attention of risk and security experts. The report also looks at business leader concerns around tech obsolescence, IP theft and cyber war risk, along with the role of insurance and what the industry can do to support companies as they look to protect themselves against new and evolving technological challenges.

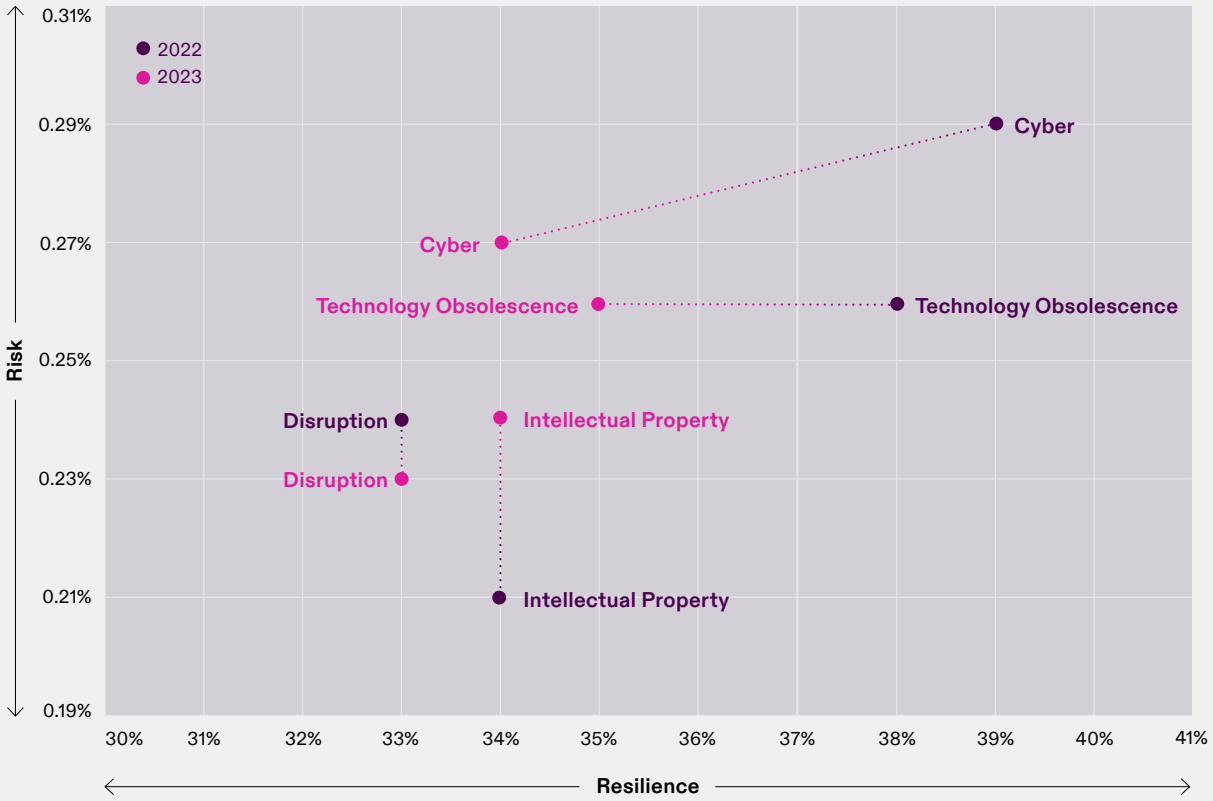
The risk landscape is constantly evolving and many businesses are finding it a struggle to keep up with the cyber threats they face. The bad actors are always thinking of, and developing, new ways to attack. To counteract this risk requires continual investment and learning. The decline in business preparedness and perception of cyber risk shows that there is a danger that the ever-present threat could be creating cyber fatigue.

For the insurance industry, working with clients to help them tackle these challenges, opportunities, and risks is vital to ensuring businesses operate in as safe an environment as possible. We need to be continually educating clients about the risks, helping them to be vigilant to the continually shifting risk landscape and demonstrate the need to continue to invest in and enforce a defence in depth risk management strategy.

Paul Bantick
Global Head, Cyber Risks, Beazley

Dulled to the danger?

Global year-on-year change of business' risk and resilience to cyber and technology issues 2022-23



These findings demonstrate a worrying 'normalising' around cyber risk concern, at a time when the stakes continue to rise as the economic impact of cyber-crime on businesses across the globe reaches new levels year on year[1]. Have security improvements really increased so much that they are now immune to the risk? Or, is cybersecurity fatigue dulling them to the danger?

[1] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Some of the key findings from our research:

27% Cite cyber as their main concern now – dropping from 34% in 2021.

74% Feel very or moderately prepared for a cyber-attack – down from 80% last year.

26% Rank tech obsolescence and the threat of new technologies such as AI as their biggest concern.

24% Rank intellectual property (IP) theft as their primary concern – in 2021 just 11% worried about this risk.

32% Plan to reconfigure their business models.

Index

AI and new technologies distract businesses as cybercrime risk begins to intensify

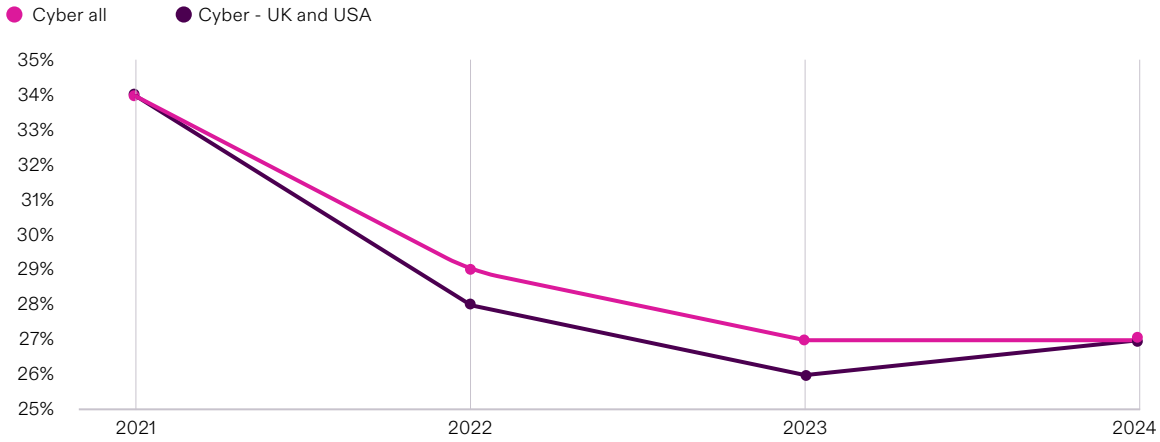
From the emergence of artificial intelligence (AI) to more sophisticated forms of ransomware, a myriad of cyber risks and challenges are now stacking up in the in-trays of executives responsible for managing these risks.

After ransomware incidents peaked in 2021-22, many may have believed, or hoped, that the worst was over - fewer high-profile hacks in the news meant that the threat was diminishing. Maintaining a constant state of vigilance is challenging and for some, the cracks are beginning to appear.

Businesses which have invested in security should take comfort that it has improved their defences. They are less exposed. However, cyber risk is evolving. Where once cyber criminals took weeks to gain access to a network, now it is often only hours.

Boardroom perception of cyber risk falls sharply from the pandemic years

Percentage of executives ranking cyber risk as their top risk now and in 12 months' time

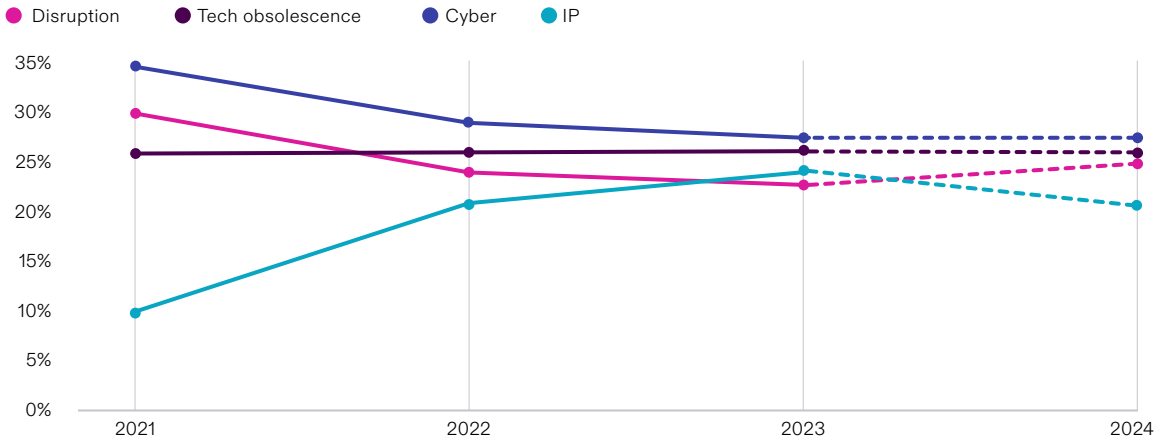


Our data shows that the perceived threat of cyber risks for global businesses has declined since 2021 and resilience has also dropped year-on-year. In 12 months' time, the perceived threat of cyber risks is predicted to remain the same. However, this is not due to increased resilience as businesses expect their ability to mitigate cyber risks to also decline.

Contrary to the perception of the cyber threat, the frequency of incidents, the disruption they cause and the economic cost are increasing. Research from CyberSecurity Ventures has shown the global annual cost of cybercrime is predicted to reach US$8 trillion in 2023, and US$10.5 trillion by 2025[2] – up from US$3 trillion in 2015 when the study began.

Technology and cyber risks impact firms in equal measure

Percentage of executives ranking cyber and technology risks their top concern now (2021-23) and in 12 months' time



The frequency and severity of cyber risks has fallen as the Ukraine-Russia conflict split cyber gangs. However, this isn't a new normal and the situation is becoming uglier by the day as new threat actors emerge and look to make up lost profits. Cyber protection cannot be a blind spot for businesses in 2023.

Meghan Hannes
Head of US Cyber
& Tech Underwriting
Management, Beazley

[2] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

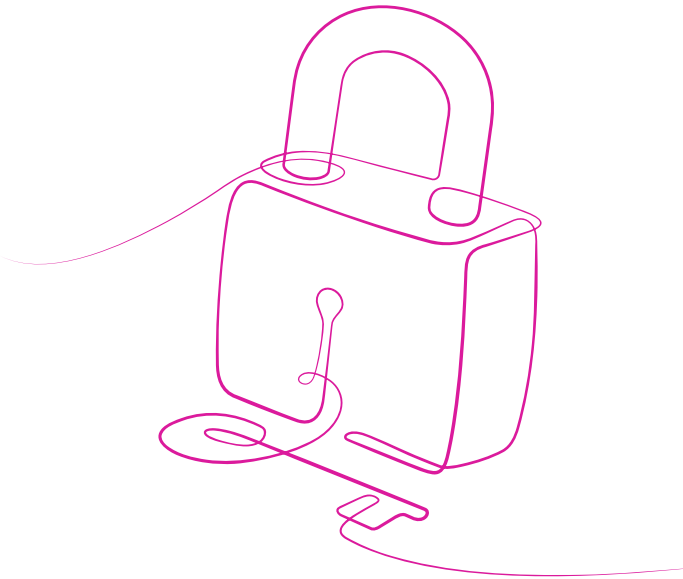
Why is there a mismatch between the view of cyber risks and reality of the current threat?

The cyber risk landscape is not static and new avenues of attack for cyber criminals are emerging. The innovations that AI and machine learning will bring to the global economy are now front of mind for business leaders. However, whilst AI's transformative potential is undeniable, it brings a new set of cyber challenges, potentially enabling threat actors to operate at a greater scale or offer novice cyber criminals easy access to sophisticated code targeted at specific organisations. NATO leaders[3] have warned that AI is a 'double edged sword' for private companies with AI-based tools able to automatically carry out attacks.

Elsewhere, the ransomware threat remains significant. Our recent **Cyber Services Snapshot Report** highlighted that phishing and software vulnerability ransomware incidents are on the rise. In 2020, data across all industries showed that, on average, 7% of company losses were caused by fraudulent instruction, whereas in the first quarter of this year, this average had risen to 13%.

Further research from Sophos shows that the average ransomware payment has nearly doubled to US$1.5m (£1.2m)[4] over the past year. As companies develop ever more complex IT infrastructures, their reliance on third party systems that process company data leaves them vulnerable as they are potentially unknowingly bringing risk into their network, as recently demonstrated by the MOVEit hack[5].

The cloud of Russia's invasion of Ukraine in 2022 continues to hang over the cyber world. A number of prominent cyber gangs split over their allegiances when the conflict started, this may have led to a reduction in the number of ransomware attacks, but it hasn't led to a reduction in cyber incidents. In 2022, Russian government-backed attackers[6] increased their targeting of NATO countries by over 300%. As the war continues, organisations and businesses across the globe are likely to find themselves on the frontline, both directly and indirectly.



[3] https://www.euronews.com/next/2022/12/26/ai-cyber-attacks-are-a-critical-threat-this-is-how-nato-is-countering-them
[4] https://www.theguardian.com/technology/2023/may/10/ransomware-payments-nearly-double-in-one-year
[5] https://www.bbc.co.uk/news/technology-65814104
[6] https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

Too small to matter?

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

Small and medium sized businesses (SMEs) have often, wrongly, believed that they are not targets for cyber criminals. Our research suggests that this misconception may be changing, as companies with an annual revenue of US$250,000 to US$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%). If this leads to investment in security, then this is clearly welcome.

However, small businesses also believe that their cyber risk will fall in the future. They predict that 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 would seem to rely on SMEs evolving their businesses while cyber criminals' approaches remain static. Unfortunately, for businesses of all sizes, this is not the case.

Why would a cyber criminal target a small business when there are so many bigger, more lucrative targets available? Unfortunately, there is an ever-growing list of businesses which have been targeted that provide the response. Business is interconnected. Supply chains for multinationals contain businesses of all sizes across every country in the world. Where the business at the end of the chain has invested heavily in its security, cyber criminals may look for weaker points of entry across an ecosystem.

Cybercrime groups are also becoming more specialised and diversified. SMEs, which often have fewer resources and less robust IT security, are now providing a training ground for new cyber criminals to learn their trade.

> **We see different hacking techniques that are specialised to the maturity of the customer the criminals are attacking. This is particularly true for SMEs, as they have weaker security systems. Many SMEs are part of a supply chain that lead to large companies, so they can act as a gateway in a hack to more lucrative funds.**

Jon Miller
CEO and Co-Founder, Halcyon

Path of least resistance

Businesses may also be targeted due to the type or volume of data they hold rather than the revenue of the organisation. Ransomware models work on the basis of either data extortion or "shaming", or both to gain payment. Businesses which hold large volumes of personal or sensitive data become a target for these cyber criminals, irrespective of the nature of the organisation which holds it. This has been borne out in a growing proliferation of attacks against public bodies and institutions[7] which often find themselves exposed through outdated systems and less robust security.

Legislation such as GDPR in Europe and CCPA in the US, aimed at minimising the levels of data which organisations retain, provides the framework for businesses, of all sizes, to reduce their exposure by seeking to reduce the level of personal data collected which cybercrime groups could target.

The view of cyber risk exposure varies markedly across industry sectors. It has been five years since the NotPetya and WannaCry attacks had a devastating and outsized impact on healthcare providers. In the UK alone, 80 National Health Service hospitals were forced to divert patients after malware prevented clinicians from accessing medical records[8]. For healthcare and life sciences businesses the threat still looms large. The intervening period has not led these organisations to implement measures which they feel make them sufficiently secure, as this sector has the lowest level of perceived cyber risk resilience across the spectrum with just over two thirds (67%) very or moderately prepared.

Healthcare is under immense pressure and scrutiny to keep up with technological advancement. As a sector that is rich with some of the most intimate individual data, but without the cash to widely invest in modernised security infrastructure, it is concerning to see that only 32% of these businesses do not feel prepared to manage and respond to cyber risk. This is particularly notable when compared with the fact that 74% of healthcare and life science sector business leaders think cyber will be one of their top three concerns in 12 months' time.

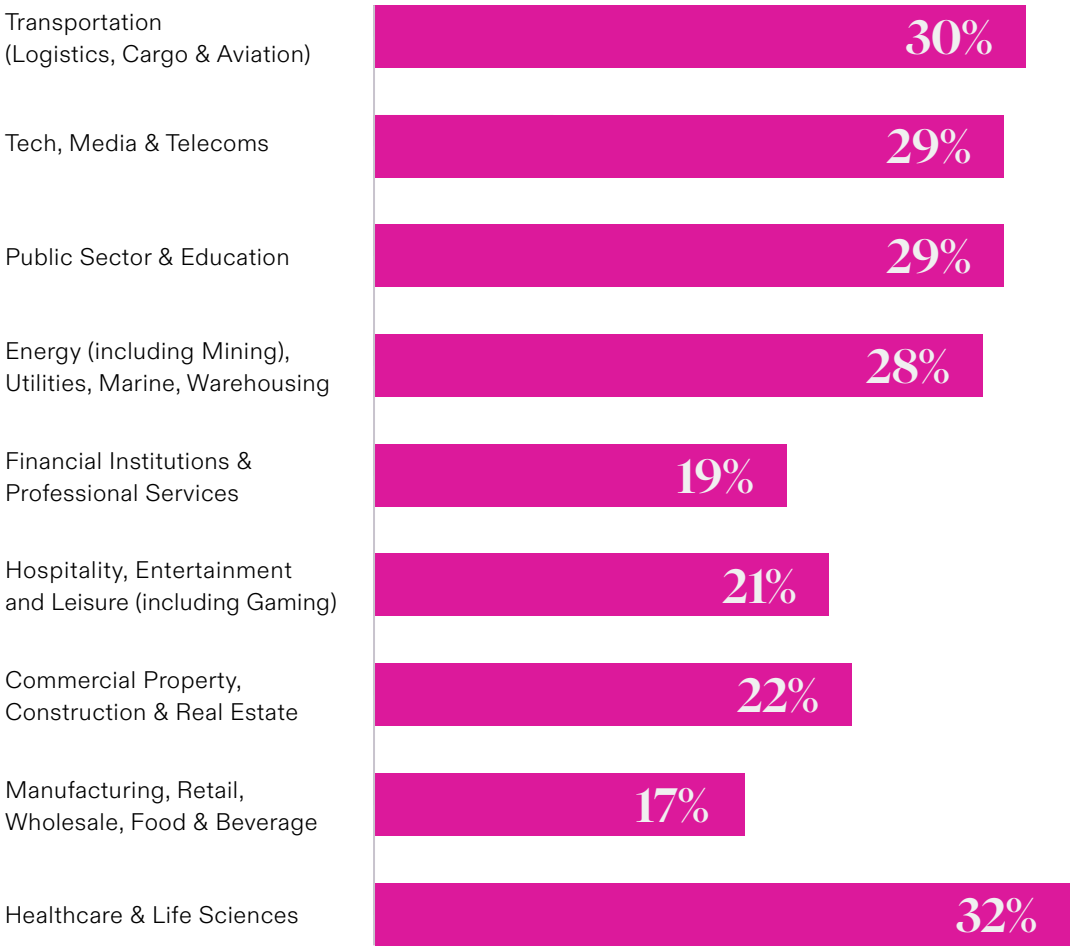
> **Hospitals hold incredibly valuable data that is costly if exposed, combined with the fact they generally have lower levels of funds to spend on cyber protection, means they're uniquely exposed to cyber-attack.**

Meghan Hannes
Head of US Cyber & Tech Underwriting Management, Beazley

[7] https://www.sentinelone.com/blog/why-governments-and-agencies-are-targeted-by-cyber-attacks-a-deep-dive-into-the-motives/
[8] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf
[9] https://newsroom.ibm.com/2022-02-23-IBM-Report-Manufacturing-Felt-Brunt-of-Cyberattacks-in-2021-as-Supply-Chain-Woes-Grew

Manufacturers' belief in the strength of their security systems may be tested

Percentage of executives feeling not prepared to anticipate and respond to cyber risks by sector



Manufacturers feel the most prepared (83%). However, manufacturers' confidence may soon be tested, as this was the second most targeted industry in 2022[9], behind only financial services.

[9] https://newsroom.ibm.com/2022-02-23-IBM-Report-Manufacturing-Felt-Brunt-of-Cyberattacks-in-2021-as-Supply-Chain-Woes-Grew

Pace of technological change is leaving businesses fearing for their future

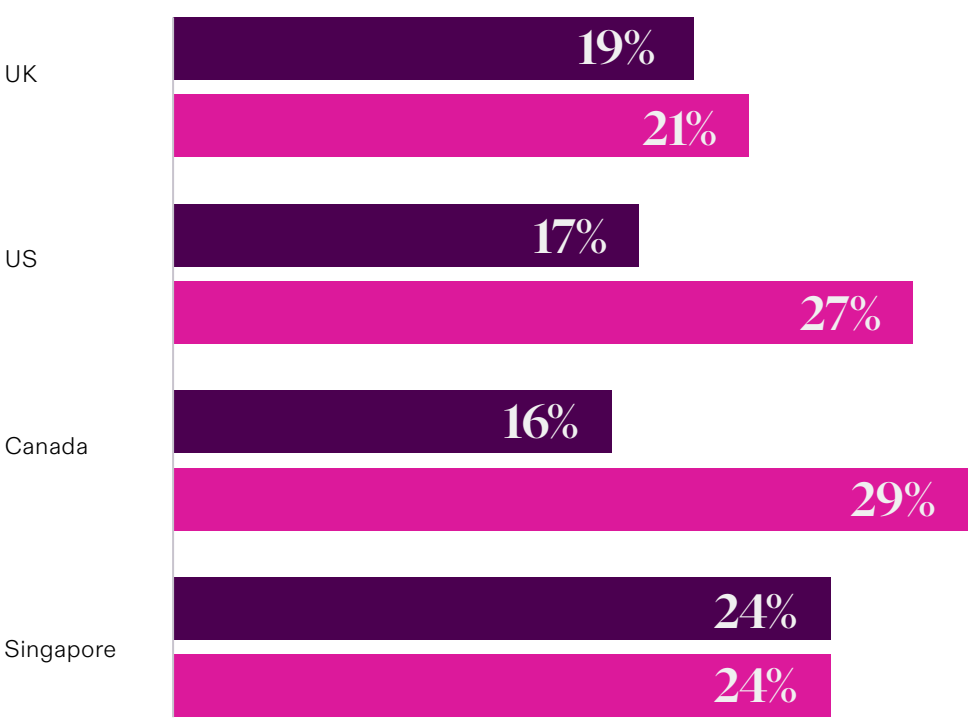
Failing to keep pace with technology and adapt to new innovations is a constant threat to businesses.

Every time we save a document we are offered a reminder of the feverish pace of technological advancement. The floppy disc icon is now the only time many of us will see this technology, which was once ubiquitous, but now seems from a different era (Sony manufactured its last disk in 2011[10]). Many reading this will understand what is meant by a "Kodak Moment", a tagline coined by the world's largest producer of photographic film throughout most of the 20th century[11]. Blockbuster Video has become a byword for a business eclipsed by a competitor which recognised how new technology would change its marketplace. The list goes on.

Technological obsolescence and the risk posed to firms has been the most consistent area of concern since our research began. In 2021, 26% of global business leaders identified it as their key technological concern, with the same again in 2022 and 2023, predicting it to remain unchanged next year. But being aware does not equate to being prepared. Resilience is dropping. More than a fifth (21%) of all businesses now feel they cannot maintain the pace for the next 12 months and nearly a third (32%) plan to reconfigure their business models.

US and Canadian businesses flagging in tech marathon

Percentage of executives that feel 'not well prepared' or 'not at all prepared' against the risk of tech obsolescence, by country



[10] https://www.wired.com/2010/04/sony-announces-the-death-of-the-floppy-disk/
[11] https://www.cam.ac.uk/research/news/the-rise-and-fall-of-kodaks-moment

The fact that businesses feel ill-equipped and plan to make wholesale changes is understandable when considering the events of the past year. The coming of age of generative AI has, or will, change the game for every industry.

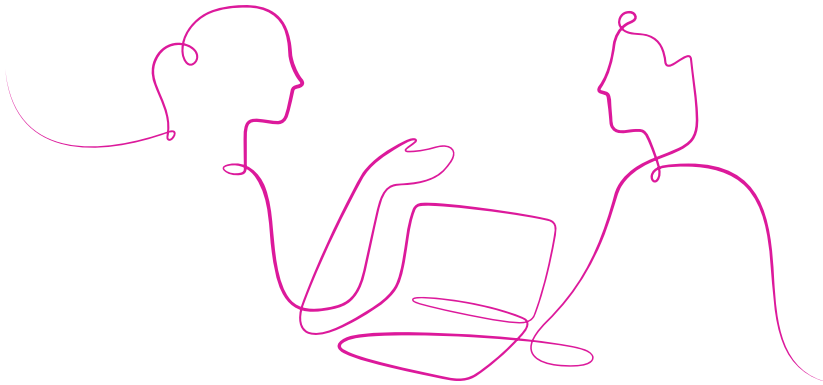
The visible potential today is just the tip of the iceberg. The benefits and impact of AI tools like ChatGPT on industries has only begun to occur, heralding generational job role and industry sector shifts. The need for businesses to react with speed to the advent of new technologies has also increased. Within a week of the ChatGPT launch, one million people had used it; within two months, the number soared to 100 million[12]. When a breakthrough occurs, it reaches a global audience almost instantly. Shareholders, consumers and stakeholders expect businesses to have an answer as to how they are implementing this new innovation, they also expect them to be managing the risks.

While AI has generated excitement, it has also seen ominous projections of job losses, whole industries becoming contracted or obsolete and concern over how it could be used maliciously. Whether there is validity in the more extreme predictions remains to be seen and the impact of AI on business will not happen overnight. What is clear is that obsolete technology poses a risk to business. Whether this is to their market share or their security, failing to keep pace has negative consequences.

Tech obsolescence fears peak among US SMEs

Smaller businesses that lack the resources to maintain the relentless momentum feel the most exposed to tech obsolescence with nearly three in ten (29%) of the businesses surveyed with an annual revenue under US$1m feeling unprepared for the risk of their technology becoming outdated. SMEs in the US earlier this year felt the least prepared with 38% citing that they are ill-equipped to maintain their technology and systems in line with new developments.

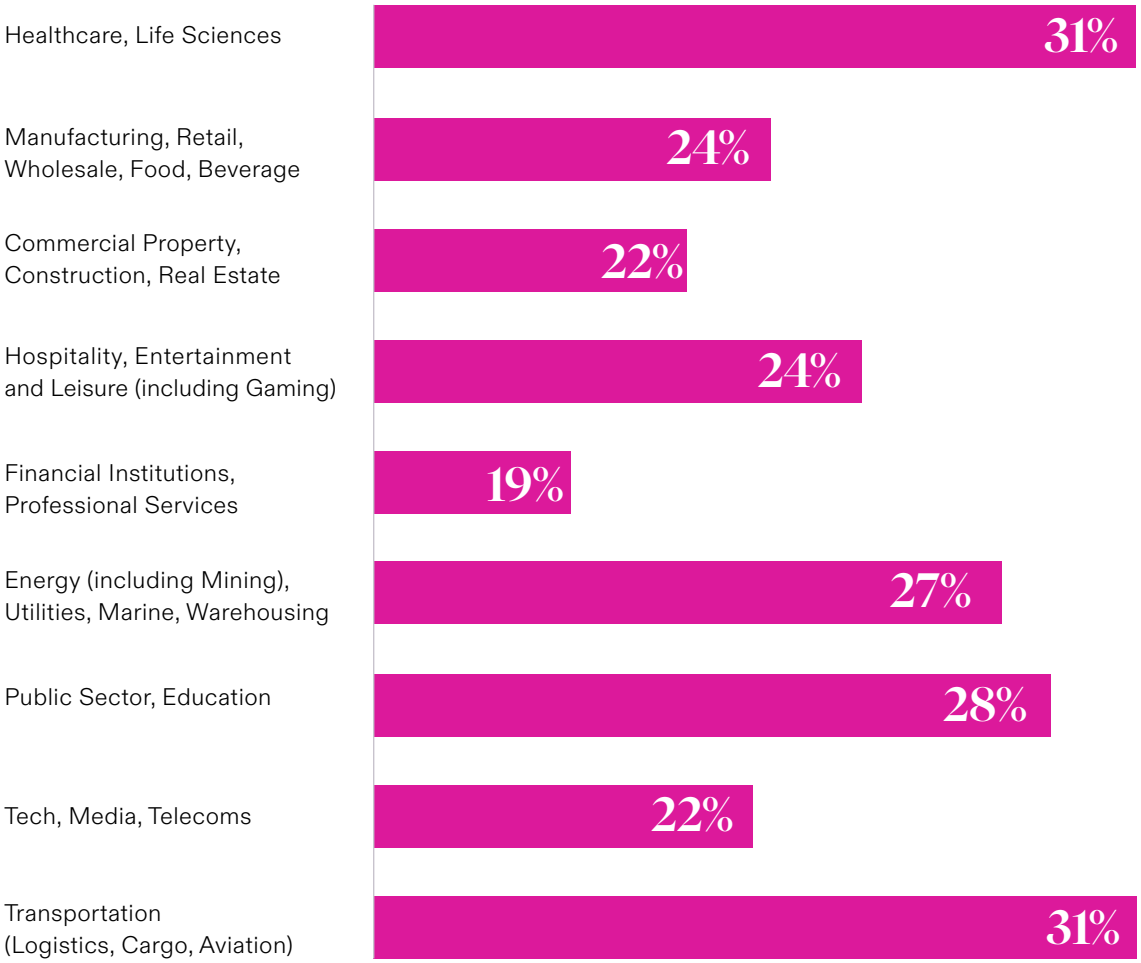
The advent of AI represents the latest peak in technological advancement and businesses everywhere are scrambling to understand how they can benefit and where they may be at risk. However, for the moment, ensuring that they are keeping up with the more mundane patches and upgrades to existing systems is proving challenging for some businesses. Where they land on the list of companies that got tripped up by failing to move with the technological times will depend on their ability to recognise threats and embrace innovation which supports their business models. While AI may be a risk tomorrow, maintaining routine security by ensuring systems are updated continues to be a risk today.



[12] https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/

Health and transportation tech leading the sectors feeling most exposed

Percentage of all executives that feel 'not well prepared' or 'not at all prepared' against the risk of tech obsolescence by sector



Smaller businesses are much more likely to have limited resources and are therefore less likely to spend capital upgrading legacy computer systems and modernising their tech stack. This is similarly true for many business sectors, where data-rich but cash-weak companies lack modern digital infrastructure – creating the perfect recipe for cyber and tech obsolescence vulnerability.

Katherine Heaton
Focus Group Leader,
Cyber Services and
InfoSec Claims, Beazley

Intellectual property risks mount for business

Since 2021, risks related to intellectual property (IP) have gone from a peripheral business challenge to a key focus for boardrooms.

Executives have become increasingly aware of the need to protect their assets and knowhow. From stealing code to copycat designs, the threat of IP theft is becoming more apparent. Even at a micro-level, businesses have to be especially vigilant with research showing that 12% of employees take company IP with them when leaving a role[13].

The proliferation of cloud computing and growth of remote working have increased the risk of businesses falling victim to IP theft. As the impact of Covid-19 subsides, remote working, as a feature of many roles, has endured as have the security headaches which accompany it. Offices have teams which have constructed IT systems with firewalls and Internet Protocol addresses. Many remote workspaces do not. Video conferencing has replaced physical meetings, meaning more and more information is shared digitally. The attack surfaces of companies have increased exponentially as a result, as has the potential for sensitive information to fall into the wrong hands.

Last year, there was a 95% increase in cloud exploitation with a near three times increase in "cloud-conscious" cyber criminals[14].

Emerging technological developments also pose new challenges for businesses attempting to protect their IP assets. New AI and machine learning tools, in particular, mean that users are able to create music, photos and other content which can then be applied to advertising or marketing campaigns. While this AI-enabled material is often perceived as new or unique, behind much of this information, however, could be protected copyrighted material. These new tools also enable almost instantaneous production of material which fails to attribute sources and violates open-source licenses, compounding fears that AI will lead to 'industrial-scale' IP theft[15].

In 2021, our Risk & Resilience survey found IP threat was regarded as being effectively minimal with only 11% of business leaders ranking it as their top risk. Fast forward to now, this risk has more than doubled (24%). IP theft has now become the cyber and technology risk for which businesses across the world feel least prepared, with more than one in four businesses (26%) reporting they feel unprepared for this risk.

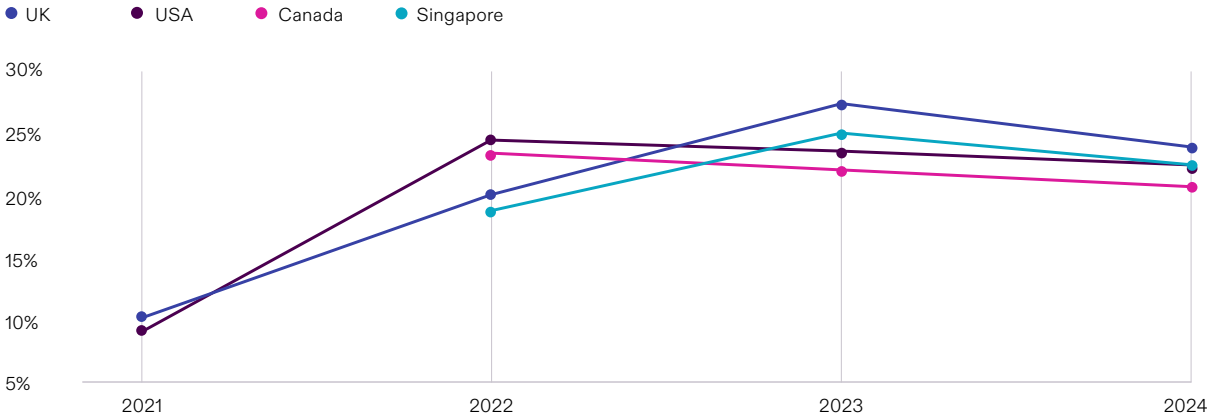
> **IP theft is an incredibly profitable and common form of cyber-attack, and many businesses may find themselves having to deal with threat actors who have been secretly embedded within their IT infrastructure, stealing IP for many years.**

Jon Miller,
CEO and Co-Founder,
Halcyon

[13] https://www.infosecurity-magazine.com/news/12-of-employees-take-ip-when/
[14] https://www.crowdstrike.com/global-threat-report/
[15] https://www.wsj.com/articles/ai-chatgpt-dall-e-microsoft-rutkowski-github-artificial-intelligence-11675466857

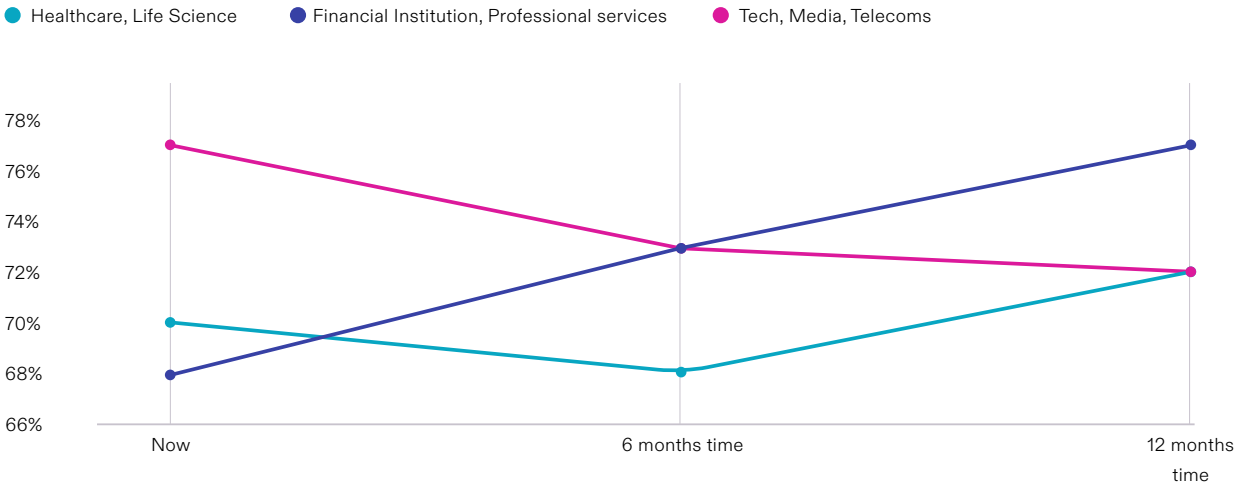
The IP threat is in the ascendancy

Percentage of executives who rank IP risks as their number one technology risk, by country



Financial and Professional Services firms most concerned about IP risk (Top 3 risk)

Percentage of executives who rank IP risks as the most significant technology risk, by sector



Financial institutions find themselves on the IP theft frontline

Concern around the theft of innovations and IP is particularly pronounced in the financial institutions and professional services sector, both now and for the long term, with more than three quarters of boardrooms (77%) believing that this will be a key concern in 12 months' time, increasing from 68% today.

As a sector the financial services industry has endured repeated high-profile incidents which have likely ingrained the risk. In 2011 former Société Générale (SG) trader Samarth Agrawal was found guilty in the US of having copied and printed reams of proprietary SG code[16] used for high-frequency trading while Sergey Aleynikov[17] was convicted of stealing code from Goldman Sachs as he prepared to move to a high-speed trading start-up.

However, whilst the risks are clear, the financial services industry is one of the most sophisticated sectors in dealing with IP and cyber threats. After repeated attacks, firms in this sector are more aware of the risks than ever before, and have the ability and resource to build deeper resilience through this experience.

[16] https://www.reuters.com/article/us-societegenerale-agrawal-conviction-idUSBRE9700SZ20130801
[17] https://www.nytimes.com/2010/12/11/business/11trader.html

Tip of the AI-ceberg

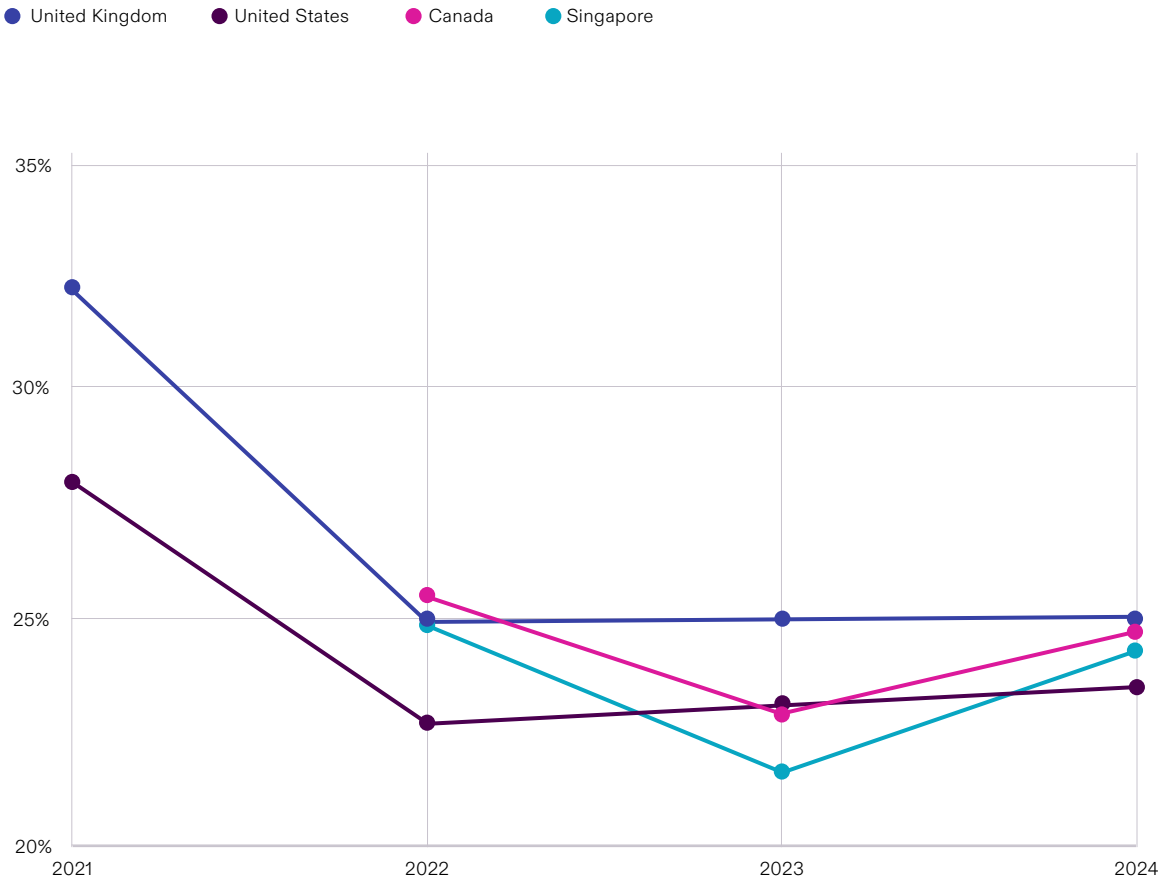
The contrast between dissipating board-level concern and the reality of the cyber & tech risk landscape is a theme that runs through this report. Concern is down, so too is resilience. Yet the danger is increasing.

The threat posed by tech disruption – the failure to innovate, to keep pace with new business developments, competitor activity, customer demand or market shifts – follows a similar pattern. In the UK and the US, leaders' perception of the risk has significantly declined since our study began in 2021 and reached a plateau today. In our survey two years ago, around a third (32%) of UK executives ranked tech disruption as the top cyber and technology risk. This dropped to almost a quarter (24%) by 2022 and has increased slightly to 25% this year. The pattern is almost identical in the US, at 28% in 2021, dropping to 22% in 2022 and again in 2023. In the US, leaders predict the risk to remain the same in 2024.

The immense changes which Covid-19 thrust on businesses and the unprecedented level of disruption caused by the need to adapt to a myriad of challenges must be taken into account when considering how this risk has been viewed in recent years. It is understandable that businesses feel they are now operating in a new normal.

Threat of tech disruption expected to plateau, yet almost a third of US business feels unprepared to face risk of tech disruption

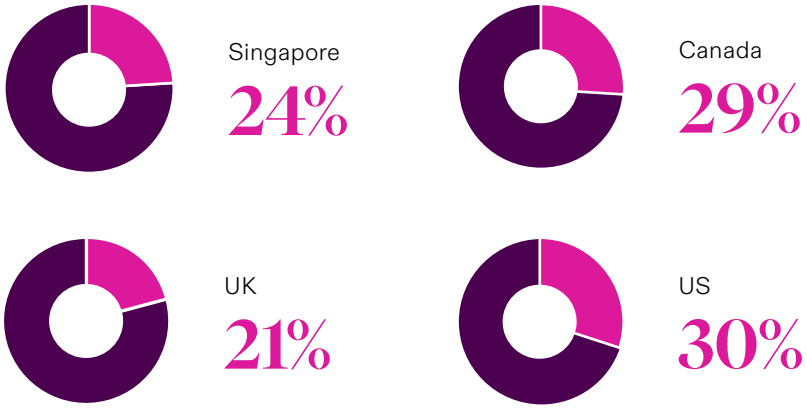
Percentage of executives who rank tech disruption as the top cyber and technology risk



Our data suggests business leaders in the US are least concerned about the risks posed by tech disruption. Yet, they also report feeling the least resilient, with one in three (30%) saying they do not feel prepared to face the risks. The seemingly paradoxical nature of these viewpoints, that a threat to which they feel less prepared is also of less concern, suggests either that boardrooms are hoping for the best, or feel unable to focus on a risk for which they are increasingly ill-equipped.

Research reveals limited appetite for disruption

Percentage of executives that are 'not well prepared' or 'not at all prepared' to face tech disruption risks



Unknown unknowns multiply

From personalised medicine to self-driving cars, the use of tools underpinned by AI has exploded in 2023. Perhaps the most prolific has been ChatGPT, an AI chatbot which pools information from across the internet to produce new written material in seconds, from pithy social media posts to handling customer complaints and churning out long-form reports.

As a result of the underpinning algorithm continuously learning from information fed in, AI has become a highly convenient tool to have at our disposal. It has the potential to completely revolutionise the way we work and live.

However, it also carries an unprecedented level of risk for business, which we are just scratching the surface of understanding. For example, reports suggest sensitive and proprietary information is being fed into AI content production engines by employees at one company, and then resurfaces in the results produced by the AI platform for employees at competitor organisations when they request similar work. In this scenario, the intellectual property (IP) risks are abundant. As we explored in the previous chapter of this report, it is hardly surprising that business leaders believe IP risks have doubled over the last two years.

Moreover, AI's growing sophistication and ease of use means it is watering already fertile ground for malicious cyber criminals, enhancing their toolkit to convince businesses by fraudulent means to transfer funds.

Deepfakes fool the world – and business will pick up the bill

In March this year, an image of Pope Francis in a white puffer coat became an overnight internet sensation. A viral tweet sharing the image was viewed more than 20.6 million times across social media and made headlines across the world's major news outlets, as the quality of the image fooled millions into believing it was real. While a seemingly harmless demonstration of the capabilities of AI, it revealed the potential for far more sinister applications of this technology and its propensity to spread disinformation as we struggle to distinguish between reality and AI creation.

AI's growing sophistication means it can now mimic the way we communicate via digital channels. That includes emails and instant messaging and, more recently, replicating voices on audio calls and faces in images and video.

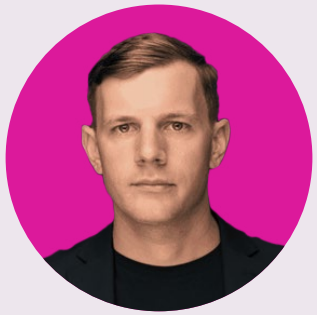
Data from our Q1 2023 Cyber Security Snapshot[18] revealed loss from fraudulent instruction is trending upward, accounting for around 13% of all cyber losses. While down on last year (16%), the number is almost double that of 2021 when our Risk & Resilience research began. Sectors at greatest risk are government organisations and non-profits, whose losses by fraudulent instruction have rocketed to represent 31% and 30% so far this year.

The hidden story is professional services. This industry has been a continuous target and suffered the most incidents of any industry in both 2022 and Q1 2023. While their proportion of incidents related to fraudulent instruction has crept up only slowly since 2021, the total number of fraudulent instruction incidents is more than double that of any other industry since 2021[19]. Similarly, professional services reported the highest proportion of business email compromise at 32%.

Spotting and mitigating the risk

As AI technology continues to grow at a pace, we can only expect the use of deepfakes to continue. Social engineering and phishing methods used by cyber criminals, which trick employees into sharing information or clicking on innocent appearing links that seem to come from a trusted source, are growing increasingly sophisticated. Businesses face the challenge of protecting their staff from identity theft and, by extension, their reputation. We have already begun to see claims notifications as a result of deepfakes used in social engineering attacks.

> **If cyber criminals begin to take advantage of new AI tools and we see articles appearing in the news on this or a high-profile incident, then this will likely prove the trigger for organisations to consider their own exposures.**



Adam Harrison
Managing Director,
Lodestone UK

[18] https://www.beazley.com/en-us/cyber-services-snapshot/defence-depth-cyber-security
[19] ibid

Modern warfare – cyber and political risks merge

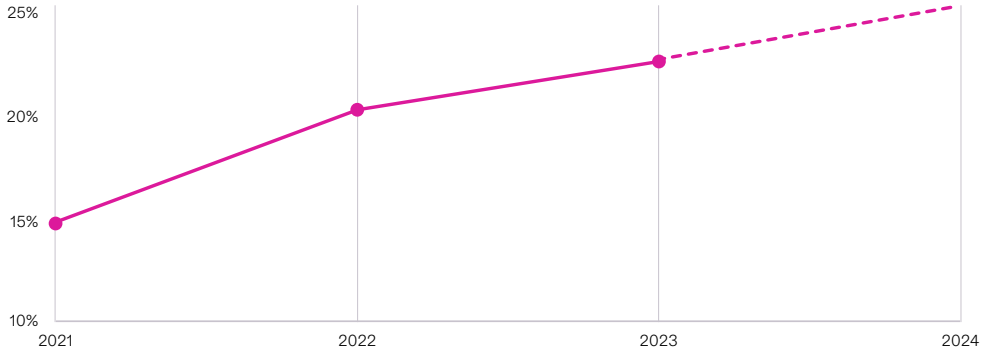
In February 2022, Ukraine's broadband satellite internet access was attacked as Russia's invasion of Ukraine got underway. This came as little surprise. Targeting communications and reducing an adversary's ability to coordinate a response is not a new military tactic.

However, rather than deploying its missiles or soldiers, Russia used a new strain of malware called "AcidRain"[20] to disable the modems in Ukraine which communicated with Viasat Inc's KA-SAT satellite network, a key supplier of internet access to Ukraine and across Europe. The US, EU and UK attributed this attack to the Russian state[21] and cyber-attacks against infrastructure in Ukraine have continued ever since.

Nearly a quarter of businesses (24%) globally in our 2023 survey believe that war and terrorism will be a key risk to which they are exposed in the next 12 months. This exposure is no longer solely determined by their proximity to a conflict. While non-native businesses rapidly withdrew their employees and closed their operations in Russia and many affected parts of Ukraine, unplugging digital links to the conflict is more complicated. Russia's attack on Ukraine's broadband spilt over into other countries in Europe with the collateral damage from state sanctioned cyber-attacks extending far beyond the borders of the primary target.

The threat of war and terrorism is an increasing concern for businesses

Number of executives in the US, Canada, UK and Singapore who ranked War & Terrorism as their number one political and economic risk



The potential impact of cyber warfare is immense and the Russian invasion of Ukraine has provided a snapshot of the potential usages of cyber-attacks when it comes to armed conflict. However, the intended effects of cyber warfare are very different from those perpetrated by cyber criminals. To consider this fully, it is necessary to dissect the motivations behind state sponsored attacks as opposed to the goals of cyber gangs. For the latter, it is about maximising financial gain so that attacks are structured to allow for a payment to be made, whether this is through ransomware, phishing, IP theft or any of the other myriad of approaches used to extort money. Individual cyber attackers, or groups of them, want their efforts to result in a pay out. They want to threaten disruption and cause enough impact to make a business fear the consequences sufficiently without destroying the potential for a repeat attack.

[20] https://securityintelligence.com/news/acidrain-malware-modems-ukraine-germany/
[21] https://techcrunch.com/2022/05/10/russia-viasat-cyberattack/

Tradecraft moves online

State-sponsored espionage has occurred for decades, with countries keeping tabs on rival financial systems or energy capabilities or seeking to access military innovations and strategies. Because they are well-funded, equipped and highly trained, state-sponsored cyber-attacks are often very difficult to detect. Even if an attack is discovered, it can easily look like another group was the perpetrator.

Proving that a state was responsible can be very difficult and diplomatically tricky. This makes cyber espionage an effective and often risk-free option for states to use. The next step up is state-sponsored IP theft. The United States Trade Representative has alleged that Chinese theft of American IP currently costs between US$225 billion and US$600 billion annually[22]. However, the impact is controlled, and hedged to avoid overly obvious attribution.

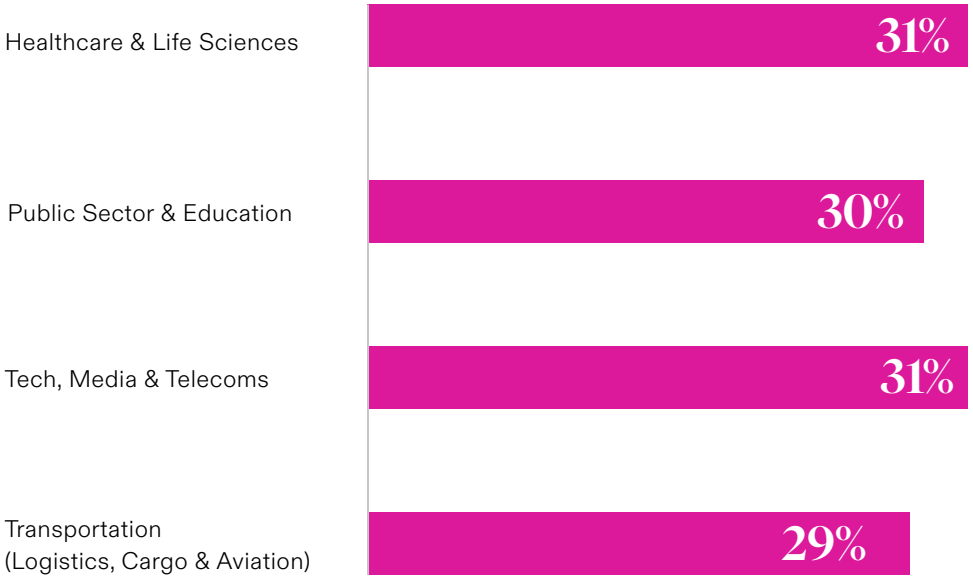
Weapons of war

Cyber warfare is intended to cause the maximum level of disruption or destruction to infrastructure to support wider war efforts or national goals. The motives are unlikely to be financial. Instead, they focus on targeting sectors of an economy which, through restricting or removing their ability to function, they can reduce that nation's ability to fight or function. Where once this might have been achieved with missiles, now nations can use malware.

However, while targets may be hit with precision, the impact and how far it will extend is less clear. The interconnected nature of global networks means that a cyber-attack against Ukrainian utilities, for example, can extend far beyond the country's borders. Our research shows that telecoms and technology businesses are particularly aware of this, with executives feeling equally unprepared to deal with the threat (31%) of any industry type alongside healthcare and life sciences firms.

Confidence is greatest within financial institutions and the professional services sector

Percentage of executives in the US, Canada, UK and Singapore who feel are 'not well prepared' or 'not at all prepared' to deal with the risk of War & Terrorism



22 https://www.fbi.gov/file-repository/china-exec-summary-risk-to-corporate-america-2019.pdf/view

Building new defences

Whilst the impact of the ongoing cyber-attacks in Ukraine has not significantly impacted businesses in other countries, this is more likely due to the actions of cyber security teams than precautions taken by the Russian attackers. However, as we have seen throughout this report, maintaining constant vigilance can breed fatigue and businesses should not rely on today's defences holding tomorrow. The same can be said for the cyber insurance market.

Traditional warfare has been excluded from most insurance policies, as markets recognised that it is too big a risk to cover. Now cyber is also a tool in nation states' arsenals, it is recognised that cyber war is similarly too big a risk for the cyber market to cope with.

What does that mean for clients? We can be very clear on the cover we are giving if they are impacted by a cyber war event. We can also help clients to be as resilient as possible to the risk so that they are as protected as possible should a cyber war event occur. And, finally, we are working in collaboration with other insurers, brokers and the Lloyd's Lab to develop a dedicated cyber war product to provide some cover in the event of a cyber war event, and we hope to launch it soon.

It is clear businesses now feel more exposed to the risk of cyber war. We must provide a solution to address our clients cyber war exposure should they wish to. Most importantly, we must do so together. The insurance industry has a long history of affecting positive change through collective action. By collaborating at this key juncture for the cyber insurance market we can offer insureds clarity and certainty when it is needed most.

> **The level of potential disruption which a cyber war attack could cause is on a scale far greater than anything we have seen before. Which is why we spend a lot of time thinking about what an attack would mean to the cyber market and how we can help our clients.**

Paul Bantick
Global Head, Cyber Risks, Beazley

The role of insurance

More than a third of businesses we surveyed (36%) plan to invest in cyber security this year. Judged on its own, this statistic could be viewed positively.

However, this represents a sharp decrease from last year (46%). The risk is not diminishing and for many businesses, particularly those in the middle market, defences are not where they need to be. The widening gulf between how the threat is perceived and the reality is stark. It is incumbent on insurers and brokers, who play a key role in highlighting the threat to businesses and the positive impact of defence in depth security, to ensure firms do not become desensitised to the cyber risk and expose themselves to ever more effective cyber criminals. Insurance must be part of the prevention.

The news agenda should not be used as a barometer of the scale of a particular threat. That AI is in focus now does not make ransomware less of a threat. Deepfakes which attract the public interest do not make it the biggest risk overnight. Businesses must ensure they resist the pull from the latest concern and stay on course, focusing on genuine and palpable threats to their operations. How and where AI will change our world will continuously evolve. Where businesses are at risk in one sector, new industries may spring up in others.

It is a generation defining innovation and the potential is almost impossible to comprehend. While boardrooms adjust to the new horizon, companies of all sizes must continue to take the necessary steps immediately in front of them. These may not be glamourous, cyber security rarely is, but they may ensure that their business is able to realise the potential in the future.

In recent years, the value of cyber insurance has been proven beyond doubt. The insurance industry has been called upon to respond to an avalanche of incidents and paid out billions in ransomware claims alone[23]. That is what we are here to do. However, for the cyber insurance market to grow, it must recognise that certain risks are too big to cover, that their impact is of sufficient scale to be considered systemic and catastrophic. These risks are few, but they do exist. Cyber war is one such risk. The potential losses are only increasing. As the wording of war exclusions evolves to reflect the reality on the ground, then a new cyber war market is evolving to furnish some of the demand.

The evolution of technology is making more and more businesses feel exposed. Insurers must ensure that they are evolving as partners. That we are supporting businesses as they embrace new innovations, jolting them from their reverie when they believe a clear threat has dissipated and working to create new solutions as risks compound and their potential impact grows.

> **These are uncertain times for many businesses and insurance must work harder to provide greater security.**

Paul Bantick
Global Head, Cyber Risks, Beazley

[23] https://www.bloomberg.com/news/articles/2023-02-24/cyber-insurance-back-from-the-brink-after-ransomware-onslaught?leadSource=uverify%20wall#xj4y7vzkg

Methodology

About the Risk & Resilience research

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:

- **Environmental** – including climate change and associated catastrophic risks, environmental damage, greenhouse gas emission, pandemic, food insecurity and energy transition 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.

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

Previous editions of the survey were undertaken between 01.02.2021 and 10.02.2021 as well as 10.01.2022 – 24.01.2022.

Contributors

Paul Bantick
Global Head of Cyber Risks, Beazley

Meghan Hannes
Head of US Cyber & Tech Underwriting Management, Beazley

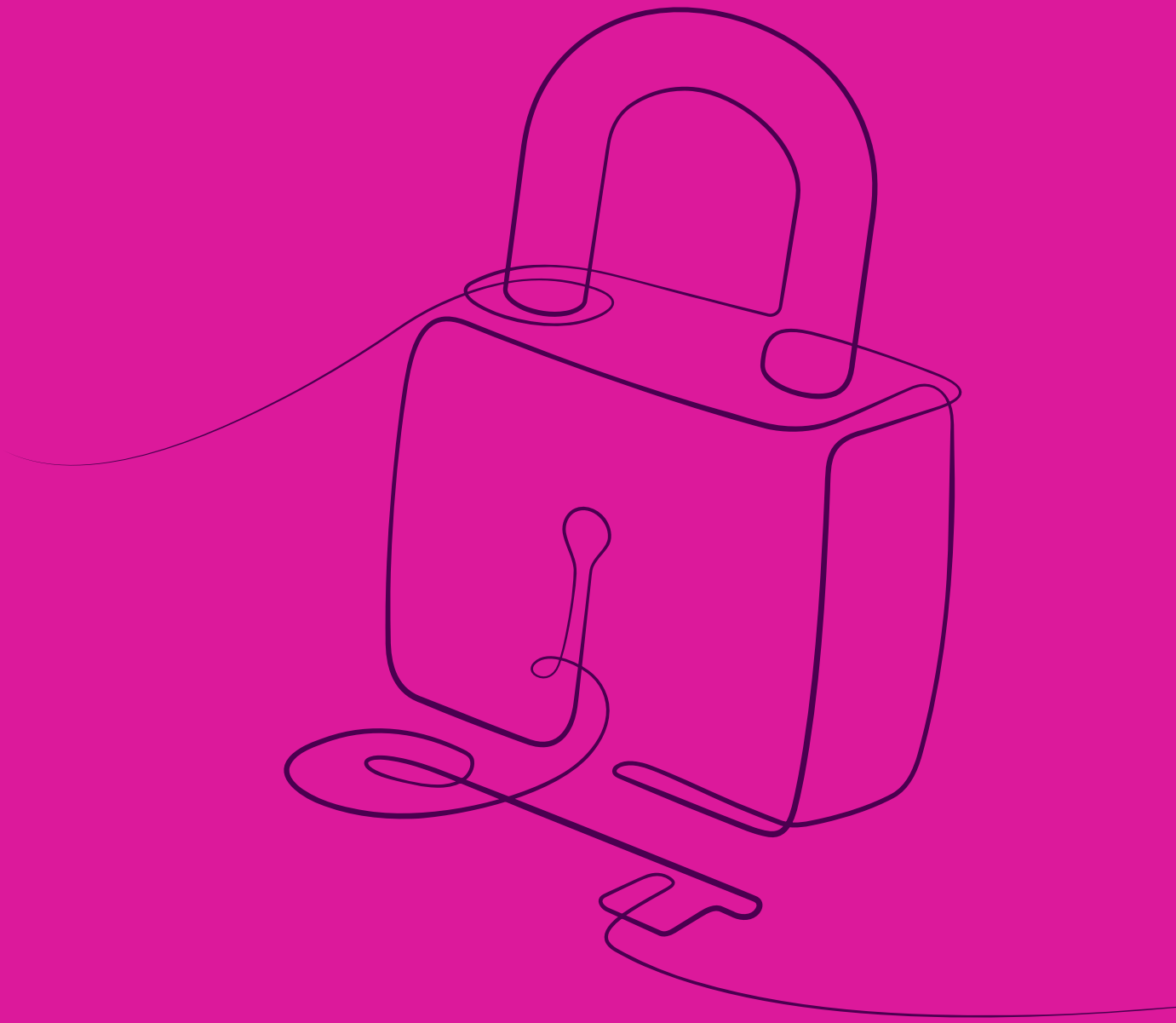
Katherine Heaton
Focus Group Leader Cyber Services and InfoSec Claims, Beazley

Adam Harrison
Managing Director, Lodestone UK

Jon Miller
CEO and Co-Founder, Halcyon

Discover more

beazley.com



beazley

Insurance. Just different.