beazley

Spotlight On Cyber & Technology Risk 2024

Resilience in a game-changing environment

Executive Summary

In today's era of accelerating cyber and technology risks, organisations are on the front line.

Our 2024 Risk & Resilience research reveals that while technology offers significant opportunities and benefits, it also presents new and heightened risks for business leaders, many of whom are unprepared for the current and future landscape.

Our survey of global business leaders reveals that generative artificial intelligence (AI) is seen as a 'friend' and 'foe'. 27% are concerned about tech obsolescence risk in the face of new technologies (such as AI), rising to 28% by 2025. And 25% believe the threat posed by disruptive technologies is the top risk they face this year. The speed of adoption of AI technologies is also reflected in our research data, with one in four (25%) of the firms we surveyed planning to invest in AI this year to improve their firm's resilience to risk. And 68% believe AI will lead to jobs being replaced in their company this year.[I]

Concern over AI, tech disruption and intellectual property (IP) risk appears to be creating something of a blind spot to cyber risk, with the percentage of executives ranking cyber risk as their top concern declining from 34% at the height of the 'ransomware pandemic' in 2021[IV] to 26% now. This stands in stark contrast to the reality of today's cyber risk landscape. One where cyber crime has evolved into a highly specialist, professionalised industry, run by ruthless threat actors motivated by financial gain.

Worryingly, our data shows that perceived cyber risk preparedness has dropped from 80% in 2022[V] to 75% this year.[II] For CEOs, who are likely to find themselves accountable in the aftermath of a cyber attack, cyber is not a risk that they can afford to take their eye off the ball with. It is, however, reassuring to note that nearly a quarter (24%) of the executives we surveyed are planning to invest in their cyber security risk management, and the same percentage is looking to explore insurance options that include risk and crisis management services.

With cyber crime 'kill chains' becoming increasingly sophisticated and harder to pre-empt, misinformation is a significant risk factor, and with new regulations on the cards, boardrooms need to be on the front-foot, ready to manage cyber and tech risks as they evolve. By gaining greater visibility with threat intelligence, building resilience strategies that pre-empt these risks, and creating a response plan in case of a cyber attack, businesses will have in place an effective cyber defence. However, as this report discusses, the range of cyber and tech risks are evolving at speed, making an 'always on' security strategy essential.

The insurance industry has an important role to play in helping firms navigate today's evolving cyber and tech risk landscape. By leveraging the vast amounts of claims, incident, and threat information data we have and translating this insight into actionable guidance and elevated resilience for a range of cyber and tech risks, we can help our clients to better mitigate risk.

The recent CrowdStrike IT outage is a timely reminder of how fragile the global technology networks are and what can go wrong when one link in the chain makes an error or costly mistake.

By helping businesses to embrace all that technology has to offer while supercharging their resilience to risk will help keep them one step ahead in the game, no matter what the future holds.

Paul Bantick
Group Head of Cyber Risks
Beazley

Alton Kizziah
CEO
Beazley Security

Key cyber & tech findings from our Risk & Resilience research

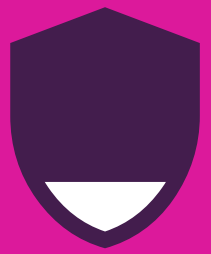
Global business leaders told us

27%

feel exposed to tech obsolescence challenges ranking it as their top risk now, rising to 28% in 2025.

26%

Their concern over cyber risk is dropping – with 26% ranking this as their top risk, compared to 34% in 2021.[IV] Yet, perceived cyber risk preparedness[II] is down to 75% compared to 80% in 2022.[V]



24%

plan to invest in cyber security this year and to explore insurance options that include risk and crisis management services.

25%

A quarter (25%) believe AI and other disruptive technologies are the biggest risk they face this year.

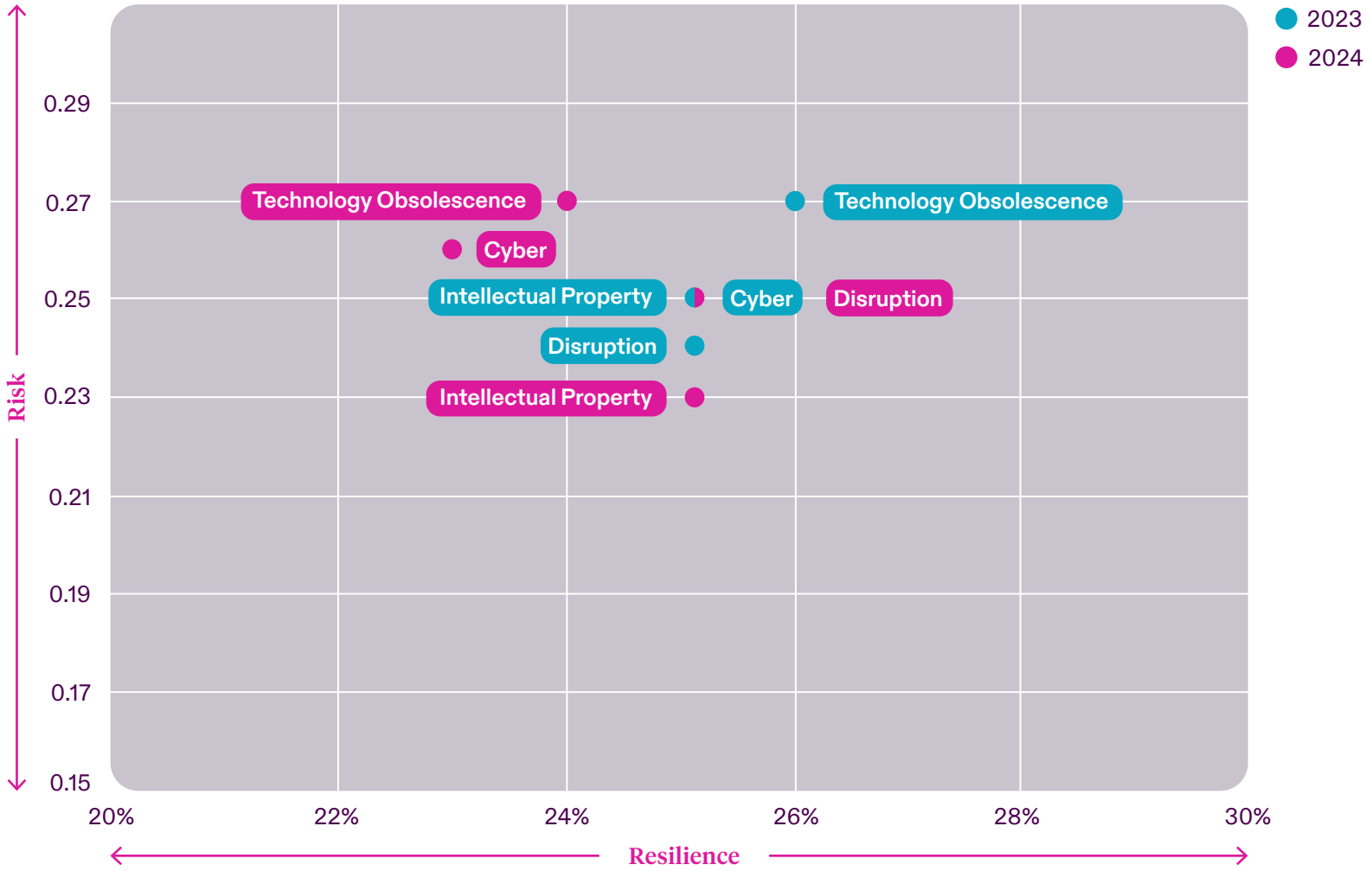
25%

AI is seen as a popular way to build business resilience, with 25% planning to invest in it this year. And 68% believe that AI will lead to jobs being replaced in their company.[I]

23%

IP risk continues to rise up their risk agenda, with 23% ranking this a top concern, up from just 11% in 2021,[IV] and a quarter (25%) feel unprepared to manage IP risk.[III]

Risk Matrix – 2023 to 2024 Risk & Resilience stats



For brokers

1 There continues to be a blind spot around the nature of cyber risk, with 75% of global executives surveyed believing they are prepared[II] for it. Our claims data shows us this is not the case, and there is an urgent need to educate firms on the changing face and sophistication of cyber crime today and the importance of 'always on' cyber resilience strategies.

2 C-suite executives are ultimately responsible for their firm's risk management of cyber and technology risks. If they get this wrong it is likely to not only result in business interruption, reputational damage and potential regulatory issues, but also directors' & officers' liability claims, as the buck stops with the board. As a result, firms need insurance programmes that cover the full spectrum of cyber and tech risks they face.

3 24% of our survey's respondents are looking to improve their resilience via insurance and, in particular, insurance with additional risk management services offered. Clearly, many recognise the benefits of the insight and expertise that the insurance industry can offer.

For businesses

1 While the advent of new technologies, such as AI, offers the opportunity to streamline operations and increase efficiency, it also presents significant risk. The pace of innovation can leave firms exposed to risk linked to tech obsolescence, more sophisticated phishing attacks, and accusations of bias in new AI systems. Staying ahead of the curve has never been more important. Firms of all sizes must be prepared to counter the ever-evolving cyber and tech threat landscape.

2 As the business world digitalises and moves into the Cloud, businesses are being targeted by cyber criminals through their suppliers. With cyber criminals favouring the path of least resistance, the need for businesses to assess their third party relationship vulnerabilities is increasingly important.

3 While insurance can provide an important safety net, no business is immune to the threat posed by cyber crime. Elevated risk requires elevated resilience and firms need to be on the front foot and use all the tools at their disposal to defend against a cyber incident, this includes gaining greater visibility with threat intelligence, building resilience strategies that pre-empt risks, and creating a response plan in case of an attack.

Index

The Changing Face of Cyber Crime

Cyber crime represents one of the greatest transfers of economic wealth in history.

The Changing Face of Cyber Crime

Cyber crime will cost companies worldwide an estimated US$10.5 trillion annually by 2025, up from US$3 trillion in 2015.[1] At an annual growth rate of 15 percent – cyber crime represents one of the greatest transfers of economic wealth in history. Yet, our Risk & Resilience survey reveals that business leaders appear to be out of step when it comes to cyber risk, with the percentage ranking cyber risk as their top risk dropping year on year. Today, the concern over the threat of cyber risk is at its lowest since 2021,[IV] declining from 34% at the height of the ransomware pandemic to 26% now. This dropping concern about cyber risk is despite multiple studies showing that the severity and cost of attacks are rising.

Over the past four decades, the threat of cyber crime has steadily increased. Cyber criminals have been swift to adopt new technologies, continually devising and honing techniques to trick individuals into revealing sensitive information or inadvertently granting access to networks via phishing attacks, by finding vulnerabilities in software or system security, or via third party suppliers.

Today, cyber crime is an industry, with sophisticated, ruthless and highly efficient operatives working in it – some state sponsored. With or without state backing, many cyber criminals continue to operate with near impunity and safe from extradition. So why do business leaders view the threat as diminishing? Is this blind faith or justified confidence?

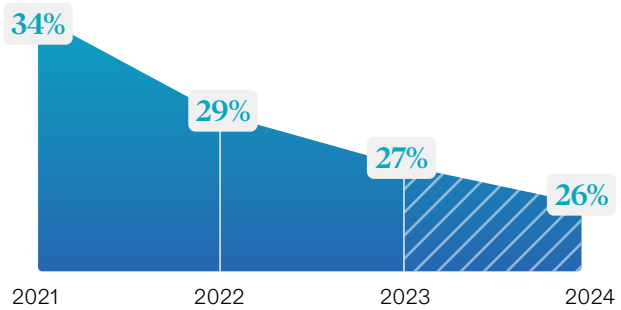
Some of the findings from this year's Risk & Resilience research show cyber risk continues to be a blind spot for global executives – where they appear to be failing to see or understand the changing face of cyber crime.

- The perceived threat of cyber to global business leaders continues to drop – with only a quarter (26%) ranking cyber as their top threat – down from 34% in 2021.[IV]
- However, perceived resilience to cyber risk is simultaneously dropping – with 75% of executives feeling prepared[II] for cyber risk, down from 80% in 2022.[V]
- And 11% of global boardrooms admitted in the survey that they believe their organisation has inadequate protection for cyber risk.[5]
- 23% of c-suite leaders said they are unprepared for cyber risks this year – this rises to 28% among large UK firms (£1bn+ revenue).[III]

> "Cyber criminals exploit businesses for financial gain. However, the nature of the attacks are becoming ever more sophisticated, in terms of the techniques and methodologies. We have seen that cyber crime networks are becoming more industrialised."

Patricia Kocsondy
Head of Global Cyber Digital Risks, Beazley

Concern around cyber risk is falling



Percentage of global business leaders ranking cyber risk as their top risk over time[VII]

> **Cyber criminals have earned hundreds of millions and are reinvesting their earnings in upgrading their offensive capabilities. Their operations are expanding, and they are investing in maintaining and accelerating that growth. This enables them to target more businesses with expensive zero-day exploits and increased sophistication."**

Francisco Donoso
Chief Technology Officer
Beazley Security

Watch the video

Many cyber crime techniques established over the past forty years continue to be used today and have been updated to meet current business paradigms. This means that, while the technical sophistication of many attackers has increased, one of the best defences an organisation can deploy is having sound process related to patching, governed access to systems, and monitoring of systems, user behaviours, and data.

Where things get more complicated is the change in motivation. Threat actors that were previously driven by activism have fallen away, almost completely, and been replaced by those motivated entirely by profit. And, as a business focused on efficiency, these actors have continued to innovate. Advanced techniques and tools that were formerly available only to nation states are now commercially available to well-funded and sophisticated criminal organisations. This raises the stakes for organizations as they face a steady supply of experts ready to infiltrate IT systems, exfiltrate data at speed, exploit their targets and sell data on the dark web to maximise profit.

Elevating cyber risk needs elevated resilience

Cyber defence tools and techniques have improved markedly over the past couple of years. However, cyber criminals have proved to be adept at evolving and finding ways around new defence methods. The tools that have been developed to protect businesses, from multi-factor authentication (MFA), virtual private networks (VPNs) and firewalls to remote access solutions, are being breached by cyber criminals. Once they have found vulnerabilities, they are quick to exploit them.

In this era of escalating cyber threats, firms need to be on the front foot and use all the tools at their disposal to defend against a cyber attack.

As we saw with the Crowdstrike IT outage in July, businesses need to remain nimble so that they can move quickly to identify vulnerabilities and patch systems when issues arise.

They need defence strategies in place, that include detailed incident response plans that consider their entire attack surface as well as back-up systems to minimise the risk if an attack should happen, often referred to as 'defence in depth' strategies.

> **There needs to be a paradigm shift in firms' approach to cyber risk management. Firms should be seeking to future-proof their resilience to cyber risk, as threat actors are successful due to evolving, but imperfect IT security, and the constant of human vulnerabilities. So, thoughtful preparation, being open to adapt as the threats evolve and dynamic response plans and vendor options, are essential."**

Marcello Antonucci
Claims Team Leader
Cyber & Tech Risks, Beazley

Watch the video

Managed detection and response (MDR) techniques that provide always-on, pro-active cyber resilience services via continuous monitoring of new threats and situations are the gold standard in cyber defence.

Spotlight on healthcare

The healthcare sector is increasingly being targeted by cyber criminals who are threatening day-to-day work and compromising confidential patient data. There are multiple reasons for this. Private patient information is highly sensitive and, by extension, highly valuable to cyber criminals.

As an industry, healthcare often continues to employ outdated technology which leaves them vulnerable to attacks. Despite the remarkable advances in medical technology, the IT systems deployed have not kept pace. Furthermore, healthcare providers often have limited budgets for cybersecurity. The combination of high reward, multiple, weak entry points and limited security has seen cyber threat actors zero in on the sector with a series of high-profile breaches in recent years.

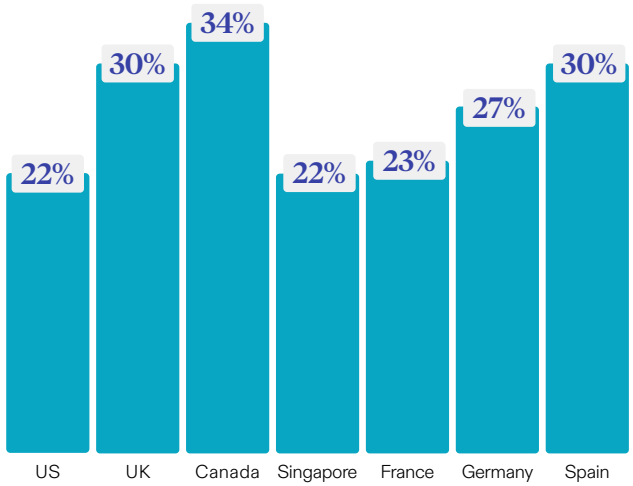
Healthcare businesses are also under scrutiny from regulators focused on protecting private customer data. For example, in the US, The Health Insurance Portability and Accountability Act (HIPAA) breach notification requirements place strict breach notification requirements on healthcare businesses. Any breach affecting over 500 individuals must be reported to the Office for Civil Rights (OCR)[2], which in turn paints a target on the backs of these institutions for plaintiff lawyers.

25%

of **global healthcare business leaders** said they are unprepared to face the current cyber threat.

The risks are further compounded by the advent of sophisticated tracking technologies and data privacy concerns. A surge in litigation, sparked by revelations that numerous hospitals had implemented tracking pixels on their websites, has led to hundreds of class actions filed against healthcare entities. These pixels, often unbeknownst to patients, can share intimate details of their health concerns with third parties, breaching patient trust and privacy. As they grapple with regulatory pressures, budgetary constraints, and the increasing sophistication of cyber criminals, healthcare providers must remain vigilant and proactive in their cybersecurity efforts.

The cyber risk for healthcare providers is elevated across the globe



Percentage of life sciences and healthcare business leaders ranking cyber as their top risk, by country

> **Hackers are targeting healthcare. Plaintiff lawyers are targeting healthcare. And people are more conscious of the data that they're sharing. Two or three years ago, you would not get a data breach class action unless there were at least 500,000 people whose data had been exposed. We now see data breach class actions being filed when there's only 1,000 people whose information was disclosed."**

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

The Need for Speed

Firms need to respond to new cyber threats fast.

The Need for Speed

Long gone are the days of hackers breaking into networks with the aim of defacing websites. The mindset of hackers has evolved. With both nation states and hacking groups instigating attacks, the speed and sophistication of the cyber 'kill chain' means all businesses are at risk of an attack. To counter this threat, firms need to respond to new threats fast.

The cyber threat landscape now includes nation states, and state sponsored hackers tend to strategically target networks and third party technology suppliers often seeking to gain access to national infrastructure or other critical supply chains. Hacking groups follow in the wake of these attacks, harnessing the malicious code used in state sponsored attacks, which is often available within hours on the dark web, to launch attacks on businesses that are often unaware that a new threat has emerged. Hackers then look for the weakest link in the chain, having honed their hacking skills to reduce data exfiltration timescales, in some cases to a matter of hours.

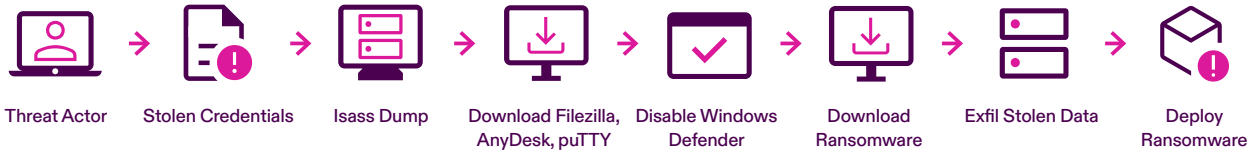
Despite the cyber threat continuing to develop and grow, our data shows that global business leaders' concern about cyber risk has consistently dropped year on year since we started our Risk & Resilience survey in 2021. The percentage of business leaders surveyed citing cyber as their biggest threat has fallen from 34% in 2021,[IV] to 26% in 2024.[VII] Yet, the tactics employed by hackers are constantly evolving, to such an extent that breaches are becoming increasingly difficult to prevent for businesses without adequate protection.

The cyber kill chain – the battle against digital threats

Understanding the cyber kill chain and defending against digital threats means understanding the hacker mindset and their tactics.

What is a cyber kill chain?

A cyber 'kill chain' is the steps an attacker takes to break into a network and steal the data held within it. While cyber kill chains can differ in format, they begin with a cyber criminal stealing security credentials and then dumping Local Security Authority Subsystem Service (LSASS) credentials, allowing them to use legitimate programs to access a network, launch an attack to either steal data and/or launch a ransomware attack.



A cyber kill chain begins with a hacker using stolen credentials to perform an LSASS dump, an attack that uncovers passwords. In an attempt to fly under the radar and circumvent detection programmes, there is a growing tendency for cyber criminals to then download programs that are not typically malicious or even use existing systems in place to go undetected.

Once in a network, hackers work within the system to disable antivirus software, facilitating the theft of sensitive data such as client information, login credentials and credit card details.

Once this data has been exfiltrated, it will be sold on the dark web, to various parties who will use it to launch attacks to monetise the data.

Hackers may also look to deploy malicious ransomware. While ransomware prevents the target business from functioning, hackers make contact to demand a ransom payment for the encryption code needed to unlock the network.

New links in the kill chain

Historically, it would not be uncommon for a hacking group to be involved in every stage of the kill chain, from writing the code and programs used to break into a network to the exfiltration of stolen data.

With the sophistication of the kill chain, the need for hackers to be involved throughout the chain has been reduced, allowing them to specialise in a particular stage or activity. As a result, there are hackers who specialise in infiltrating networks, known as initial access brokers. These bad actors gain a foothold in networks before selling that access on the dark web. The individuals looking to purchase that access will then steal confidential data such as passwords and credit card details that are also sold on the dark web. Subsequently, a separate hacking group will likely deploy ransomware.

A race against time

Certain businesses in the US, deemed to form part of the country's critical infrastructure, such as financial services, transportation and energy firms, are legally required by the Cyber Incident Reporting Act to report data breaches to the Cybersecurity and Infrastructure Security Agency within a set timeframe[3]. However, if the business has been unable to secure its network before publicly filing a report, it will likely face a further wave of attacks. With a network's vulnerabilities in the public domain, cyber crime groups can easily retrace the steps of the original hackers to steal sensitive data. As a result, the aftermath of a cyber attack is a race against time for businesses to secure their systems before reporting the attack.

> **"The ability to monetise nearly every stage of a cyber kill chain has given cyber criminals the freedom to specialise their skillset and lowered the barriers to entry for hackers. A web of specialised hackers operating in individual areas of a cyber kill chain is more effective than hackers working across the full chain, and leaves businesses vulnerable to a wider pool of threat actors."**

Bob Wice
Head of Underwriting Management, Cyber Risks
Beazley

An example of the ingenuity of cyber criminals is a new technique called SIM swapping. Developed to help them bypass MFA security measures, hackers impersonate the victim and approach their mobile phone provider, looking to receive an alternative SIM card for their particular mobile. This gives the hacker access to the victim's mobile, allowing them to view text messages that contain MFA passcodes, which they use to gain access to company networks.

Over 1 in 10

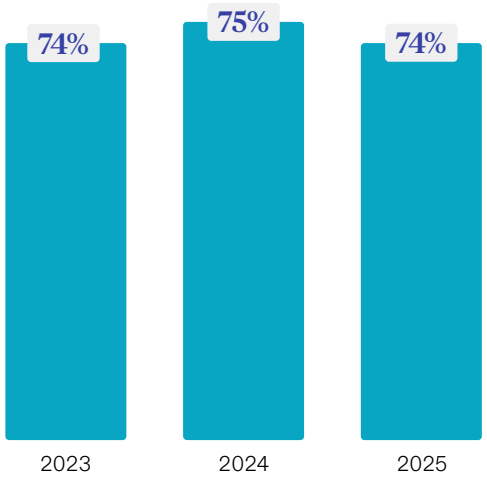
global business leaders (11%) we surveyed believe that they do not have adequate cyber provisions in place to defend against a cyber attack today.

24%

Encouragingly, our data finds that **24% of business leaders** surveyed plan to invest in cybersecurity measures this year, as their confidence in their ability to defend against a cyber attack, although surprisingly high, is dropping year on year.

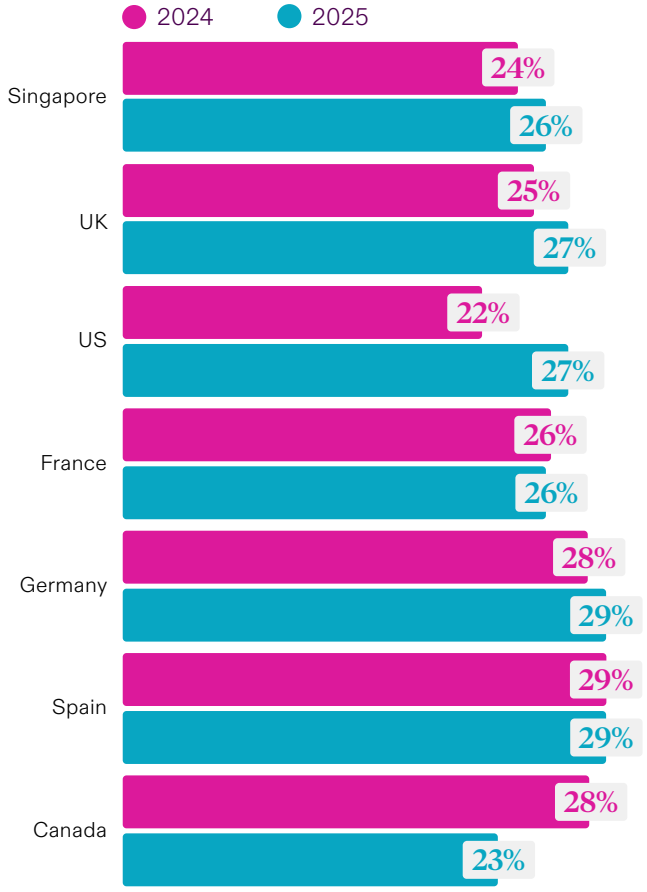
Supply chains have become an additional focus of cyber criminals in recent years as firms look to outsource services and capabilities to external vendors and suppliers. Cyber criminals know that third parties often hold sensitive data about clients which can lead to a larger breach. Third party suppliers also offer an opportunity to gain access to their customers' networks. Conducting thorough due diligence on third-party vendors and their cybersecurity measures is often an oversight which can have significant consequences.

Changing confidence levels in ability to counter cyber risk



Percentage[II] of global business executives feeling prepared to respond to the threats posed by cyber risk over time[VII]

Cyber threat predicted to rise in most regions



Percentage of business leaders ranking cyber as their number one risk in 2024 and 2025[VII]

> "With increasing sophistication in the kill chain, it is essential that organisations stay vigilant across their technology environment. Cyber criminals are now using global supply chains to their advantage, making advanced exploits available for sale or even selling access to organisations to entities that are focused on monetising an attack. The need to invest in cyber resilience is universal and it can't be narrowly focused only on traditional attack vectors."

Bobby Venal
Labs Principal Researcher
Beazley Security

AI-enabled Cyber Crime: The Next Frontier?

Cyber criminal groups are using AI to enhance their activity, and be more daring in their attack tactics than ever before.

AI-enabled Cyber Crime: The Next Frontier?

After a breakout year in 2023, artificial intelligence (AI) technology is now being mobilised by cyber criminal groups to automate and enhance their activity, work faster, and be more daring in their attack tactics than ever before.

On Monday 29th January 2024, a local clerk at an engineering firm reported to the Hong Kong authorities that they had attended a video conference call and been duped into paying HK$200m of their company's money to a fraudster.[4] Soon after the investigation was started by the Hong Kong Police Force, senior superintendent Baron Chan realised that this business had suffered one of the boldest thefts using AI to date.

Within a week, Chan sent a warning to the world, notifying media that this was a deepfake attack on the business.[5] He said: "Because the people in the video conference looked like the real people, the informant made 15 transactions as instructed... I believe the fraudster downloaded videos in advance and then used AI to add fake voices to use in the video conference."[6]

It was later revealed that this employee worked for British multi-national company, Arup, which has 18,500 employees across 40 countries. While this occurrence at Arup has now become known as the 'Zoom of Doom', the firm is not alone in facing the threat of deepfake dupes. The world's largest advertising firm WPP was exposed to a deepfake attack when CEO Mark Read had his voice cloned by scammers who used a fake WhatsApp profile to try and trick colleagues into sharing money and personal details.[7] In April, similarly, a LastPass employer thwarted a cyber-attack by criminals using deepfake audio to impersonate its CEO Karim Toubba.[8]

While AI has generated excitement, these examples highlight how this technology is now being weaponised by organised cyber criminals to trick employees and steal millions from companies. No longer can employees believe what they see and hear, and more sophisticated authentication techniques are needed to prevent these kinds of attacks from occurring.

> "The issue of authenticity is going to be a massive challenge for business leaders and courts in the years ahead. How do you verify information and data like voices and pictures in a world where AI easily deceives people? These deepfake issues will manifest in hacking, transfer of money, and fake news which will proliferate in the coming years."

Melissa Collins
Cyber & Technology
Claims Focus Group Leader,
Beazley

AI goes phishing

For decades, phishing attacks have relied on deception to extract sensitive information from businesses and workers who are unaware of the intentions of the hacker. Historically, fraudsters have developed strategies such as fake websites and emails which require significant effort from cyber criminals to manufacture and deploy. AI is now changing the game, fast.

In the arena of phishing scams, at every stage of an attack, AI is empowering cyber-criminals with the ability to enhance their techniques and increase their threat to victims.

In the preparation phase, the technology can analyse vast amounts of information in seconds and use analytics to identify trends among targets, so that it can identify the best method and time to catch out victims. The AI bot can further create templates for emails and messages that come across as human in tone, creating authentic call-to-actions that deceive victims into visiting a website or downloading malware. Making phishing attacks harder to spot.

After a target enters the phishing site, AI can create follow-up messages or adapt the content in real-time to extract more data from the victim, in turn, enabling the attack to be more effective. Once the sensitive data is collected, hackers use AI to automate their attempts to access and extract data from the victims' systems. AI can do this faster than any human could.

AI-enabled phishing attacks like these are leaving victims and businesses exposed to a more heightened risk than ever before.

To mitigate this accelerating risk, business leaders need to ensure they put in place checks and balances across their systems. One area of focus for firms should be training colleagues in cyber security so that they know how to identify the signs of a phishing scam and flag issues to security teams at speed. Only by sharing knowledge across the business can companies pre-empt, respond, and adapt to a fast-changing risk landscape. Furthermore, in the future, as AI becomes more widely used by cyber security professionals, we may see more firms finding opportunities to fight back against cyber criminals with AI technology.

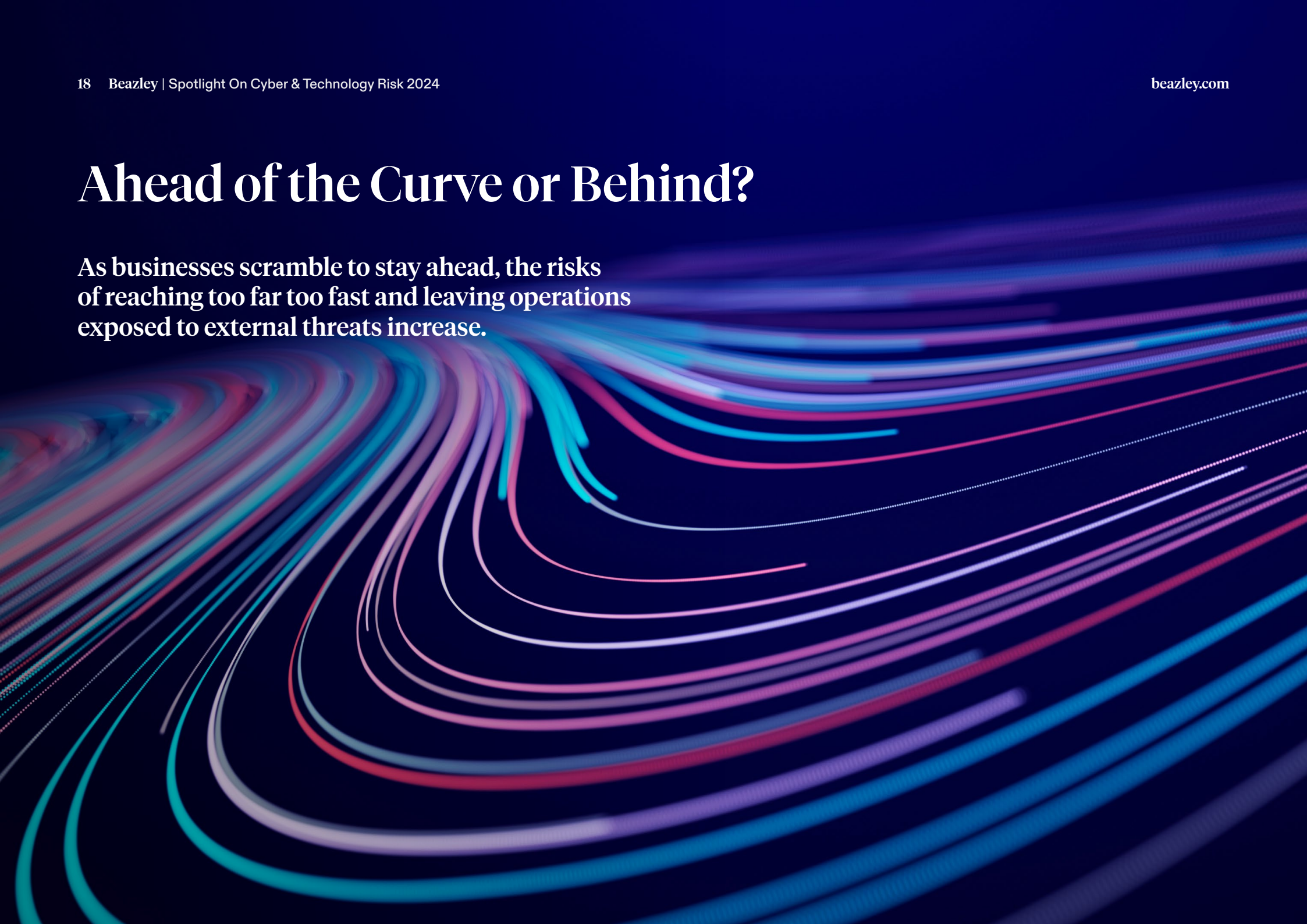
> **"Businesses need to be constantly alert to new cyber risks emerging – AI-enabled cyber risk is increasingly becoming the next frontier for firms. Business leaders need to consider what controls and training programmes they have in place so that staff identify any AI-generated scams and report suspicious activity."**

Christian Taube
VP Cyber Services – International, Beazley Security

Watch the video

Ahead of the Curve or Behind?

As businesses scramble to stay ahead, the risks of reaching too far too fast and leaving operations exposed to external threats increase.



Ahead of the Curve or Behind?

How are we using generative AI? Are we ahead of the competition? Behind? Where will we be this time next year? These questions are being discussed by business leaders around the world. As businesses scramble to stay ahead of the perceived position of their competitors, the risks of reaching too far too fast and leaving operations exposed to external threats increase.

While AI allows businesses to boost the efficiency of their operations, the technology also comes with inherent risks. Business leaders across the globe must contend with a host of potential harms created by this technology and keep up with the rapid pace of innovation.

Investment into generative AI hit US$25.2bn in 2023, almost eight times higher than in 2022.[9] In addition, the number of AI patents being granted each year has grown significantly since 2010, rising from under 5,000 in 2010 to over 60,000 in 2022.[10] The AI explosion is well and truly underway.

68%

of the **executives** we surveyed believe that AI will lead to job losses in their company.[I]

Research has found that 79% of business leaders have used generative AI in some capacity, with 22% using it on a regular basis.[11] Combined with our research, which found that a quarter (25%) of global business leaders surveyed plan to invest in new technologies such as AI this year, it is clear that AI is already vital to the operations of many businesses across the globe. With 60% of jobs in advanced economies exposed to AI,[12] the technology is set to have a transformative impact on societies across the globe.

Friend?

The technology can automate time-consuming admin tasks like data processing, along with more high-level tasks such as content drafting. While large language models are still in their infancy, many business leaders are already evaluating the immense possibilities this technology presents for innovation in their business.

Foe?

However, businesses should not underestimate the potential threats posed by AI-powered platforms. For example, when using AI to draft content, businesses risk becoming embroiled in disputes around intellectual property and copyright. Failing to consider the risks associated with the rise of AI-powered platforms can place a business at risk of serious repercussions.

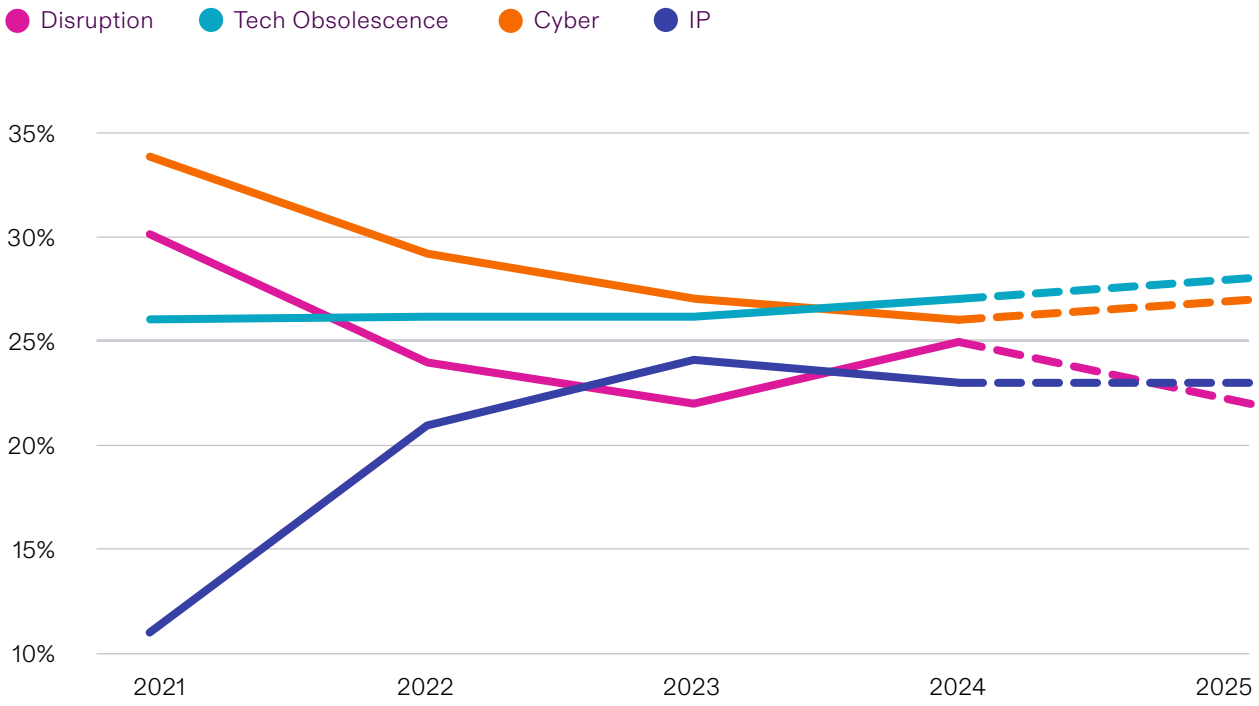
As AI and machine learning become mainstream and quickly render existing technologies out of date, the tech obsolescence risk heightens, as does the cost of maintaining legacy systems. Businesses may also have to navigate complex integrations of new technologies with their existing systems, which in turn can create cyber risk.

> “Given the continuous pipeline of innovation, tech obsolescence risk will become increasingly difficult for businesses to navigate in the coming years. However, while AI technology is still developing, authenticity is already proving to be a significant challenge. The versatility of the technology lends it to a host of applications, such as disinformation campaigns, which businesses must be prepared to counter.”

Melissa Collins
Cyber & Technology Claims Focus Group Leader, Beazley

Watch the video

Tech obsolescence risk leads the cyber & tech risk ranking



Percentage of global business executives ranking technology risks as their top risk over time[VII]

Continual technological innovation leaves business leaders on the backfoot

The wide array of threats that businesses face following the rise of AI, from intellectual property and copyright risks to tech obsolescence, are doubly concerning when considering how the technology is still in its infancy. As AI and machine learning become mainstream, the fast-paced nature of innovation and shortened development cycle of new technology will quickly render existing technologies out of date. As a result, these innovations heighten the tech obsolescence risk for businesses, who are under increasing pressure to adapt.

With tech innovation increasing, and shortening the lifespan of existing technologies, businesses will need to upgrade their systems on a more regular basis. This will leave them navigating complex integrations and plugging gaps within their existing systems. Firms hoping to realise efficiency gains and keep pace with competitors may find that new technology is not compatible with legacy systems. As a result, upgrading systems to support new interfaces could be costly and time-intensive, as well as expose them to more risk.

With over a quarter (27%) of global business leaders surveyed citing tech obsolescence risk as the biggest threat they face this year, and with 28% expecting that threat to continue in 2025, businesses recognise that the speed of innovation within this space poses a significant threat. Businesses know AI will have an impact on their operations, with 68% believing that it will lead to jobs being replaced in their company.[I] They also lack resilience, with almost a quarter (24%) feeling unprepared[III] to deal with technological developments.

New tech – new risks

As business leaders rush to adopt AI, they are likely to become more vulnerable to external threats and needing to navigate a host of new risks.

For example, it is unclear whether the written content produced by generative AI programmes such as ChatGPT is governed by existing copyright legislation. This lack of clarity has led to several high-profile legal disputes, such as comedian Sarah Silverman's suit against OpenAI and Meta, alleging various copyright infringements, including vicarious copyright infringement, unfair competition and unjust enrichment.[13] While the a Federal District Judge dismissed a number of the claims in November 2023, the central theory of copyright infringement, i.e., that the use of books to train AI systems, is copyright infringement, was not dismissed.[14]

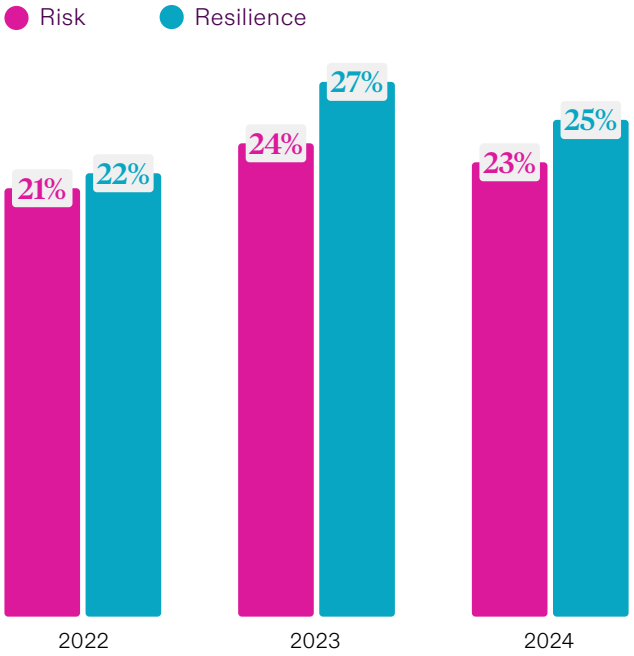
These risks run deeper than the news media and are increasingly common in other content-reliant industries such as the music industry. Numerous artists have asserted a copyright infringement lawsuit against Stability AI, Midjourney and other companies, accusing them of misusing visual artists' work to train their artificial intelligence-based image generation systems. The artists have argued that Stability, Midjourney, DeviantArt and Runway AI copied and stored their work on company servers and could be liable for using it without permission.[15]

These disputes form part of a wider debate surrounding AI tools, where developers have come under fire for a lack of transparency. The Foundation Model Transparency Index, published in May 2024, concluded that a number of foundation model developers such as OpenAI and Google lack transparency.[16] This primarily concerns the disclosure of training data and methodologies.

Amid this backdrop, where businesses utilising generative AI face a growing risk of class actions, it is perhaps unsurprising that business leaders are placing growing emphasis on intellectual property (IP) risks.

Our data found that concern around IP is growing among global business leaders, rising from just 11% in 2021,[IV] to 23% in 2024.[VII] Concerningly, a quarter (25%) of business leaders surveyed feel unprepared to counter this threat.[III]

Concern around intellectual property risk continues along its upward trajectory



Percentage of global business executives surveyed ranking the intellectual property risk as their top risk and feeling unprepared against the intellectual property risk over time[VII]

Travelling at the speed of light

The advent of new technologies continues at an unprecedented pace – hardly giving businesses time to absorb and adopt one new 'transformative' technology before another comes along.

For example, AI Agents are on the horizon - software programs that humans can instruct to perform routine tasks.[17] AI Agents could be entrusted with a business' payment details to perform transactions for example, and have the potential to bring about seismic societal change. However, it comes with inherent risks.

While it can be tempting to rush to adopt new 'transformative' technology to gain a competitive advantage, businesses need to adopt a robust risk mitigation strategy and perform diligent horizon scanning when adopting new technology.

42%

of **business leaders** surveyed said they currently operate in a high-risk environment.

While early adopters can benefit, the nature of new technology represents an unknown quantity, and the risks it poses are often not fully understood until widespread adoption occurs. For example, while AI Agents are likely to boost productivity and complete admin tasks for businesses, they could also be used by hackers to access systems or even negotiate with victims. Last summer also saw the advent of WormGPT on the dark web, used by hackers to perfect their phishing emails.[18]

Naturally, regulation is passed in response to technological innovations, with the EU AI Act being a case in point. As a result, the emphasis lies with business leaders to assess the risks of new technologies in the first instance and take appropriate measures to protect themselves. Amid a backdrop of fast-paced innovation and increasingly complex technology, managing resilience is becoming a significant challenge for businesses.

> "The AI explosion is well underway across the globe, exposing businesses to a host of novel threats. AI has lowered the barriers to entry for a new generation of hackers. It offers them a pathway to generating revenue from fraud, then graduating to more sophisticated cyber intrusion. In a competitive, fast paced industry, AI developers sometimes have a propensity to overlook vulnerabilities before bringing products to market. Businesses must be cautious when adopting new technologies, making the need for a robust risk mitigation strategy - and selection of products which are secure-by-design - greater than ever."

Alex Creswell OBE
Strategic Adviser
Beazley

Regulatory Landscape – Fit for Purpose?

What happens when technological innovation outpaces the ability of regulators to keep up?

Regulatory Landscape - Fit for Purpose?

What happens when technological innovation outpaces the ability of regulators to keep up? This phenomenon is known as 'the pacing problem,' and regulators around the world are flagging. However, there are signs that they are getting a second wind. For businesses, the AI and technology advancements on which many have staked the next stages of their growth may soon face a host of new red tape.

The pace of technological advancement has been breathtaking. New innovations appear, come on stream, and are adopted with increasing speed. For businesses that can quickly integrate new software, there is the potential and promise of commercial advantage. From new climate tech to game-changing advances in medical technology, we have seen the power of groundbreaking developments and how they quickly move into our everyday lives. However, there is an increasing awareness of the rising risks and potential harms of easy, unfettered access to these tools.

27%

of **business leaders** surveyed are most worried about their ability to keep up with technology market shifts.

For governments and regulators, innovations present new challenges. How can they encourage innovation and investment while balancing their duty to safeguard consumers and society from the risks presented by new tech? How can they keep up with the speed of innovations when the product development cycle continues to shorten?

In the UK, last year, the Online Safety Act was passed by Parliament to protect children from online harm, while empowering adults with more choices over what their children see online.[19] In the US, the American Privacy Rights Act has been introduced to Congress by a bi-partisan group to regulate high-impact social media companies and large data holders on data privacy.[20] In March this year, the EU implemented the Digital Markets Act which enables greater oversight of Core Platform Services and Big Tech firms such as Meta, Google, and Microsoft.[21] All of this new red tape demonstrates an increasingly proactive stance of legislators when it comes to tech regulation and creating safeguards for society. The result? Scrutiny of activity is intensifying.

> "Privacy and data risks have been a significant challenge for businesses in recent years with concerns around consent. The US federal government is currently looking to legislate in this space to create standardised rules for data collection and sharing. There is a high likelihood of this passing in Congress at some point in future, leading to a step change in data handling."

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

The eye of the storm

Tech firms are increasingly finding themselves in the eye of the storm amidst growing geopolitical tension. The World Economic Forum previously noted that AI, blockchain and 5G capabilities have quickly become the 'frontlines of either global competition or coordination' as tech becomes an important battleground for global superpowers. We saw this in 2019 when the Trump administration blacklisted telecoms firm Huawei from the US after security concerns over spying.[22]

Since then, the China-US tech war has evolved considerably. In April this year, President Joe Biden signed a new law that gives ByteDance, the Chinese owner of TikTok, nine months to divest its stake in the social media app or face a ban in the US.[23] The law further bans Apple, Google and others from offering access to the app unless the sale takes place. The decision is currently being contested by ByteDance in the US but reflects the growing role of sanctions on tech firms around the world.

Examples like this highlight how firms and technology service providers can find themselves as chess pieces in the geopolitical landscape. For businesses that rely on components of their technology stack from sanctioned countries and businesses, they will likely experience disruption and additional costs as they look for alternative solutions.

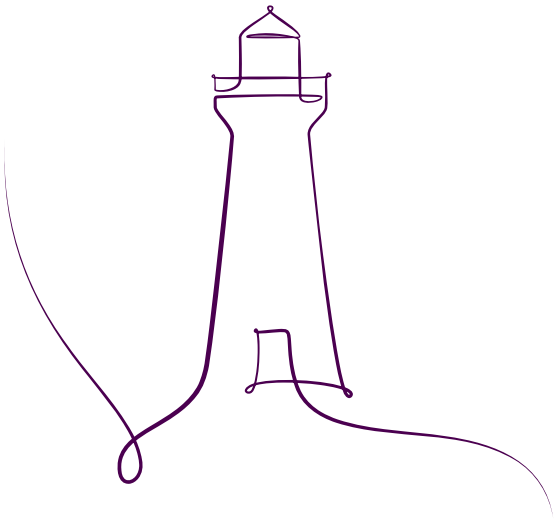
One area in particular that is experiencing an uplift in regulatory activity is in the realm of AI as policymakers try to get a grip on the technology. Italy was the first Western country to block the use of ChatGPT in April 2023 following concerns around data privacy.[24] While Italy has since reinstated ChatGPT, the country's Data Protection Authority found in 2024 data privacy violations on the platform and is investigating OpenAI and its new AI model, 'Sora'.[25] Simultaneously, in the US, legislators have increasingly zoned in on AI, with Sam Altman, CEO of OpenAI, previously testifying in front of Congress on AI risks in March 2023.[26] Since then, President Biden's White House has published an Executive Order on the development and usage of AI tools.[27]

As innovations, such as voice-AI, emerge every month and legislators grapple with the longer-term effects of AI, they are finding it hard to keep pace with the speed of technology developments and uses. For now, it remains unclear how AI regulation will evolve and be formed across legislators. While regulation remains in its early stages and is only coming into law in certain jurisdictions, the consequences for businesses who fail to adhere to or keep abreast of new rules and regulations could be costly.

Stuck in the middle

Every business, no matter its size or the sector, is likely to be exposed to new regulations and policy decision-making in the years ahead. For companies operating in multiple locations, the challenge becomes more acute as countries and regulators diverge on their approach. The lack of uniformity in tech regulation means that business leaders need to be aware of new regulations, rules and frameworks in different countries and how these initiatives can impact their operations and personnel on the ground.

Failure to comply with new rules can lead to costly fines from regulators, hampering the growth ambitions of firms, and harm their reputation. This results in a heightened risk for directors & officers who might not be aware of new regulations and the potential impact on their businesses. To stay ahead, ultimately, boardrooms need to anticipate new requirements and understand the associated risks of any new regulation. By doing so, companies can minimise the risk of potential exposures and remain one step ahead.



The Role of Insurance

In the face of an ever-evolving threat landscape, insurance can provide businesses with a vital safety net to help reassure investors and employees. Our research shows that 47% of global executives surveyed said their trust in insurers has increased, and 24% are seeking to explore insurance options that include crisis and risk management services.

Clearly, the insurance industry has a vital role to play. By leveraging claims, incident data, and threat information data and insight and translating this into actionable guidance to help elevate resilience for a range of cyber and tech risks, we can help our clients to better mitigate risk.

Today, in this era of escalating threats, effective risk management requires cutting edge security expertise, and the latest risk insights – fast. However, being reactive is no longer enough. Businesses must build a living and breathing cyber ecosystem, a long-term risk management strategy that seeks to pre-empt the risks, adapt risk mitigation strategies as risks morph and evolve, and considers how they will react and cope in the face of an incident.

The risk of tech obsolescence, tech disruption and IP risk are all rising up global executives' risk agendas as the speed of digitalisation continues at pace. These risks, along with cyber risk, have the propensity to spill over into other areas of risk – such as directors' & officers' liability. With cyber and tech risk touching every aspect of a business today, making the right risk mitigation choices, and having the right long-term, insurance partners on side, has never been more important.

Insurers and brokers must continue to build long-term partnerships with clients, engaging and educating businesses on the threats that cyber crime and new technologies pose, while sharing their expertise on best practice resilience and defence strategies.

By boosting their cyber resilience, and by working in partnership with their insurer, businesses can not only reduce the risk of being attacked, but they can also increase their ability to respond to an incident more effectively.

47%

of **global executives'** trust in insurers has increased.

24%

of **global businesses** are seeking to explore insurance options with crisis and risk management services.

> **"With the sophistication of the cyber attack environment, it is surprising that only around 1 in 10 (11%) of the global business leaders we surveyed believe that they do not have adequate cyber provisions in place to defend against a cyber attack today. Now is not the time to become complacent. Having adaptive defence in depth cyber strategies in place and working closely with cyber security experts and insurers has never been more important."**

Melissa Carmichael
Head of Cyber Risk US
Beazley

Watch the video

Methodology

About the Risk & Resilience research

During January 2024, we commissioned research company Opinion Matters to survey the opinions of over 3,500 business leaders and insurance buyers of businesses based in the UK, US, Canada, Singapore, France, Germany and Spain 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.
- **Geopolitical** – including strikes and civil disruption, changes in legislation and regulation, economic uncertainty, inflation and war & terror.
- **Business** – including supply chain instability, business interruption, boardroom risk, crime, reputational and employer risk and failure to comply with ESG regulations and reporting requirements.
- **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: US$250,000 - US$999,999, US$1m - US$9.99m, US$10m - US$99.99m, US$100m- US$999.99m, US$1 billion plus.

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

This year's survey was undertaken between 05.01.24 and 15.01.24. In 2021 the survey was undertaken with respondents based in the UK and US. In 2022 and 2023 the sample base also included respondents based in Canada and Singapore and, in 2024 the sample base was expanded to include respondents in France, Germany and Spain.

Contributors

Marcello Antonucci
Claims Team Leader – Cyber & Tech Risks, Beazley

Paul Bantick
Group Head of Cyber Risks, Beazley

Melissa Carmichael
Head of Cyber Risk US, Beazley

Melissa Collins
Cyber & Technology Claims Focus Group Leader, Beazley

Alex Creswell OBE
Strategic Adviser, Beazley

Francisco Donoso
Chief Technology Officer, Beazley Security

Katherine Heaton
Claims Focus Group Leader – Cyber Services & InfoSec Claims, Beazley

Alton Kizziah
CEO, Beazley Security

Patricia Kocsondy
Head of Global Cyber Digital Risks, Beazley

Christian Taube
VP Cyber Services – International, Beazley Security

Bobby Venal
Labs Principal Researcher, Beazley Security

Bob Wice
Head of Underwriting Management, Cyber Risks, Beazley

References

1. Forbes: https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/?sh=2633e3ce3b0c
2. https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
3. Critical US Companies Legally Required To Report Cyberattacks (tech.co)
4. https://www.theguardian.com/world/2024/feb/05/hong-kong-company-deepfake-video-conference-call-scam
5. https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video
6. https://www.theguardian.com/world/2024/feb/05/hong-kong-company-deepfake-video-conference-call-scam
7. https://www.ft.com/content/308c42af-2bf8-47e4-a360-517d5391b0b0
8. https://www.scmagazine.com/news/lastpass-thwarts-attempt-to-deceive-employee-with-deepfake-audio
9. AI Index Report 2024 – Artificial Intelligence Index (stanford.edu)
10. AI Index Report 2024 – Artificial Intelligence Index (stanford.edu)
11. The state of AI in 2023: Generative AI's breakout year | McKinsey
12. Gen-AI: Artificial Intelligence and the Future of Work (imf.org)
13. These Are The High-Stakes AI Legal Battles To Watch In 2024 - Law360
14. These Are The High-Stakes AI Legal Battles To Watch In 2024 - Law360
15. Stability AI, Midjourney should face artists' copyright case, judge says | Reuters
16. Stanford CRFM
17. What are AI Agents?- Agents in Artificial Intelligence Explained - AWS (amazon.com)
18. What is Worm GPT? The new AI behind the recent wave of cyberattacks | Dazed (dazeddigital.com)
19. UK Government | May 2024
20. Global Treasurer | May 2024
21. Herbert Smith Freehills | March 2024
22. Bloomberg | April 2024
23. Reuters | May 2024
24. BBC | April 2023
25. Data Guidance | March 2024
26. CNN | May 2023
27. White House | October 2023

Footnotes

I. 'Somewhat agree' and 'Strongly agree' answers combined.

II. 'Moderately prepared' and 'Very prepared' answers combined.

III. 'Not very well prepared' and 'Not at all prepared' answers combined.

IV. This figure is based on research undertaken in January and February in 2021 with 1,000 executives of firms based in the UK and US of varying sizes, operating in 10 broad industry sectors with international operations.

V. This figure is based on research undertaken in January 2022 with 2,000 executives of firms based in the UK, US, Canada and Singapore of varying sizes, operating in 10 broad industry sectors with international operations.

VI. The 2023 research was undertaken in January 2023 with 2,000 executives based in the UK, US, Canada and Singapore of varying sizes, operating in 9 broad industry sectors with international operations.

VII. This year's survey was undertaken between 05.01.2024 and 15.01.2024 with 3,500 executives based in the UK, US, Canada, Singapore, France, Germany and Spain of varying sizes, operating in 9 broad industry sectors with international operations.

Discover more
beazley.com

Beazley plc (BEZ.L) is the parent company of specialist insurance businesses with operations in Europe, United States, Canada, Latin America and Asia. Beazley manages seven Lloyd's syndicates and, in 2023, underwrote gross premiums worldwide of $5,601.4m. All Lloyd's syndicates are rated A by A.M. Best.

Beazley's underwriters in the United States focus on writing a range of specialist insurance products. In the admitted market, coverage is provided by Beazley Insurance Company, Inc., an A.M. Best A rated carrier licensed in all 50 states. In the surplus lines market, coverage is provided by Beazley Excess and Surplus Insurance, Inc. and the Beazley syndicates at Lloyd's. Beazley's European insurance company, Beazley Insurance dac, is regulated by the Central Bank of Ireland and is A rated by A.M. Best and A+ by Fitch.

Beazley is a market leader in many of its chosen lines, which include professional indemnity, cyber, property, marine, reinsurance, accident and life, and political risks and contingency business.

For more information, please go to: beazley.com

BZCBR119

beazley security

About Beazley Security and Full Spectrum Cyber

Beazley Security is a global cyber security firm committed to helping clients develop true cyber resilience. By combining decades of cyber security protection, detection, response, and recovery expertise with the insurance precision, award winning claims and risk mitigation capability of Beazley Insurance, to offer a unique cyber ecosystem that is always pre-emptive, responsive and adaptive.

Discover more at beazley.security

beazley

Insurance. Just different.