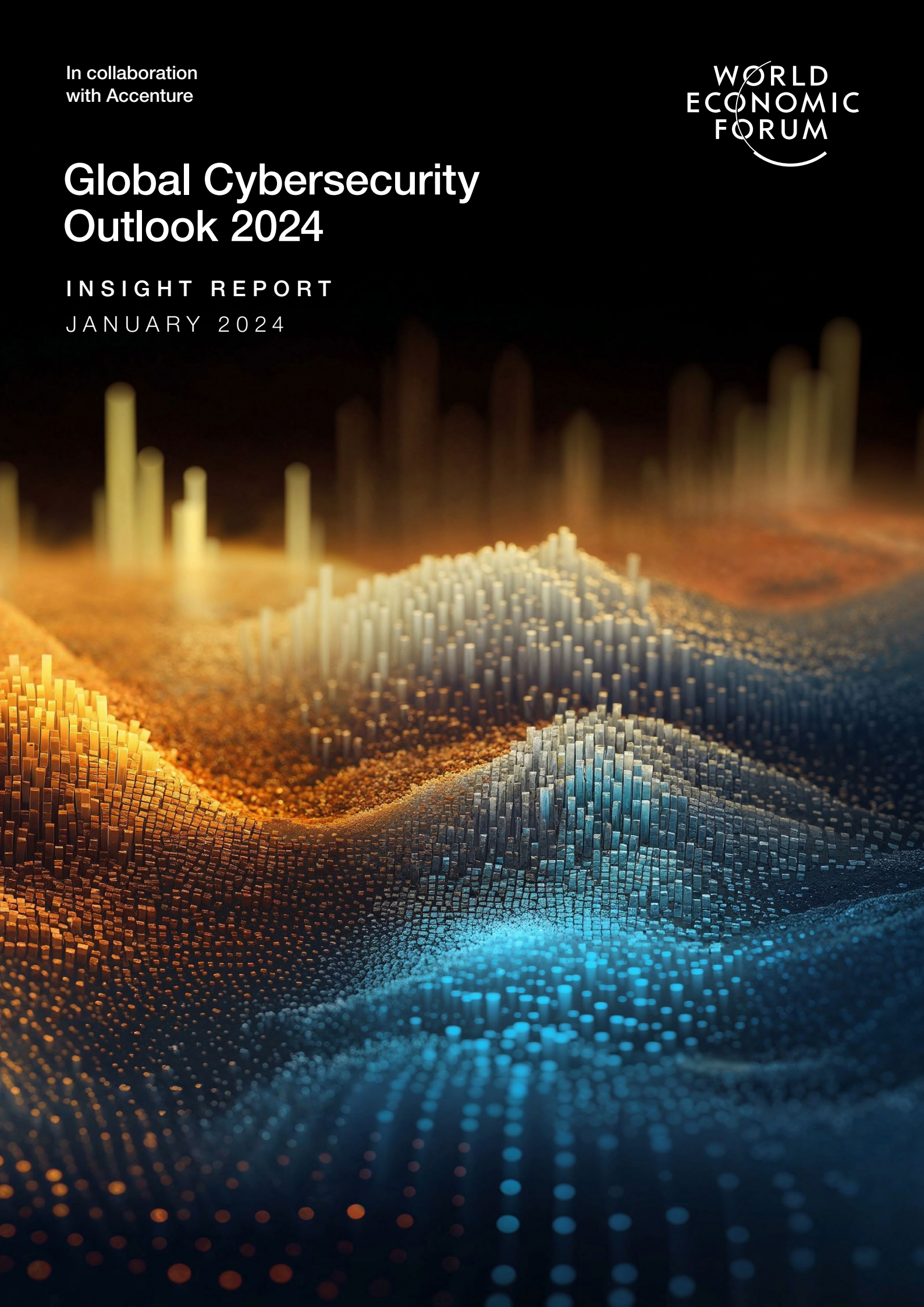
In collaboration with Accenture

WORLD ECONOMIC FORUM

Global Cybersecurity Outlook 2024

INSIGHT REPORT

JANUARY 2024



Images: Getty Images, MidJourney

Contents

Foreword

Jeremy Jurgens
Managing Director, World Economic Forum, Switzerland

Paolo Dal Cin
Global Lead, Accenture Security, Italy

In the ever-evolving landscape of cybersecurity, this year's Global Cybersecurity Outlook provides crucial insights into the multifaceted challenges facing leaders across the globe. Geopolitical instability, rapidly advancing technologies and an increasing gap in organizational cyber capabilities reinforce the need to build resilience and enable systemic global collaboration.

Building on the priorities outlined in last year's report, the World Economic Forum's Centre for Cybersecurity remains committed to bridging the gaps between the public and private sectors and between cyber and business leaders. The report serves as an instrument to distil cyber-risk issues into achievable insights tailored to today's executives.

While there is a notable sense of optimism stemming from increased executive-level awareness of the cybersecurity ecosystem and its risks, the report also underscores a growing cyber divide. Organizations demonstrating cyber resilience are increasingly distinct from those grappling with cybersecurity challenges. The dialogue between cyber and business executives has shown improvement, yet significant disparities persist among industries, countries and sectors, demanding continued attention and collaboration.

Looking ahead to the challenges of 2024, the report illuminates major findings and puts a spotlight on the widening cyber inequity and the profound impact of emerging technologies. The path forward demands strategic thinking, concerted action and a steadfast commitment to cyber resilience.

This report invites leaders not only to recognize the hurdles but also to actively embrace the opportunities for positive change. It is a call for collective effort and innovation, urging leaders to work collaboratively towards a more secure, resilient and trustworthy digital future.

Executive summary

Looming cyber inequity amid a rapidly evolving tech landscape emphasizes the need for even greater public-private cooperation.

In 2023 the world faced a polarized geopolitical order, multiple armed conflicts, both scepticism and fervour about the implications of future technologies, and global economic uncertainty. Amid this complex landscape, the cybersecurity economy[1] grew exponentially faster than the overall global economy, and outpaced growth in the tech sector.[2] However, many organizations and countries experienced that growth in exceptionally different ways.

A stark divide between cyber-resilient organizations and those that are struggling has emerged. This clear divergence in cyber equity is exacerbated by the contours of the threat landscape, macroeconomic trends, industry regulation and early adoption of paradigm-shifting technology by some organizations. Other clear barriers, including the rising cost of access to innovative cyber services, tools, skills and expertise, continue to influence the ability of the global ecosystem to build a more secure cyberspace in the face of myriad transitions.

These factors are also ever-present in the accelerated disappearance of a healthy "middle grouping" of organizations (i.e. those that maintain minimum standards of cyber resilience only). Despite this divide, many organizations indicate clear progress in certain aspects of their cyber capability. This year's outlook also finds cause for optimism, especially when considering the relationship between cyber and business executives.

These are the major findings from this year's Global Cybersecurity Outlook and the key cyber trends that executives will need to navigate in 2024:

There is growing cyber inequity between organizations that are cyber resilient and those that are not.

In parallel, the population of organizations that maintain a minimum level of cyber resilience is disappearing. Small and medium enterprises (SMEs),[3] despite making up the majority of many country's ecosystems, are being disproportionately affected by this disparity.

- The number of organizations that maintain minimum viable cyber resilience is down 30%. While large organizations demonstrated remarkable gains in cyber resilience, SMEs showed a significant decline.
- More than twice as many SMEs as the largest organizations say they lack the cyber resilience to meet their critical operational requirements.
- 90% of the 120 executives surveyed at the World Economic Forum's Annual Meeting on Cybersecurity said that urgent action is required to address this growing cyber inequity.

Emerging technology will exacerbate long-standing challenges related to cyber resilience.

This will in turn accelerate the divide between the most capable and the least capable organizations.

- As organizations race to adopt new technologies, such as generative artificial intelligence (AI), a basic understanding is needed of the immediate, mid-term and long-term implications of these technologies for their cyber-resilience posture.
- Fewer than one in 10 respondents believe that in the next two years generative AI will give the advantage to defenders over attackers.
- Approximately half of executives say that advances in adversarial capabilities (phishing, malware, deepfakes) present the most concerning impact of generative AI on cyber.

The cyber-skills and talent shortage continues to widen at an alarming rate.

- Half of the smallest organizations by revenue say they either do not have or are unsure as to whether they have the skills they need to meet their cyber objectives.
- Only 15% of all organizations are optimistic that cyber skills and education will significantly improve in the next two years.
- 52% of public organizations state that a lack of resources and skills is their biggest challenge when designing for cyber resilience.

Alignment between cyber and business is becoming more common.

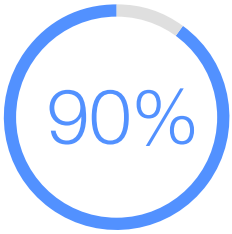
Organizations (including both business and cyber leaders)[4] must continue to invest in and maintain an awareness of essential security fundamentals.

- 29% of organizations reported that they had been materially affected by a cyber incident in the past 12 months.
- The largest organizations say that the highest barrier to cyber resilience is transforming legacy technology and processes.
- There is a clear link between cyber resilience and CEO engagement. This year, 93% of respondents that consider their organizations to be leaders and innovators in cyber resilience trust their CEO to speak externally about their cyber risk. Of organizations that are not cyber resilient, only 23% trust their CEO's ability to speak about their cyber risk.

Cyber ecosystem risk is becoming more problematic.

For any organization, the partners in its ecosystem are both the greatest asset and the biggest hindrance to a secure, resilient and trustworthy digital future.

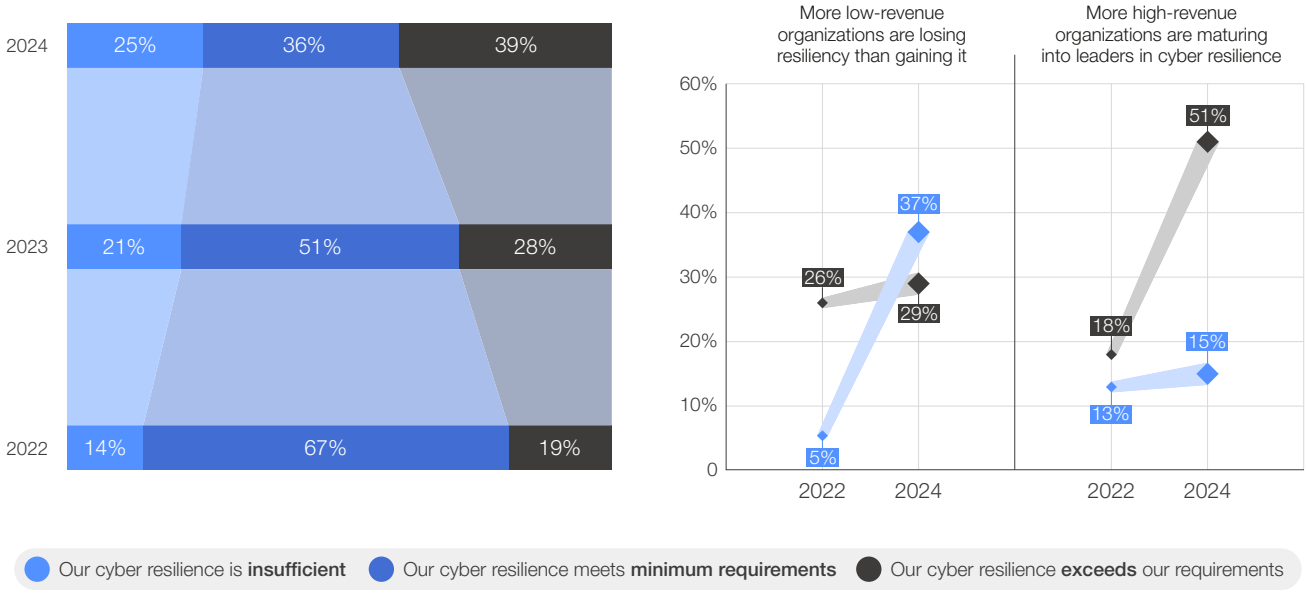
- 41% of the organizations that suffered a material incident in the past 12 months say it was caused by a third party.
- 54% of organizations have an insufficient understanding of cyber vulnerabilities in their supply chain. Even 64% of executives who believe that their organization's cyber resilience meets its minimum requirements to operate say they still have an inadequate understanding of their supply-chain cyber vulnerabilities.
- 60% of executives agree that cyber and privacy regulations effectively reduce risk in their organization's ecosystem – up 21% since 2022.



90% of cyber leaders who attended the Annual Meeting on Cybersecurity believe that inequity within the cybersecurity ecosystem requires urgent action.

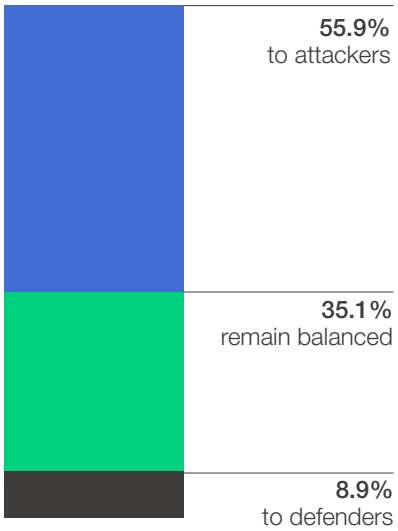
There is growing cyber inequity between organizations that are cyber resilient and those that are not

What is the state of your organization's cyber resilience this year?

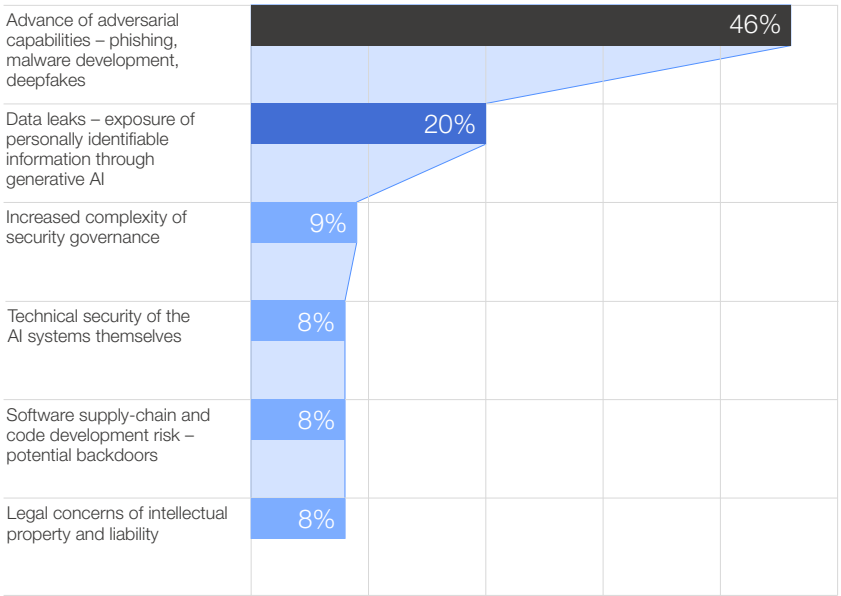


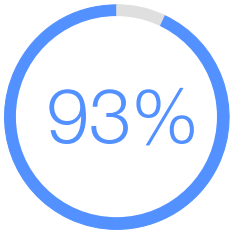
Emerging technologies will exacerbate long-standing challenges related to cyber resilience

In the next two years, will generative AI provide overall cyber advantage to attackers or defenders?



What are you most concerned about in regards to generative AI's impact on cyber?

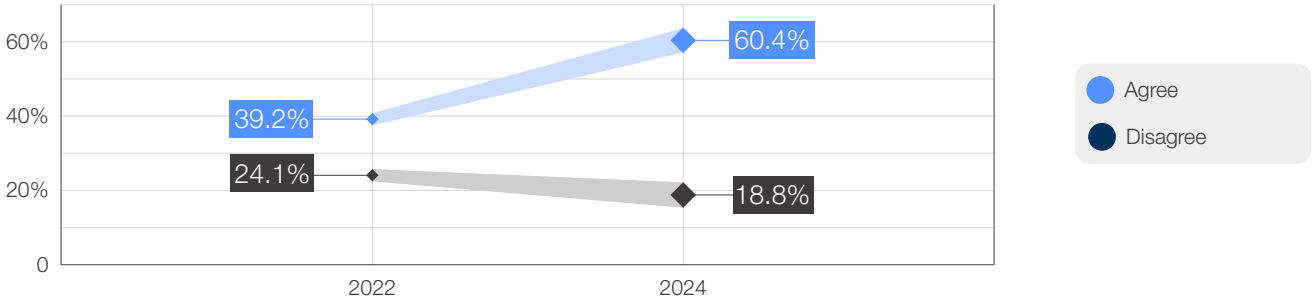




93% of leaders of organizations excelling in cyber resilience trust their CEO to speak externally about their cyber risk.

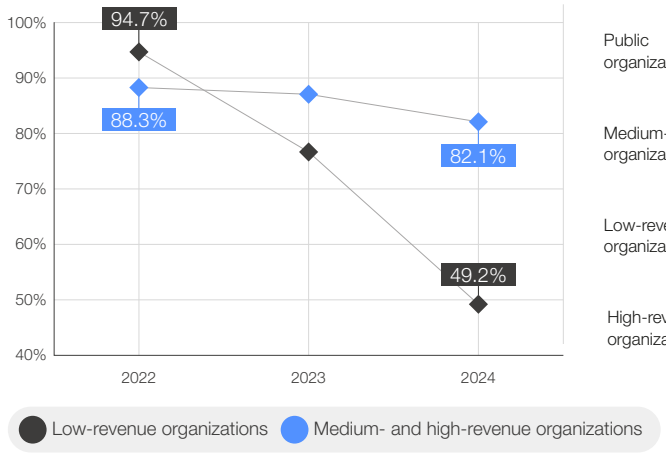
Cyber regulations are perceived to be an effective method of reducing cyber risks

Do you believe cyber and privacy regulations effectively reduce cyber risks?

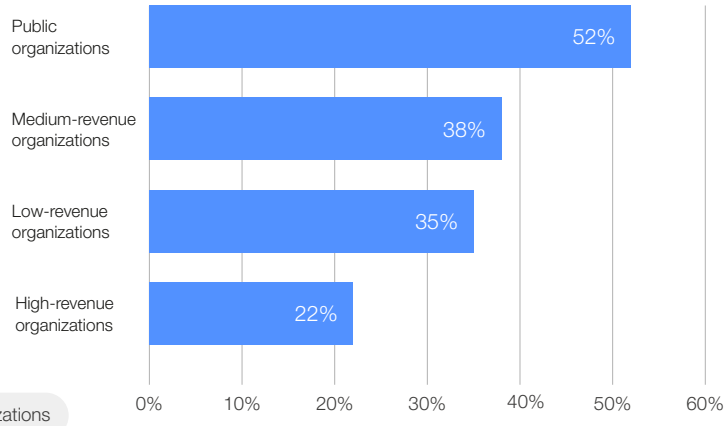


The cyber skills and talent shortage continues to widen at an alarming rate

Does your organization have the skills needed to respond to and recover from a cyberattack?

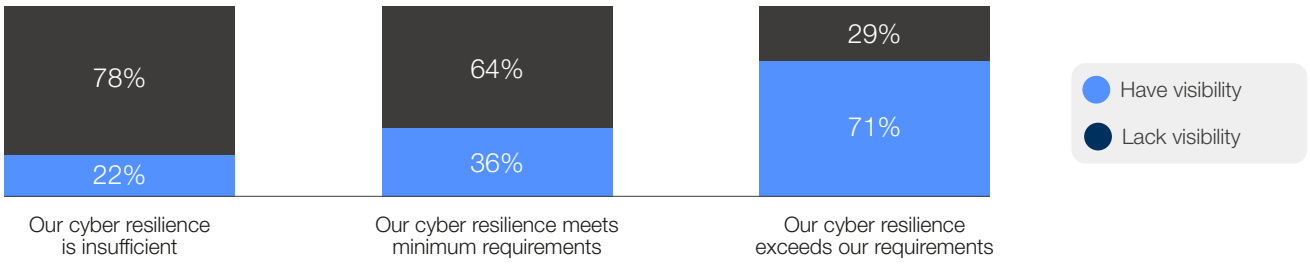


Are resources or skills gaps the biggest challenge for your organization when designing for cyber resilience?



For any organization, the partners in its ecosystem are both the greatest asset and the biggest hindrance to a secure, resilient and trustworthy digital future

Do you have visibility of your third-party risk?



1 Understanding global cyber inequity

A systemic solution is needed to address the inequity in cyber-resilience capacity across organizations and countries.

1.1 The state of cyber inequity

In 2022, the cybersecurity economy[5] grew twice as fast as the world economy.[6] In 2023, it grew four times faster. Although organizational investment in cyber resilience overall is on the rise, rapid innovation and growth often lead to uneven development.

This unevenness creates major economic and social benefits for some; generally, the largest and most developed economies reap the rewards of new technologies, while less developed nations, sectors and communities continue to fall behind. In this case, rapid technological growth, although benefiting many in terms of access, innovation and even collaboration, is also creating systemic inequity in the global cybersecurity economy and belies a pronounced disparity between the cyber-resilience capability of organizations that make up its markets.

The 2024 Global Cybersecurity Outlook (GCO) finds that organizations that maintain minimum viable cyber resilience – that is, a healthy middle grouping of organizations – are disappearing. Organizations reporting such a minimum viable cyber resilience are down 31% since 2022. The distance between organizations that are cyber resilient enough to thrive and those that are fighting to survive is widening at an alarming rate. As a result, the least capable organizations are perpetually unable to keep up with the curve, falling further behind and threatening the integrity of the entire ecosystem. The cost of accessing adequate cyber services, tools and talent, and the early adoption of cutting-edge technology by the largest organizations in the ecosystem are two core factors driving the divide.

A few statistics further illustrate the trend towards imbalance. The smallest organizations are more than twice as likely as the largest to say they lack the cyber resilience they need to meet their minimum critical operational requirements.[7] At the other end of the spectrum, the highest-revenue organizations are 22% more confident than the smallest organizations that their cyber resilience exceeds their operational needs. And yet the smallest-revenue organizations are also a troubling three times more likely to lack the cyber skills they need to meet their cyber-resilience objectives.

This phenomenon is particularly alarming in light of the interconnected nature of the cyber ecosystem. One of the core measurements of cyber resilience is an understanding of your ecosystem, inclusive of assessments of supply-chain and third-party risk. For those large organizations reporting that they are leaders in cyber resilience, the emergence of this drastic drop in cyber resilience of small organizations should be especially alarming. Consider a 2023 report from SecurityScorecard and the Cyentia Institute, which found that "98% of organizations have a relationship with at least one third party that has experienced a breach in the last two years".[8] This type of entanglement should be reason enough for those that are most cyber resilient to proactively help organizations in their ecosystem to move towards a healthier cyber posture.

Several other factors may unduly influence and exacerbate the vulnerabilities of those SMEs in this widening disparity. Among small organizations – which are often unable to prevent critical operational disruption from an incident and can incur disproportionate financial loss to recover – only 25% carry cyber insurance. That's three times less likely than the largest organizations by revenue, which report a 75% cyber-insurance adoption rate. The results are also consistent for organization size by employee count. The more employees within an organization, the higher the adoption rate of cyber insurance; 85% of organizations with more than 100,000 employees carry cyber insurance, while only 21% of organizations with 250 employees or fewer have a policy. As the prices of cyber insurance continue to rise exponentially, the expectation is that this gap will widen in parallel, leaving smaller organizations with even fewer options to reduce their risk.

FIGURE 3 **Organizations that carry cyber insurance by number of employees**

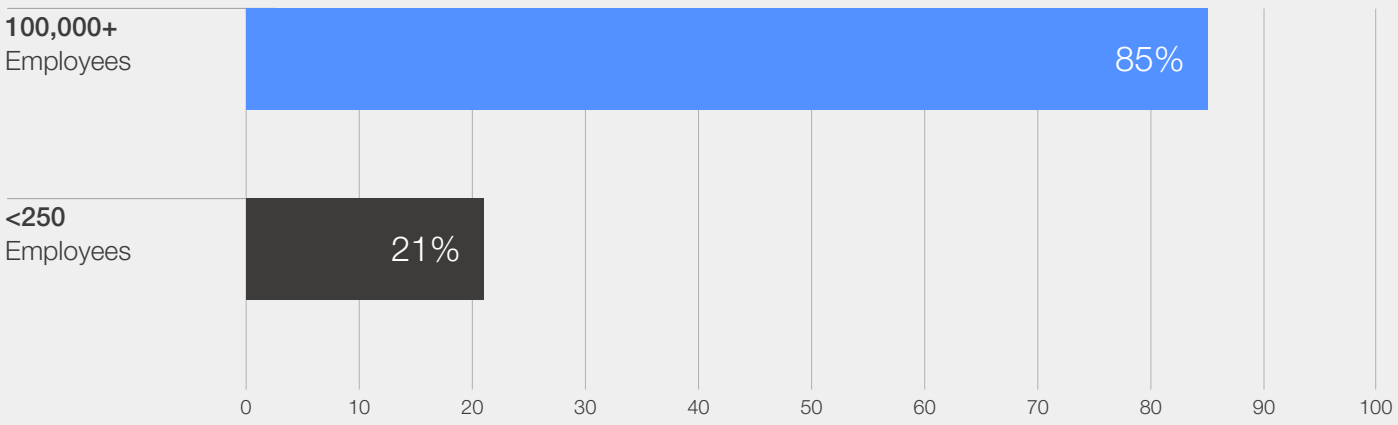
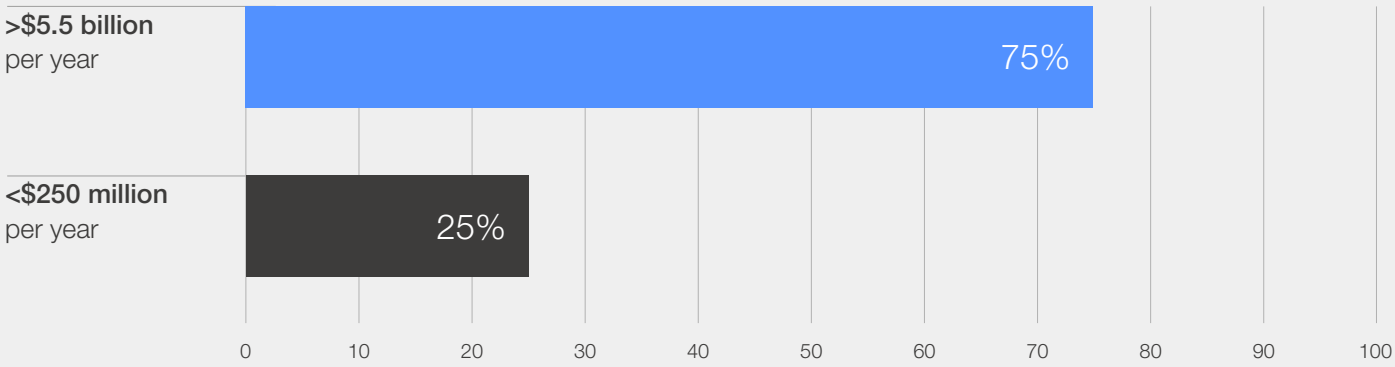


FIGURE 4 | **Organizations that carry cyber insurance by revenue**



Globally, disparity across geographies is also reflected in the analysis. Perhaps unsurprisingly, this global cyber gap tends to mirror other global development indicators. The lowest number of self-reported cyber-resilient organizations are in Latin America and Africa, while the highest number come from North America and Europe. Similarly, Latin America and Africa reported the highest number of insufficiently cyber-resilient organizations, while North America and Europe reported the lowest number.

This phenomenon, sometimes characterized as the "cybersecurity poverty line (CPL)", generally refers to the prohibitive cost of securing robust cybersecurity for an organization's personnel, technology and systems. But this divide goes far beyond prohibitive costs. Consider the cyber-skills gap, a well-documented issue for even the largest global organizations. Other factors, such as knowledgeable leaders, the ability to understand shifting best practices, and access to highly innovative technologies, also dramatically affect an organization's ability to stay ahead of the curve. As the Atlantic Council puts it, "Cyber poverty exhibits dynamics very similar to real-world poverty: simply providing money or free expertise does not necessarily address poor technological designs, poor market incentives, misaligned sociocultural attitudes towards security, or other barriers."[9]

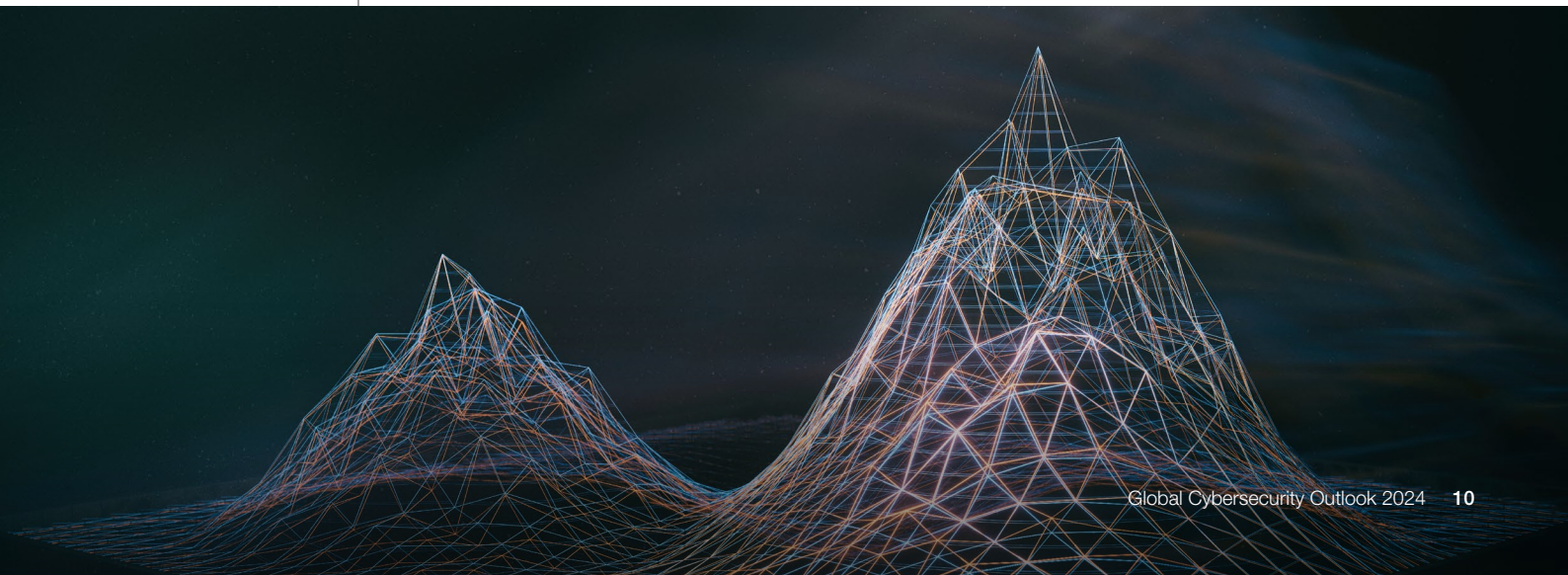
The disparity may be ultra-visible now, but it has been developing for years, and the cyber-resilience inequity trend has been steadily increasing over time. Among the lowest-revenue organizations, lack of sufficient cyber resilience is up a troubling 32% since 2022. Among the highest-revenue organizations, reported deficiencies in cyber resilience are similar to those reported two years ago.

Additionally, the number of organizations with lower revenue that reported their cyber resilience exceeds their operational requirements has not increased over the past two years. Conversely, among large-revenue organizations, cyber confidence rose 32%.

Although there are generalized economic norms indicating that this is healthy competition, cyber leaders know that the digital ecosystem is so intertwined and fragile that to continue on this trajectory is more harmful than healthy.

When asked to comment on this disappearing middle grouping of organizations, Rotem Iram, Chief Executive Officer of At-Bay, neatly summed it up in this way:

> **Security solutions are becoming too sophisticated, to the point where many SMEs struggle to operate them, let alone afford them.**



1.2 Core drivers of cyber inequity

Organizations of all sizes and maturity levels have often struggled to maintain central tenets of organizational cyber resilience. Historically, however, several factors began to stratify the cyber capability of both public- and private-sector organizations. Some organizations prioritized resilience, incorporated it into corporate culture and invested accordingly, while others did not. Some sectors more strictly regulated their members – for example, out of concern for human safety or national security, to safeguard personally protected information, or to protect the global financial system. Other organizations were forced to contend with a more hostile threat landscape and suffered a significant, often public incident.

Over time, differences in organizational, sectoral and country-specific circumstances, as well as varied responses to universal cyber challenges, separated the market into clear leaders and stragglers. Add to the equation the pace of the rising cost of access to adequate cybersecurity capability and what results is the current state of cyber inequity between small and large organizations, between the public and private sectors, and among organizations operating in different economies around the world.

The digital divide in access to the internet provides a useful parallel. Consider the comment from Angel Gonzalez Sanz, Head of Science, Technology and Innovation in the Division on Technology and Logistics of the United Nations Conference on Trade and Development (UNCTAD), that, "although 63% of the world's population is connected to the internet; least developed countries still only count 27% of their populations as internet users".[10] The digital ecosystem is so highly interconnected and influenced by geopolitics, economics and the rapid emergence of new technology that no entity can afford to be perpetually trapped under the capability curve, least of all the organizations that are already the most at risk.

As Abhay Raman, Senior Vice-President and Chief Security Officer at Sun Life, put it:

> **Affordability is a critical determinant of cyber-resilience success. We should therefore design risk-appropriate, affordable and fit-for-use cyber-resilience architectures for large multinationals and SMEs alike.**

The risks associated with continuing to exacerbate this technological divide between organizations and nations that can and cannot adequately mitigate cyber events poses both a threat to the entire ecosystem and outsized risks to those that are already vulnerable. The imbalance in global internet access presents a prescient example of the consequences of sustaining an unequal digital ecosystem.

Doing so requires a systemic solution, with participation from everyone – SMEs, multinational corporations (MNCs), non-governmental organizations (NGOs) and governmental organizations. Fortunately, cyber executives agree: 90% of the 120 executives surveyed at the World Economic Forum's Annual Meeting on Cybersecurity said that urgent action is required to address this growing cyber inequity. There is evidence of an appetite for systemic collaboration that supports SMEs. For example, in 2020, the World Economic Forum brought together partners from telecommunication companies, civil society and cyber organizations to publish cybercrime prevention principles for internet services providers. This is an example of systemically important actors such as internet service providers working to protect the entire ecosystem, including smaller players.[11]

2

A world in geopolitical and technological transition

The rapid spread of generative AI and other new technologies that can easily be used by cyberattackers poses a serious threat both for business and in public life.

2.1 Geopolitical tensions and cyber

In this year's Global Cybersecurity Outlook survey, 70% of leaders stated that geopolitics has at least moderately influenced their organization's cybersecurity strategy. The influence of geopolitics has remained as persistently top of mind as it was last year, with 74% of respondents from the 2023 report stating the same. This year, 32% of 37 CISOs surveyed separately said they are adjusting their cybersecurity strategy by increasing the use of threat intelligence reports and further developing their incident response plans. Increasingly alarming attacks against critical infrastructure, and elements in global supply chains, coupled with economic instability, have the potential to cause macro-impact.

Geopolitics also directly influences how quickly the risk landscape can shift for an organization or country. Some 72% of leaders report that they understand this rapidly shifting landscape and are actively integrating current events into how they manage their cyber risks.

Just as cybersecurity breaches weaken our faith in the systems that underpin economies and societies, other technological risks, such as disinformation, can do the same. Often the same defenders are called upon to help combat both. A key example of this is how public- and private-sector organizations alike are reevaluating both the vulnerabilities of specific institutions and processes, such as elections, in the face of intense geopolitical strife, and increased technological capability.

An example of the intersection of geopolitical turmoil and artificial intelligence, deepfakes and sophisticated phishing campaigns have the potential to become weaponized to disrupt democratic election procedures. Although information warfare is not a new concept, the decentralization of information sources, and the rapid advance of technology, makes defending against these types of malicious threats a key concern in the coming year and beyond.

Looking ahead to 2024, these risks will compound to take centre stage. More than 45 countries will hold elections over the next year to determine who governs more than 50% of the world's GDP.[12] With the proliferation of new technologies such as generative AI and their use by cyber adversaries becoming more widespread, safeguarding the integrity and fairness of the electoral process becomes of paramount importance.

In Slovakia's September 2023 elections, for instance, a deepfake audio clip was released that purported to show a candidate discussing how to manipulate the election with a media representative.[13]

Artificial intelligence advances pose more risks than deepfakes or misinformation. To understand the intersection of cyber and election security,[14] there are six areas of risk that should be noted as next year's elections unfold.

- **Misinformation and disinformation:** organized campaigns spreading misinformation through social media or other channels can influence public opinion, cast doubt on election integrity and sway election outcomes.
- **Deepfakes:** in this specific species of disinformation, AI-generated deepfake videos or audio recordings can be used to spread false information about candidates or manipulate public perception.
- **Automated disinformation:** AI algorithms can be employed to generate and spread large volumes of disinformation, making it harder to detect and combat.
- **Targeted advertising:** AI-driven microtargeting of mis- or disinformation of voters through personalized advertisements can be used to manipulate opinions or suppress voter turnout.
- **Data privacy concerns:** where voting information is drawn from national ID, residence records or other methods that connect to personally identifiable information (PII), automated processing may create avenues for the leakage of personal data not relevant to voting eligibility determinations.
- **Algorithmic manipulation of social media:** AI algorithms on social media platforms can be manipulated to amplify certain political messages or suppress others, influencing public opinion.

It is worth noting that while generative AI will add to the complexity of attacks, it is not the only concern in relation to the rise in cybercriminal activity due to geopolitical tensions. Over the past five years, the number of malware families[15] and variants that have infiltrated at least 10% of global organizations has doubled.[16]

Cyberthreats to the electoral process are just one example of how the confluence of emerging tech, cyber and geopolitics might demand global attention in the coming year. A collaborative approach ensures a multipronged defence strategy, fortifying the overall resilience of election systems against a diverse spectrum of cyberthreats.

2.2 New technology, same fear

Emerging technology is becoming available more widely and far faster than in the past. This rapid uptake of technologies has outpaced the ability of civil society, regulators and organizations to truly implement safety and security principles. Furthermore, to responsibly implement leading-edge technology, it is critical to reinforce the underlying systems required to support it. Otherwise, organizations will likely allow deficits in fundamental security, resilience and trust to be exacerbated.

The 2024 Global Cyber Outlook findings indicate that organizations are paying attention and reacting quickly to mitigate the risks of adopting emerging technology. The meteoric rise of large language models (LLMs) and generative AI over the past 12 months is a key example. Although quantum technologies may be temporary eclipsed by the zeal surrounding generative AI, it is still on the minds of respondents as a matter to be addressed. In one way, quantum is making its way back to the forefront; in November 2023, the United States was working to instate the National Quantum Initiative Reauthorization Act.[17]

In the 2022 Global Cybersecurity Outlook,[18] approximately half of leaders said that automation and machine learning would have the greatest influence on cybersecurity in the following two years. Nearly two years later, executives still feel the same – this year, approximately half of leaders still agree that generative AI will have the most significant impact on cybersecurity in the next two years. Industries such as cybersecurity (65%), agriculture (63%), banking (56%) and insurance (56%) all had the largest percentages of leaders choosing generative AI as the biggest influence on cybersecurity.

TABLE 1 **Sectors that leaders perceive will be affected by generative AI, with percentages, and perceived resilience**

Industry	Percentage of leaders who think generative AI will most significantly affect cybersecurity in the next two years	Percentage of leaders who think their organizations are at least minimally cyber resilient
Cybersecurity	65%	94%
Agriculture, food and beverage	63%	38%
Banking and capital markets	56%	68%
Insurance and asset management	56%	89%
Professional services	53%	69%
Information technology and telecommunications	52%	81%
Health and healthcare and life sciences	46%	62%
Retail, consumer goods and lifestyle	44%	67%
Energy technology, energy utilities and oil and gas	41%	94%
Policy and administration	40%	60%
Education	33%	67%
Software and platforms	15%	77%

Leaders also express concerns about the impact on cybersecurity in the near term. This year, 56% of leaders said that generative AI will advantage cyberattackers over defenders in the next two years. More specifically, their greatest concern about generative AI is that it will advance the adversary's ability to undertake actions that defenders are already fighting against such as phishing, developing custom malware and propagating misinformation.

As Kris Burkhardt, Global Chief Information Security Officer from Accenture, stated:

> **We must strengthen our defences across the board, and the same can be true for any emerging technology. A lot of the attack vectors seem to be the same, they just tend to be amplified.**

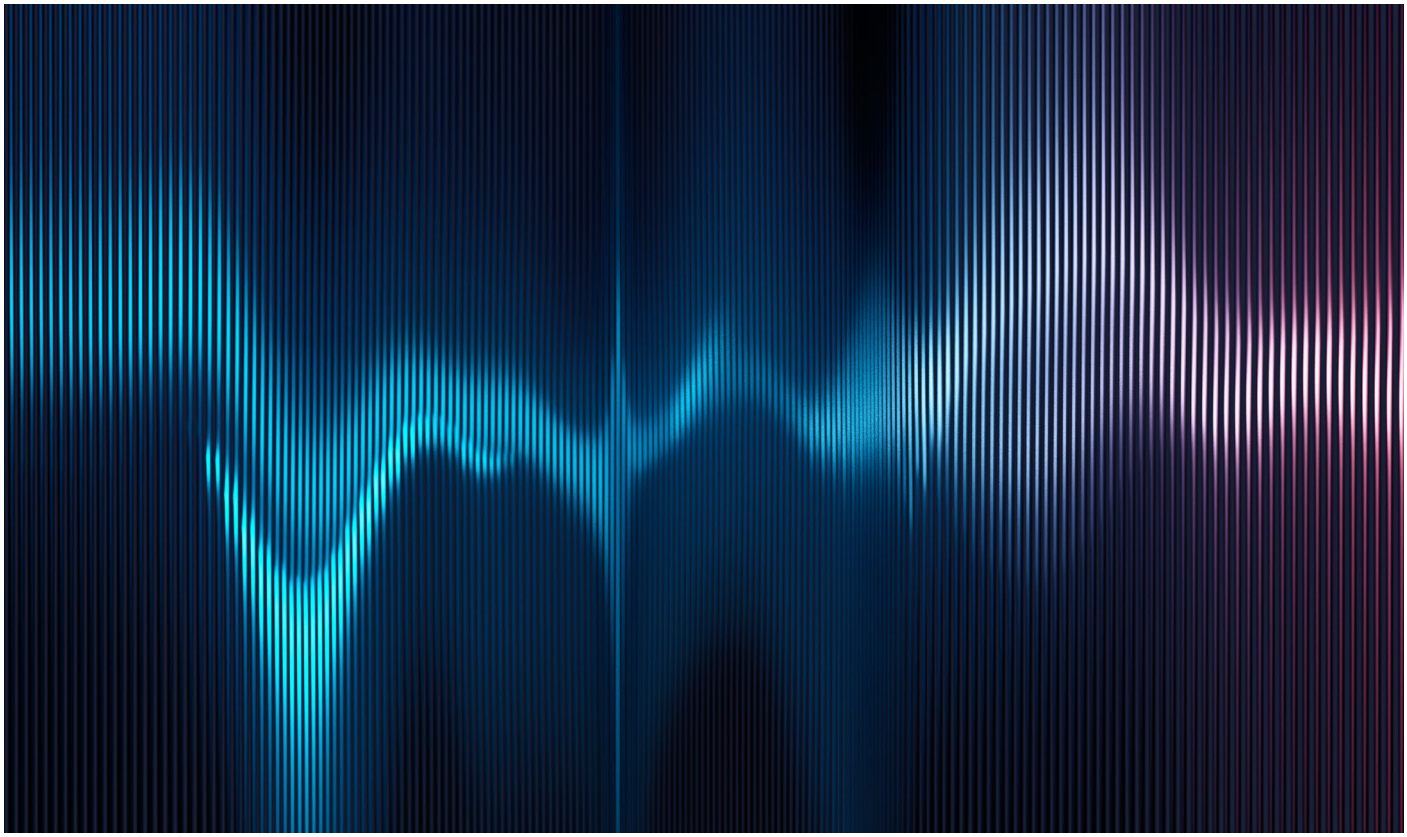
The same attack vectors that have been employed by cybercriminals are still being used; however, new technology paves the way for nefarious activity. Generative AI chatbots are making it much easier for cybercriminals to create believable phishing emails and write custom malware. Although popular commercial chatbots have built-in censors and proactive controls to prevent abuse, cybercriminals are adopting large language models to design malicious subscription-based services. Chatbots such as FraudGPT and WormGPT are lowering the skills required to commit complex and convincing campaigns.[19]

BOX 1

AI used to create convincing deepfake

In August 2023, a software company fell victim to one of the most advanced and complicated social engineering attacks, which used AI to create a deepfake audio of an employee. The company was first targeted through a well-timed and targeted smishing campaign that was themed around open enrolment for health insurance. One employee clicked on the link in the text message and provided their credentials to the fake system. Immediately after the attacker received the credentials, they called the employee's phone to retrieve the multifactor authentication (MFA) code.[20]

These actions raised suspicion from the employee, but because the attacker using a deepfake audio of a familiar colleague, the employee ignored the red flags and provided their MFA code to the attacker. Between the credentials and the MFA code, the attacker was able to add their personal device to the employee's Okta account (Okta is an identity cloud that links all apps, logins and devices). This allowed the attacker to gain approval from the authentication systems used by the victim organization.[21] Although direct attribution to a malicious chatbot may be difficult, organizations can expect even more of these complex and convincing phishing, vishing and smishing attacks.[22]



> The tedious job of data classification can be made less of a manual chore with the help of generative AI.

For most organizations, the potential upside of implementing leading-edge technologies such as generative AI or the metaverse is vast. Generative AI is predicted to increase global GDP by 7% over a 10-year period.[23] Organizations around the globe are able to use the metaverse as a safe, effective and low-cost way to educate and train people.[24] However, the speed and scale at which technology is entering the ecosystem is deepening executives' concerns and stressing the underlying technology systems in their organizations.

When 120 leaders at the World Economic Forum's Annual Meeting on Cybersecurity were asked whether evaluating the impact of emerging technology risk on the broader organization or better covering cybersecurity fundamentals and addressing existing gaps should be the bigger priority for their board or most senior leadership in the upcoming year, almost three-quarters (73%) stressed the importance of cybersecurity fundamentals and addressing existing gaps.

Leading-edge technology itself could also be part of the solution. Applying emerging technologies to foundational security elements is a powerful opportunity to help alleviate the reliability and availability challenges with which many organizations have struggled for years.

A prime example of this is the improvement of the software development life cycle (SDLC). Prompts to an LLM can be used as a method of ensuring that requirements, design guidelines or software architecture are all coded and implemented as planned in the software.[25] The LLM can evaluate and review the code with precision and speed and serve as a way to test the code for errors or scan for vulnerabilities before release. Software engineers can partner with LLMs to work towards developing more complete, secure code, eliminating some of the human-error aspects of the SDLC.

To take this a step further, LLMs can be used to help translate software developed in deprecated or obsolete code into a current, more secure language. Setting aside concerns about propriety code being leaked, all of the above use cases would vastly benefit the security of open-source software.

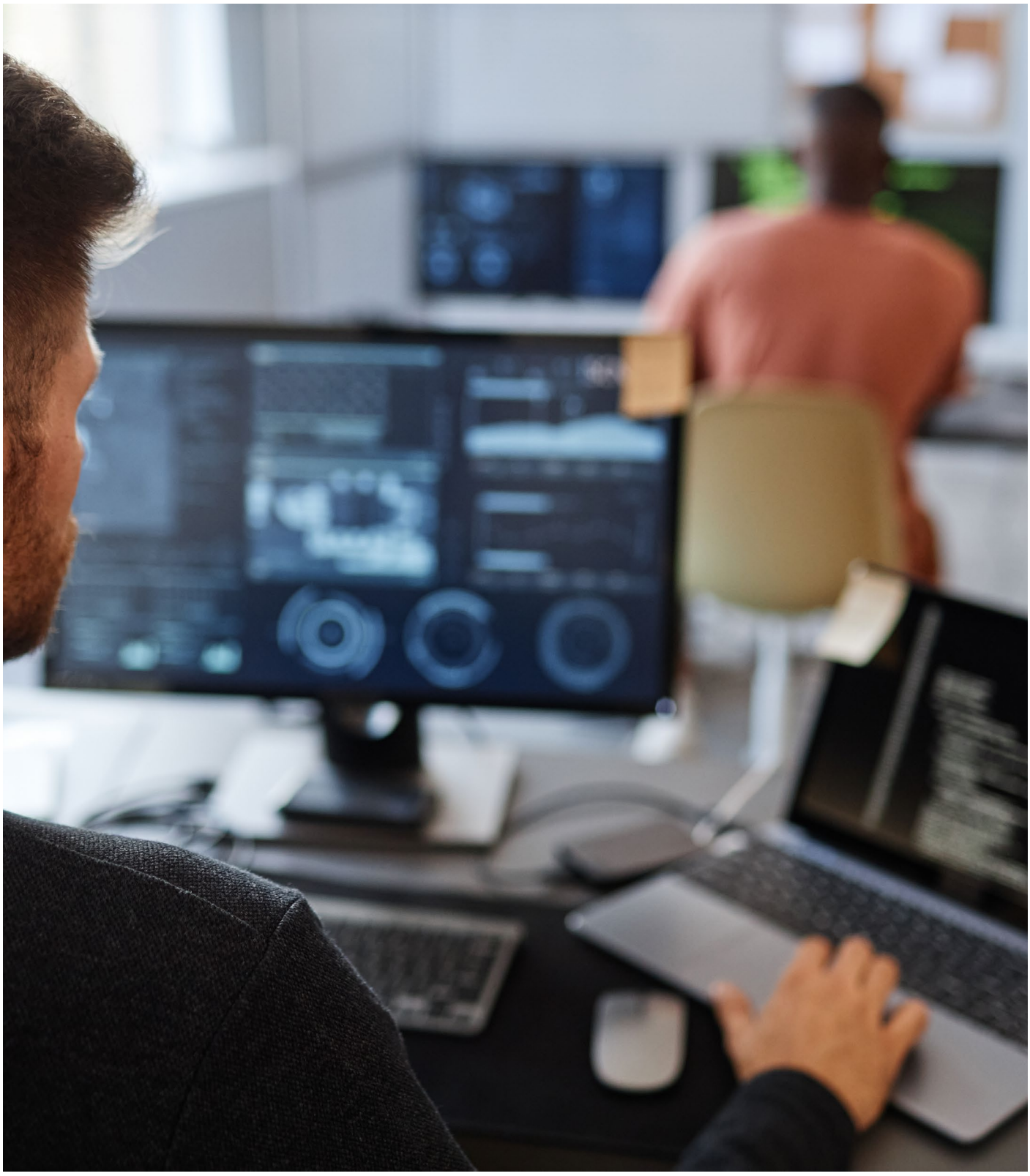
The SDLC is not the only area to benefit from LLMs. The tedious job of data classification can be made less of a manual chore with the help of generative AI. Many of the large software organizations are creating tools that will enable an organization to automate the process of ensuring data is classified and marked in line with organizational policy. When 13% of leaders state that employees were the reason behind a material incident in the past 12 months, data labelling and marking becomes imperative.

Applying and using LLMs in a security operations centre (SOC) is another way to adopt emerging technology into existing foundational cybersecurity. LLMs can be used as a way of automating or assisting an analyst to threat-hunt with more accuracy or develop less noisy and higher-fidelity rules. In fact, according to Splunk's *The CISO Report*, 27% of surveyed chief information security officers (CISOs) will use generative AI in their SOCs to do just that – provide data enrichment of alerts and incidents.[26]

These three examples are only illustrations of how generative AI can be used to alleviate some of the issues with established cybersecurity challenges; however, it cannot solve all of them. In its current state, it will not be able to fully replace skills that are grounded in creativity or human judgement nor require nuanced communication decisions, which include roles such as information security analysts.[27]

3 In the thick of the cyber-skills shortage

Creative action is needed to address the growing cyber-skills gap.

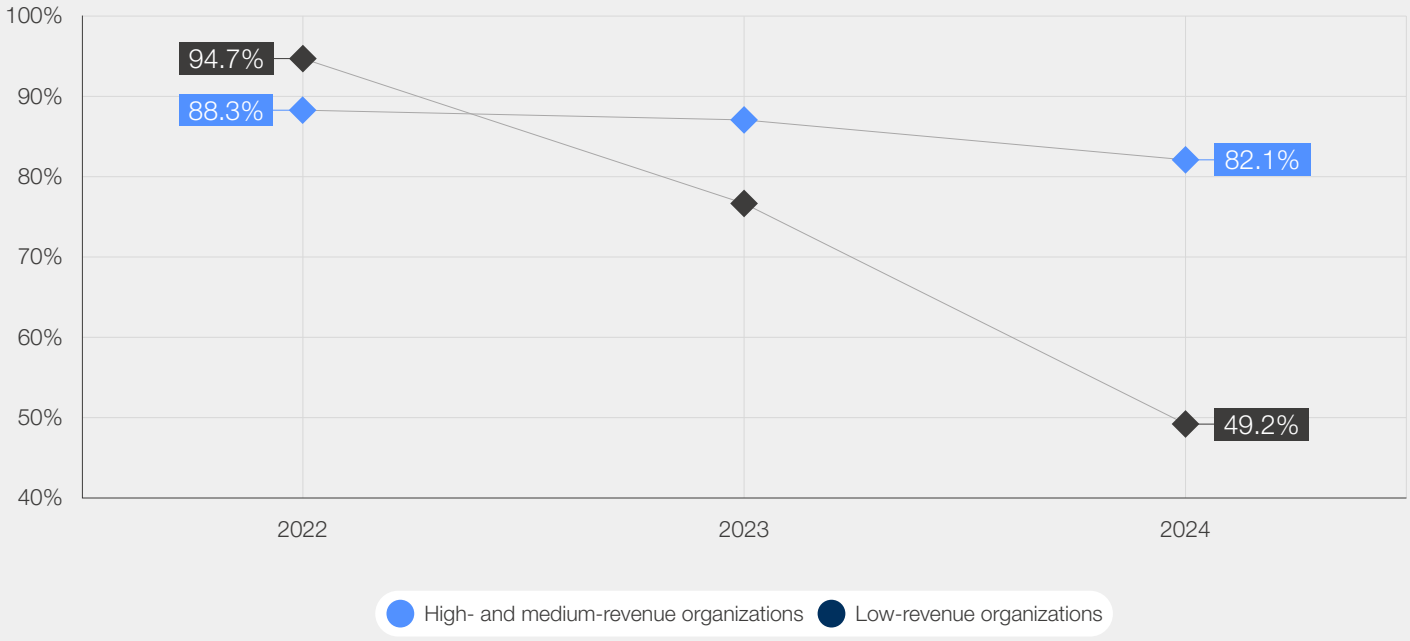


3.1 The skills gap

Executives know that in an evolving cybersecurity landscape, with economic uncertainties, attracting and retaining cybersecurity talent is a crucial aspect of organizational success. The supply of emerging technology entering the digital ecosystem will continue to significantly intensify the demand for skilled professionals. Yet the pool of available professionals is already too small and the pipeline of rising talent is woefully dry. Year on year, more organizations lack the right number of people with the right skills to meet their cyber-resilience objectives.

In 2022, 6% of leaders reported that they were missing the skills and people they needed to respond to a cyber incident. In 2023, this doubled to 12%. This year, when asked whether their organization has the skills it needs to accomplish its cyber objectives, 20% said that they do not. Leaders who are unsure if they have the required skill sets also rose from 4% in 2022 to 11% this year.

FIGURE 5 **Do you have the skills needed to achieve your cybersecurity objectives?**



This shortage is not related solely to having the resources to perform specific tasks; a lack of critical technical and soft skills is quickly becoming the largest barrier preventing an organization from achieving its strategic cyber-resilience objectives. This year, 36% of respondents said that skills gaps are the main challenge to achieving their cyber-resilience goals. Some 78% of respondents reported that their organizations do not have the in-house skills to fully achieve their cybersecurity objectives. This is worsened when factoring in that 57% of respondents from an ISC2 cybersecurity workforce study[28] believe that the shortage of cybersecurity staff is putting organizations in moderate to extreme risk of experiencing a cybersecurity attack.[29]

In a concerning indication of inequity, 31% of leaders from the smallest organizations by revenue reported that they are missing critical people and skills; yet only 11% of leaders from the largest organizations said the same. This aligns with 34% of respondents from the ISC2 cybersecurity workforce study, who indicated that the most important cause of a cybersecurity staff shortage is their organization not having the budget.[30] Even if they could get access to enough people, they cannot compete for the right talent. While the skills gap is affecting all organizations, the smallest organizations are facing the greatest challenge.

To fill these gaps, organizations are looking internally. Although many employers are still looking to hire experienced cybersecurity professionals (33%), the number one way in which organizations are filling these roles is by upskilling existing employees (41%). In fact, to upskill the workforce, as many as 91% of organizations are willing to pay for cybersecurity training and certification for their employees.[31] The motivation to upskill can also be

observed from the side of professionals. Research shows that more than 70% of employees would consider returning to college to pursue a degree or certificate that would allow them to work in cybersecurity if their employers provided funding.[32] Although non-traditional recruitment paths are a promising way to ensure an organization has the skills it needs, few leaders are choosing it.

Microcredentials – certifications or short educational courses, rather than traditional university degrees – are one way to fill skills gaps and open up a new pipeline of talent for organizations.[33] However, considering that the majority of cybersecurity roles and positions today still require a university degree, it comes as no surprise that only 9% of organizations report taking advantage of that pipeline by recruiting outside of traditional cyber degrees or credentials.[34] Apprentice programmes are an even less tapped opportunity for talent; only 8% of organizations use these programmes to close the skills gap. Without intervention, this gap will continue to widen unopposed.

Another rift between the smallest and largest organizations by revenue is the ability to recruit traditional cybersecurity professionals. Only 21% of respondents from the smallest organizations by revenue said they would close the skills gap by recruiting experienced cyber professionals; in comparison, 36% respondents from the largest organizations by revenue said the same.

The smallest organizations by revenue also place more pressure on employees to upskill independently. Although 15% of respondents from these organizations expect their employees to upskill independently, only 4% of the respondents from the largest organizations by revenue said the same. The burden then falls to the smallest organizations by revenue to find creative solutions to secure the resources needed to respond and recover from a cyber incident. The cyber skills shortage continues to widen and uncertainty grows surrounding the securing of resources.

To tackle the shortage of cybersecurity skills and talent, and raise awareness among decision-makers about the implications of the cybersecurity skills deficit for the global economy and security, the World Economic Forum's Centre for Cybersecurity has established the Bridging the Cyber Skills Gap initiative. Taking a multistakeholder approach and using diverse perspectives from industry leaders, government agencies, civil society and academia, the initiative aims to create a strategic cybersecurity talent framework and devise actions to help individuals enter and thrive in the cybersecurity workforce.

> **World Economic Forum research indicates that by 2027, 44% of workers' core skills will be disrupted because technology is moving faster than companies can design and scale their training. This is true in cybersecurity, where the talent gap continues to pose very real challenges across public and private industries. To address this, organizations must tap into new talent pools – beyond 'traditional' candidates with previous cyber experience – and provide employees with upskilling opportunities like certification programmes. These hiring and retention strategies can help organizations keep pace with the evolving threat landscape.**
>
> Ken Xie, Founder, Chairman of the Board and Chief Executive Officer at Fortinet

4 Cyber resilience for a new era

The GCO Survey results provide insights into leaders' attitudes towards cybersecurity and how prepared their organizations are to face new cyber challenges.

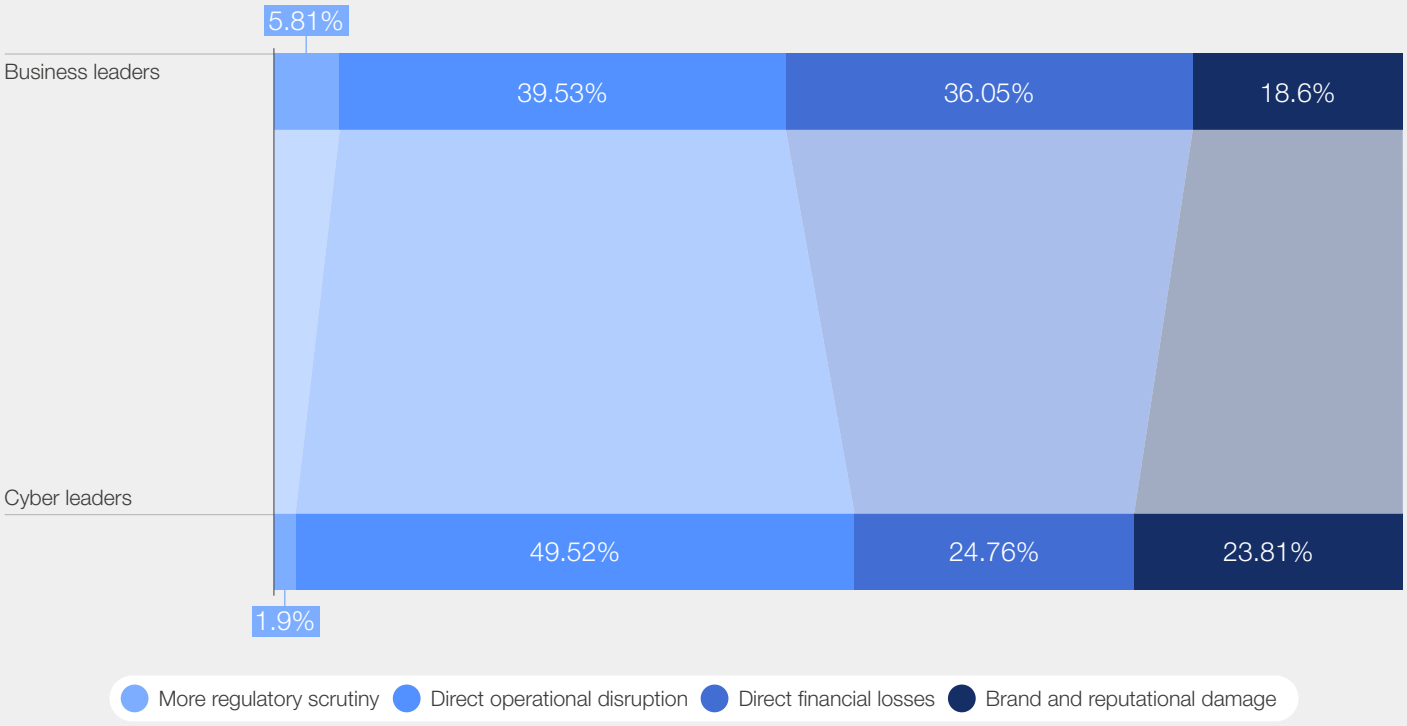
4.1 Marrying legacy concerns with new risks

In the survey conducted for the 2024 GCO report, 45% of leaders said that operational disruption is their greatest concern with regard to suffering a cyber incident. This holds true when cyber and business leaders are grouped: 50% and 40% respectively said that operational disruption is their greatest concern.

BOX 2 **The World Economic Forum's six consensus-based principles for board governance of cyber risk**

- **Embed cybersecurity as a strategic business enabler**
- **Establish and maintain core security fundamentals**
- **Understand the economic drivers and impact of cyber risk**
- **Incorporate cyber-resilience governance into business strategy**
- **Align cyber-risk management with business needs**
- **Ensure organizational design supports cybersecurity**[35]

FIGURE 6 **What impact from a cyberattack are you most concerned about?**

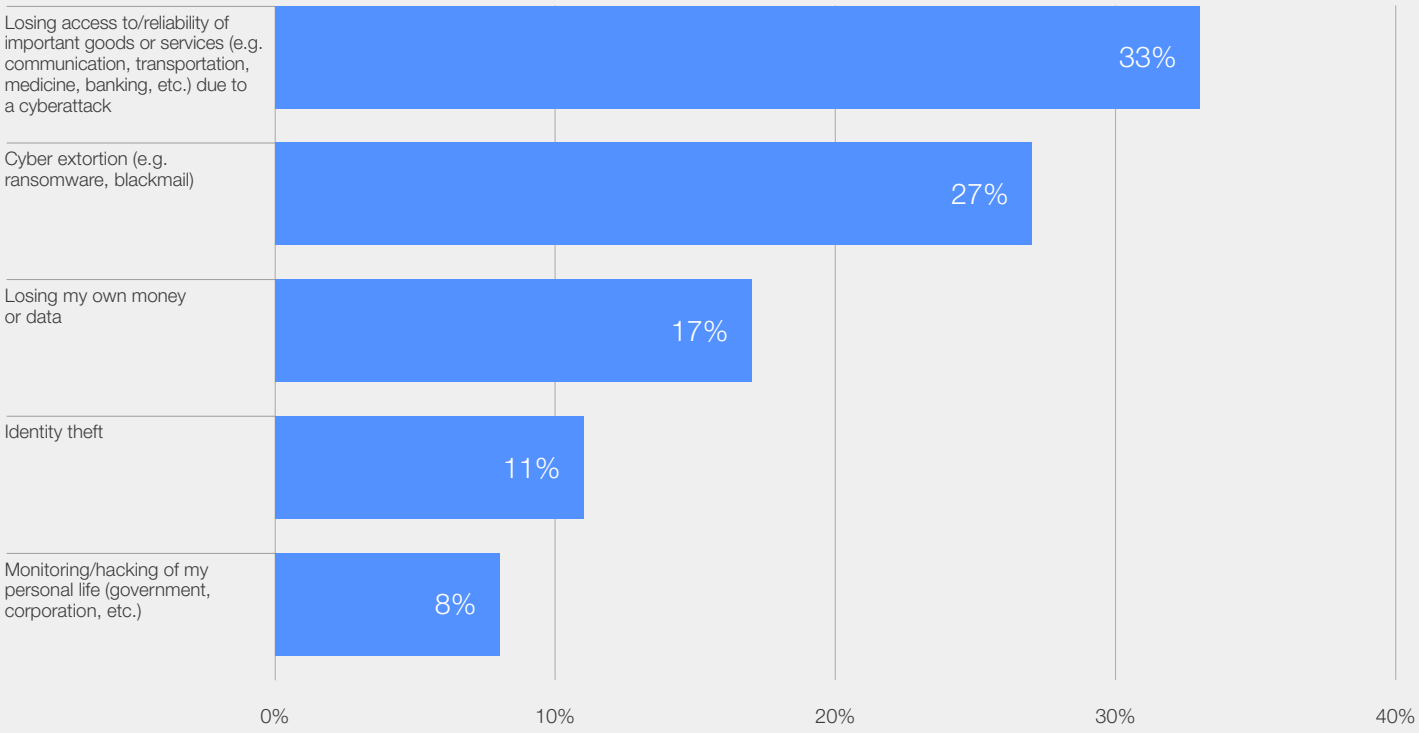


From a regional perspective, a majority of leaders from Europe and North America reported that operational disruption was their greatest concern. However, a majority of leaders from Africa, Asia and Latin America reported that their greatest concern was suffering direct financial losses, such as from a ransomware attack. The most chosen answer by leaders from the Middle East was brand and reputation damage.

Similar to the overarching concern about operational disruption, when leaders were asked what personally keeps them up at night, they said that losing access to important goods and services and cyber extortion are the most concerning. The concerns about disruption are not unfounded when considering that 29% of leaders stated that their organization had experienced a *material impact* from a cyberattack in the past 12 months.

Regionally, more than half of leaders from Europe and North America reported that their organization carries cyber insurance. More than 60% of leaders from all other regions reported that their organizations do not carrier cyber insurance.

FIGURE 7 | **What keeps you up at night?**

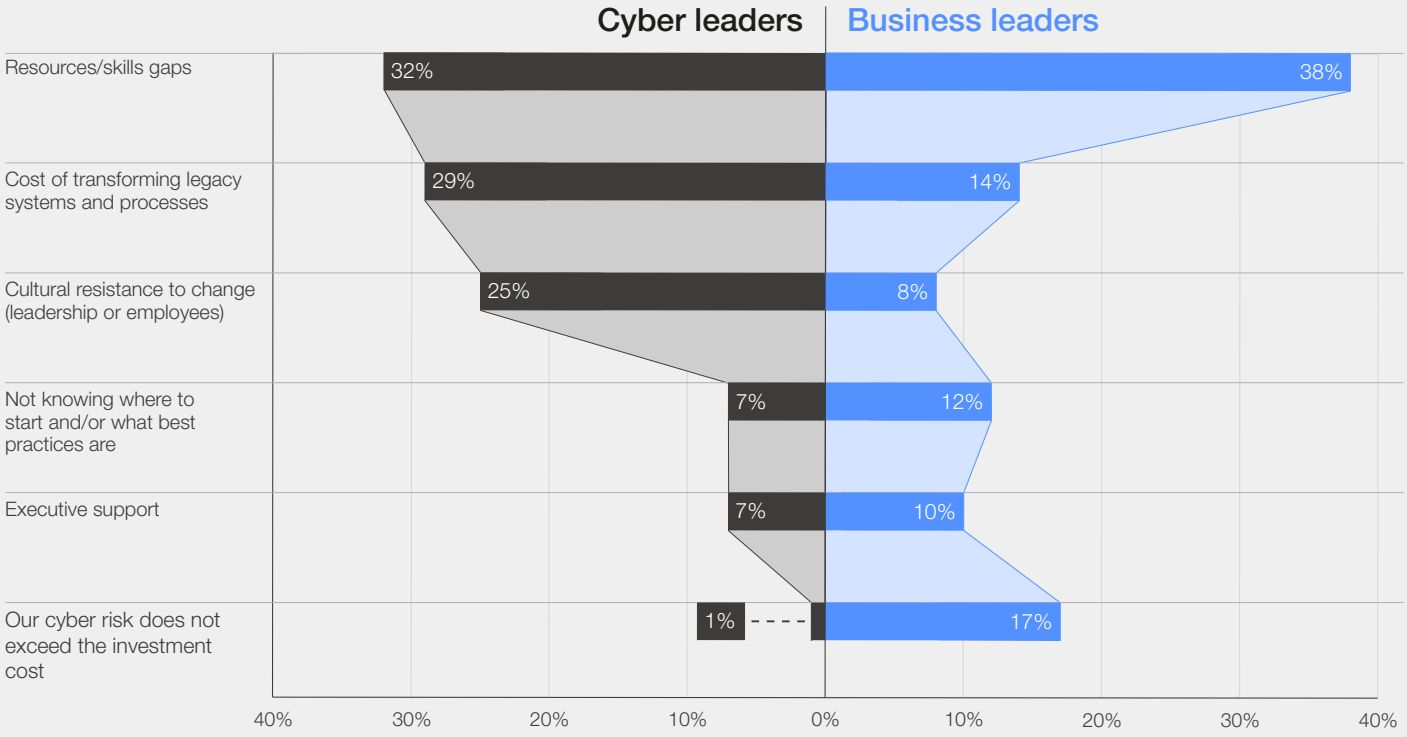


In September 2023, a global gaming and entertainment company was brought face to face with its worst fears. A social engineering attack, which took place during a 10-minute phone call to the organization's help desk, sparked a 10-day critical disruption.[36] Stronger cybersecurity foundations, with a focus on awareness, education and more robust incident response plans, could have mitigated the resulting disruption to the organization. This event occurred without the confirmed use of generative AI, which further stresses that the foundational cybersecurity elements need to be put in place and mastered to contend with the potential rise in advanced attacks from new capabilities.

Organizations need to focus not only on the emerging and new but also on older technology or legacy systems. For the largest organizations by revenue, 44% of survey respondents said that securing legacy technology is their highest barrier to cyber resilience. For them, it is an even greater challenge than gaining enough executive support or filling skills gaps. During several workshops convened for this report, discussions on resilience focused heavily on the importance of operational technology security. Legacy systems were most pronounced in organizations with an operational technology (OT) footprint.[37]

This issue becomes more apparent when looking at how responses differ between cyber and business leaders. Following on from the fact that the gap between cyber and business leaders is closing, the main conclusion of the GCO 2023 report, both groups said that resource or skills gaps were the highest barrier to cyber resilience (38% of business leaders and 32% of cyber leaders).

FIGURE 8 | **What are your highest barriers to cyber resilience?**



For security leaders, securing legacy technology (29%) and cultural resistance to change (25%) followed close behind. Interestingly, this is where business leaders' paths diverged, with only 14% and 8% respectively agreeing with security leaders on these challenges.

Both securing legacy technology and a cultural resistance to change stem from issues with resources and skills gaps. It appears that in the view of security leaders, these challenges cannot be addressed until they have the people and skills with which to address them. For business leaders, these challenges are more tenable, as their work is not immersed in the day-to-day tasks of designing for cyber resilience.

The barrier will become even higher as organizations rush to adopt generative AI and other elements of emerging technology. However, most organizations either do not upgrade older systems or do so much more slowly than the speed at which they introduce more tools and new technologies. This in turn expands their technological footprint and adds risk.

What is more, larger organizations weighed down by a greater and older technology burden will be less able to assist and monitor the smallest organizations in their supply chain. This would strain support mechanisms in the ecosystem and exacerbate the inequalities discussed in the previous section. As Janus Friis Bindslev, Chief Digital Risk Officer of PensionDanmark, put it:

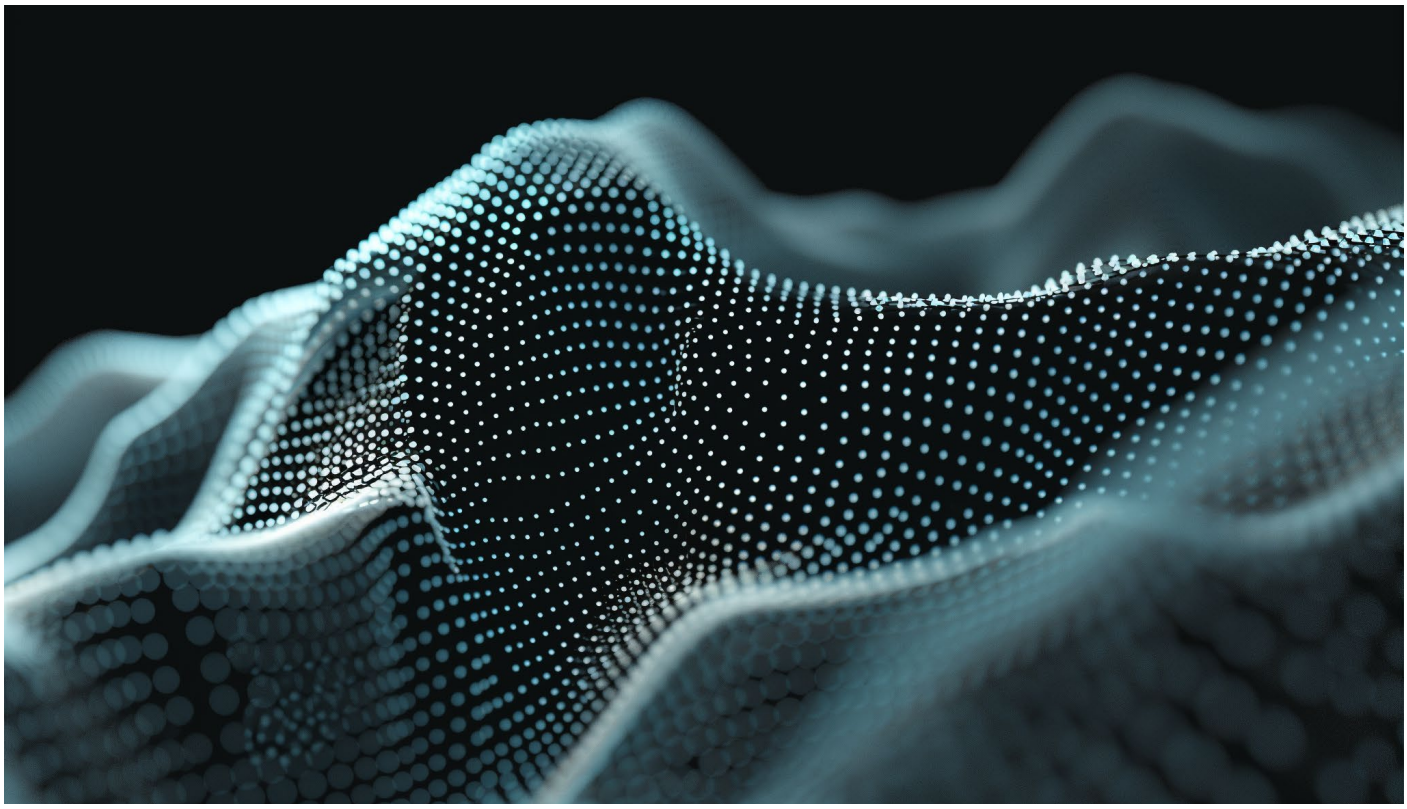
> **Sometimes you call it legacy, but previous issues with underlying technologies and complexity that larger companies typically carry around will be more apparent with the new innovations we're seeing. There wasn't such a rush to solve those issues before, but now those issues will be amplified.**

4.2 Emerging technologies and the state of resilience

Cyber resilience is built step by step through prudent planning and long-term commitment to organizational change. Security leaders are always at risk of being distracted from their core work by hype about instant solutions, the need to focus on the secure implementation of new technologies or the tension created by a well-grounded fear of imminent attacks. Despite the noise, the organizations surveyed show that a degree of strategic patience and prudent cyber-resilience practices are slowly but surely having an impact.

The accelerated adoption of emerging technologies does, of course, create new security challenges. However, many of the security leaders involved in this study argued that maintaining a focus on tried and tested cyber-resilience practices will help detect and mitigate risks early.[38] These principles are exemplified by the corresponding responses from cyber-resilient organizations. Critically, the number of leaders who report that they are confident in their organization's cyber resilience has risen steadily year on year for the past three years and is up 20% from 2022.

Driving this confidence is the emphasis organizations are placing on integrating cybersecurity into their enterprise risk, gaining executive leadership buy-in and shifting the organizational culture.



4.3 Cybercrime and the state of resilience

In this year's Outlook report, the vast majority of leaders (81%) responded that they feel more exposed or similarly exposed to cybercrime than last year. This is despite Fortinet's annual threat report finding a 75% drop in exploitation attempts per organization. They note that while this may initially seem hopeful, it is more likely a combination of improvements in the ability of defenders to detect attacks, and better and more precise targeting from cyber criminals.[39]

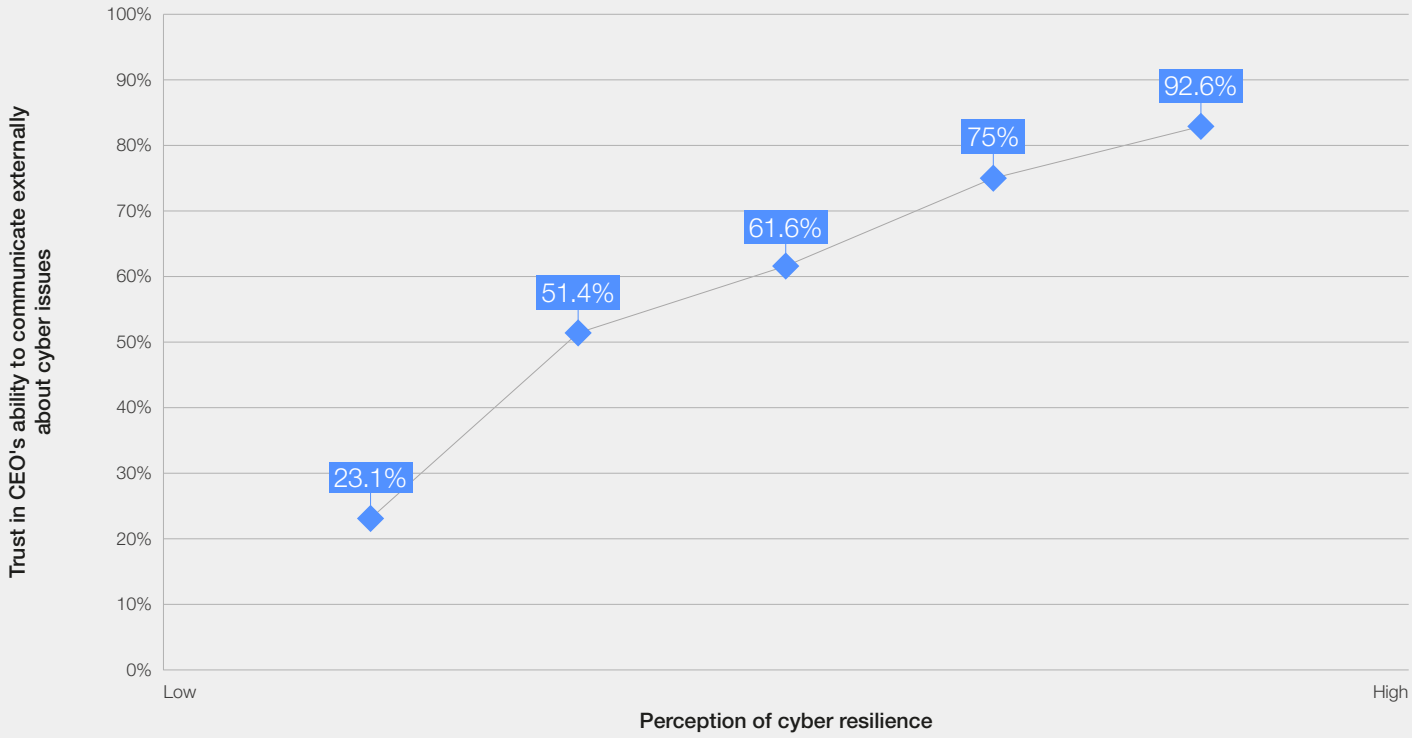
Exposure to cybercrime does not always need to directly correlate with the number of attacks. Workshops with security leaders undertaken at the World Economic Forum's Annual Meeting on Cybersecurity in late 2023 suggest that as cybercriminals gain access to new technologies that increase the speed and level of tailoring of their attacks, security leaders will continue to benefit from focusing on cyber-resilience essentials. This includes maintaining leadership support, integrating cyber into enterprise risk management and continuing to capitalize on the cultural and structural changes organizations need to make to adapt to new technologies.

4.4 Business leadership and the state of resilience

In 2023's Outlook report, security executives expressed increased concern about the level of cyber resilience in their business. In parallel, the level of awareness of cyber risk and cybercrime among business executives led to a marked increase in concern about the ability of their organizations to be cyber resilient. This might be due to business leaders' better understanding of the damage that a major cyberattack could do to their operations, commercial relationships and reputation.

Cyber resilience and CEO trust are tightly connected. This year, a resounding 93% of the respondents that consider their organizations to be leaders and innovators in cyber resilience trust their CEO to speak externally about their cyber risk. None of the security leaders from the group of organizations that self-reported as cyber resilient said they distrust their CEO to speak externally about the state of cyber resilience in their organization.

FIGURE 9 **Organizations with higher cyber resilience are more likely to trust their CEO**



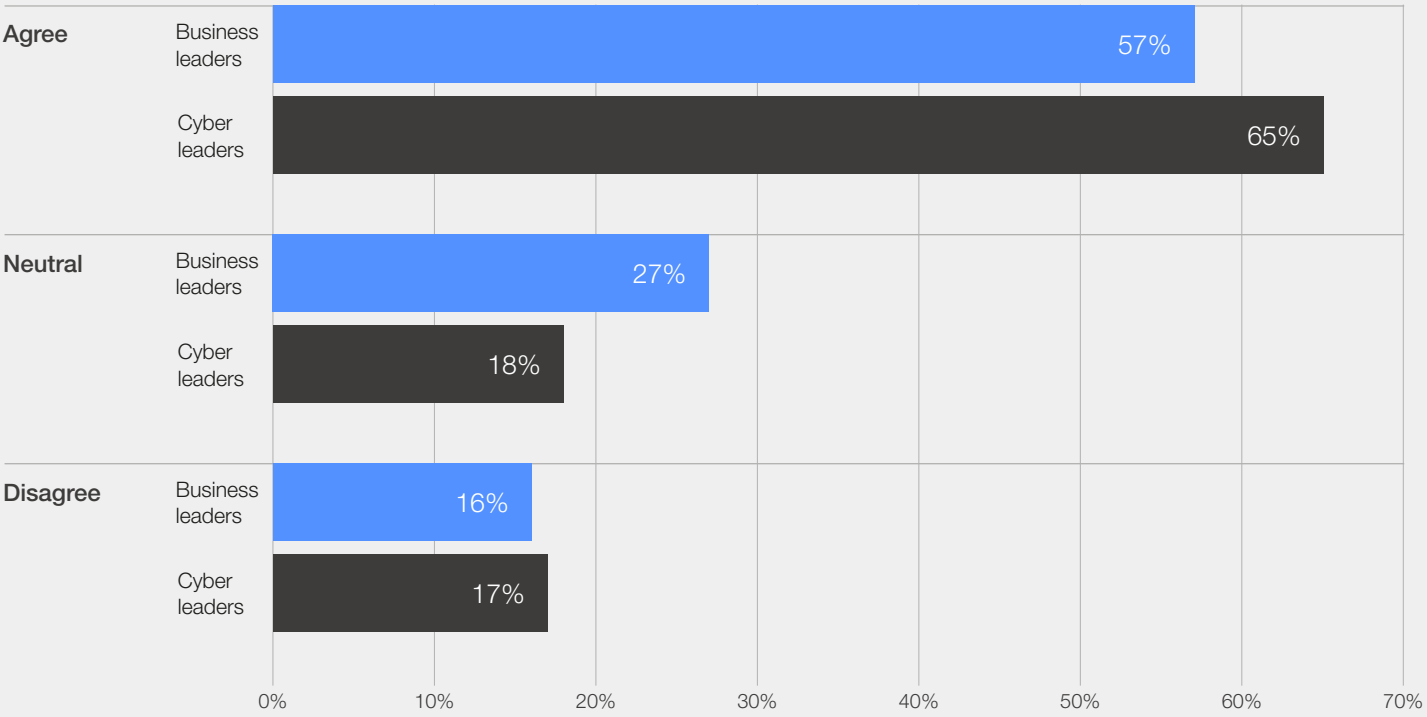
Of the respondents reporting that their organizations are not cyber resilient, 77% either distrust or are unsure about their CEO's ability to speak about their cyber risk.

This suggests that organizations in which executive leadership is engaged in how cyber risk is managed are more cyber resilient. A security leader's trust in their CEO's ability to talk to external partners about cyber resilience is a proxy measurement for how engaged the C-suite is in the management of cyber risk. Firms that report high levels of trust in their CEO to articulate the organization's cyber-resilience posture also self-report as being more cyber resilient.

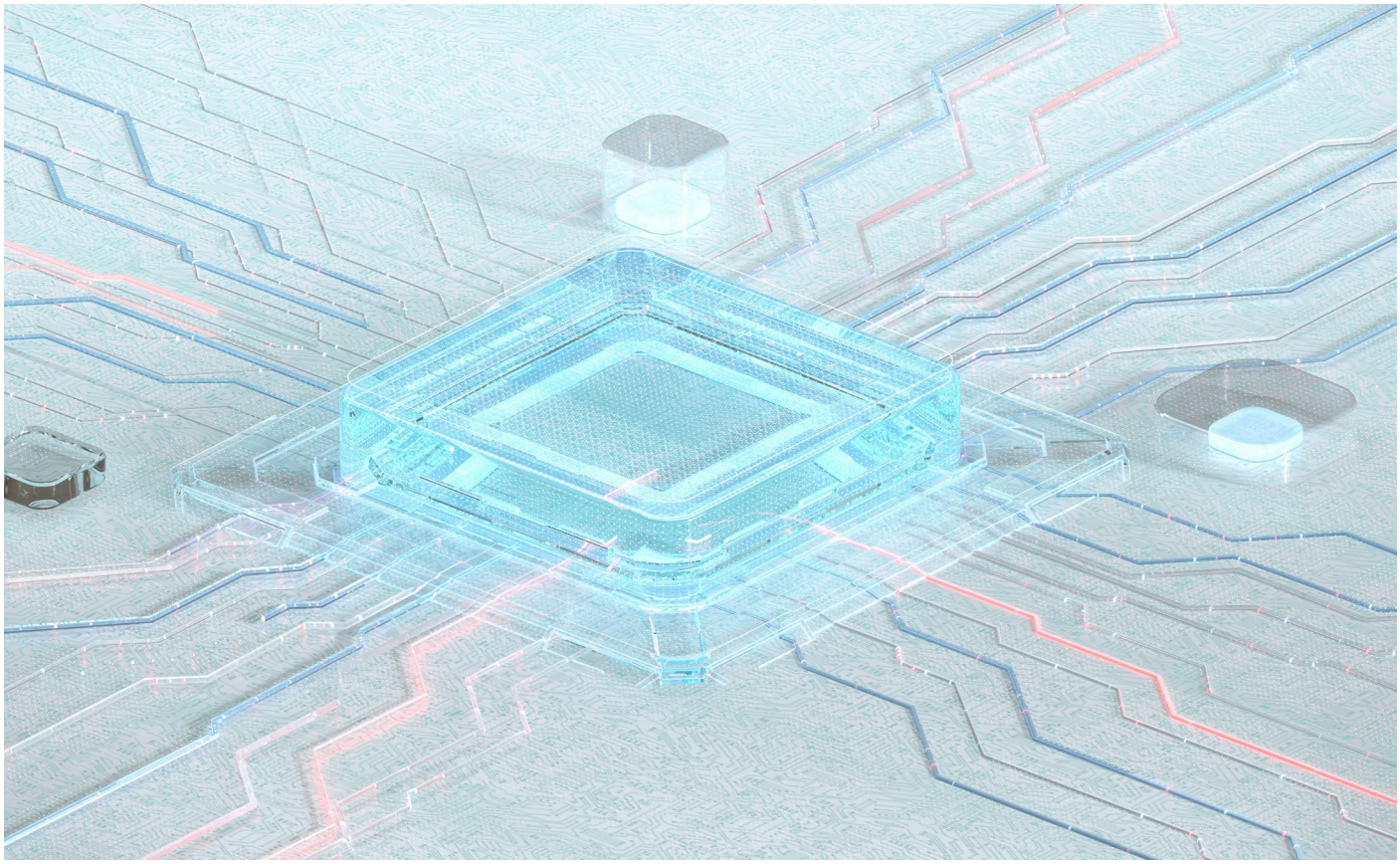
CEOs are more aware of their organization's cyber risk than ever before. Some 74% of CEOs are concerned about their organization's ability to avert or minimize damage to the business from a cyberattack[40], according to Accenture's The Cyber-Resilient CEO report. Executive leadership is using cyber incidents (29%) and reports and statistics (24%) to educate and influence their decisions regarding cybersecurity. This suggests that a significant minority of organizational leaders are professionalizing their approach to cybersecurity decision-making by bringing in sources that were previously reserved for security leaders or subject-matter experts.

Building upon the importance of an enterprise-wide approach to cyber resilience is the integration of such an approach into enterprise risk management. Some 78% of respondents who are confident in their organization's cyber resilience also report that cyber resilience has been integrated into their enterprise risk management. The alignment between cyber and business leaders can also be seen here: 65% of cyber leaders and 57% of business leaders report that cyber resilience is integrated into their risk management.

FIGURE 10 | **Do you agree with the statement "Cyber resilience in my organization is integrated into enterprise risk management (e.g. financial, strategic and operational risks)"?**



The connection between resilience and trust demonstrates the importance of both cross-departmental knowledge and C-suite-level support. It also indicates that the most important drivers of an organization's cyber resilience are the foundational concepts of leadership support, business integration and ecosystem collaboration. The journey to resilience is never-ending, but one that can be tackled if undertaken together.



4.5 Governance and the state of resilience

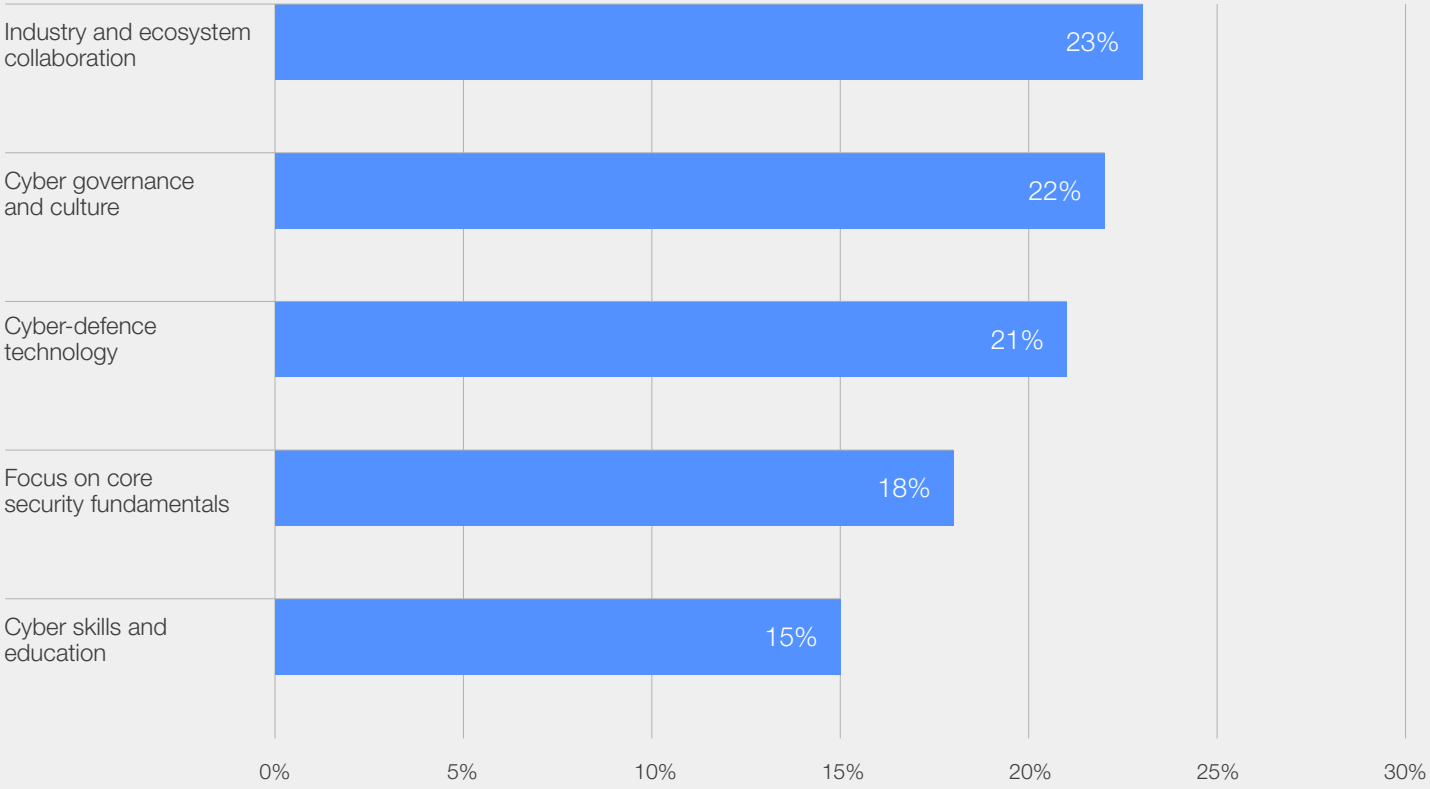
To date, notable progress has been observed when it comes to organizational cyber resilience. Yet only 22% of respondents are optimistic that cyber governance and culture will improve in the next two years. And when compared by different organizational demographics, a frustrating but familiar picture emerges.

Some 40% of respondents from public organizations suffered a material impact from a cyberattack last year. Larger organizations by revenue and public organizations, even if they are more resilient overall, are more likely to experience a cyberattack. This could be due to a larger attack surface, more valuable assets or simply that they have the resources to sustain and recover from a cyberattack in the first place.

As Aleksandr Yampolskiy, Chief Executive Officer of SecurityScorecard, put it:

> **Trust is now not just about you, but it's about your entire digital ecosystem. You could send your paperwork to a tax audit firm. Then the tax audit firm gets hacked. Your sensitive information is on the cover of a newspaper. So, even if it's not you that got hit, you are still going to suffer financial losses and reputational damage.**

FIGURE 11 **What are you most optimistic about?**



4.6 Ecosystem resilience

Public organizations are taking action, understanding that building up the SMEs in their digital ecosystem strengthens the entire system. In November 2023, the federal government of Australia announced an AUD 18-million deal to uplift their country's SMEs' ability to react and respond to cyber incidents. SMEs form 97% of businesses in Australia, and the package will assist them in a variety of fundamental cyber-resilience practices including education materials, requirements on how to upskill, cyber-maturity assessments and guidance on how to better respond to cyber incidents.[41]

Australia is not the only country or region to actively partner with the private sector to uplift its cybersecurity posture – the European Union is also focusing attention on the cybersecurity positioning of its private organizations. The European Cybersecurity Competence Centre (ECCC) is an EU initiative to build a stronger cybersecurity posture through a new framework, research and information sharing.[42]

The ECCC has hosted information-sharing events to strengthen the collective cyber resilience of its participating countries. The first such event took place in November 2023, and focused on cybersecurity awareness.[43] Participating countries, such as Luxembourg, Belgium, the Netherlands, Italy, Germany and Estonia, were able to share their lessons learned and best practices on how to promote effective cyber awareness, not just with business, but with the workforce and general population.

However, one critical governance issue, which is also at the heart of trust in the digital ecosystem, still needs to be addressed. There is a glaring imbalance of responsibility for security between technology producers and technology consumers. For years, organizations and individuals have had the primary responsibility for ensuring the hardware and software they use is securely and resiliently implemented, operated and maintained. When incidents do happen, the burden of remediating and recovering from it similarly resides with the user, along with the associated financial burden. This situation is indicative of the technology and cybersecurity industry's expansive growth over the past two decades, its relative immaturity compared to more established sectors of consumer goods and the associated growing pains as it matures.

BOX 3 Focus on the CISO

Chief information security officers (CISOs) believe that addressing the balance of liability for cyber incidents is getting ever more urgent. At one World Economic Forum session at the Annual Meeting on Cybersecurity in November 2023, approximately 50 participants from all regions of the world discussed this topic at length. Some security leaders argued that liability and regulation can work directly against practices important for protecting the wider ecosystem, such as cross-industry collaboration and information sharing during live attacks.

In general, public-sector organizations have been asking security leaders to share more information on incidents and to do so at speed. This naturally requires a trade-off on accuracy as it takes time to understand the full scope and impact of a cyber incident. At the same time, security leaders feel they will be penalized for providing incorrect information.

In 2022 the focus of regulators and public agencies was on the role of the board in managing cybersecurity risk. In 2023, however, scrutiny has expanded to include security leaders.

Many security executives are now held personally accountable for the state of their organization's cybersecurity – which comes to light only after an incident. Discussions are taking place globally on a range of CISO liability-related behaviours, from intentional malicious behaviour to negligence. In fact, in May 2023, former Uber CISO, Joseph Sullivan, was fined and sentenced to three years' probation after being the first cybersecurity executive to be convicted of covering up elements of a data breach perpetrated by external attackers.[44] Six months later, former SolarWinds CISO, Timothy Brown, was charged with securities fraud by allegedly overstating SolarWind's cybersecurity practices and allegedly understating or failing to disclose known cybersecurity risks prior to the company's breach in 2020, which had a systemic impact across several jurisdictions.[45]

The cases taken against Uber and SolarWinds are tackling highly undesirable behaviours, but an unintended consequence is the creation of an atmosphere of legal risk that could raise additional obstacles for security leaders who wish to improve systemic cyber resilience by, for example, sharing information with their peers during an ongoing attack. Public-sector agencies might reduce some of the unintended negative consequences of their actions by providing security leaders with clearer guidance on what is expected of them during events such as live cyber incidents.

This is a contentious topic that has spawned a nuanced debate. This year's surveys, interviews and workshops indicated a consensus towards a balance of responsibilities. The most frequently encountered view is that it is not sustainable to simply shift all responsibility to the technology companies – the consumer must continue to play an appropriate part in maintaining cyber trust.

Feedback from expert interviews and workshops run to support this report suggest that the combination of convenience, prospects for business acceleration and fear of being left behind tempts organizations into introducing new technology into their environment much faster and with less fundamental security than is prudent. Cyber leaders understand that a core part of the solution is a fundamental shift in the economic incentive structure for those innovating in technology and cyberspace.

Michael Daniel, President and Chief Executive Officer of the Cyber Threat Alliance, characterized the situation in this way:

> **"As an industry we have pushed cybersecurity responsibility all the way out to the edge, which isn't very efficient. But if you're going to realign the burden toward secure by design, you also have to change the incentive structure for the technology providers to create upside for them.**

Nonetheless, notable efforts are under way in both governmental programmes and private-sector initiatives to spread the responsibility for security by design more evenly. The United States National Cybersecurity Strategy and US Cybersecurity Infrastructure and Security Agency (CISA)'s "Secure by Design, Secure by Default" campaign are prominent examples. The European Union's proposed Cyber Resilience Act is another high-profile effort.

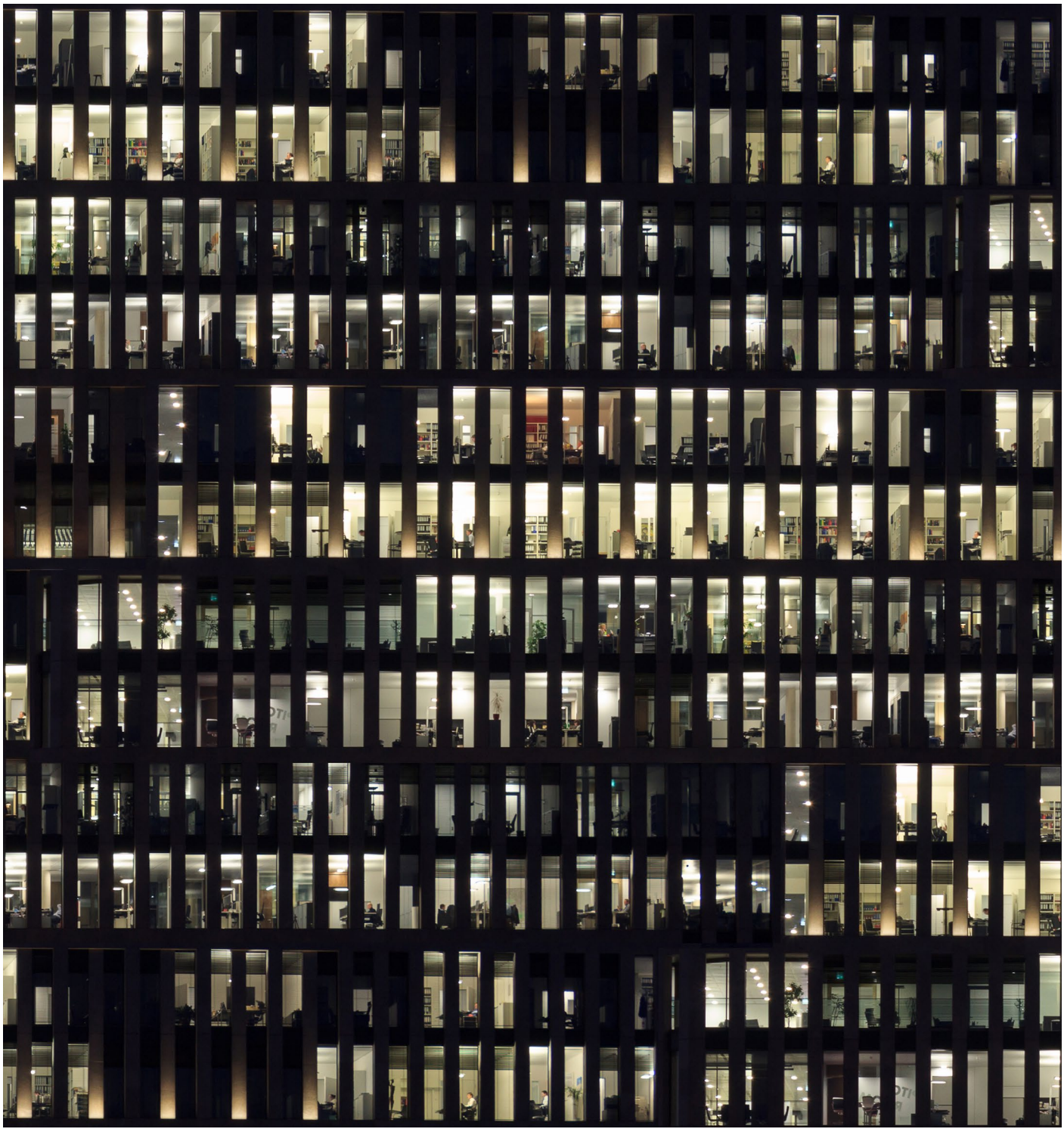
Both of the above examples strongly advocate making technology manufacturers and service providers more responsible for ensuring that their products were created with security from the beginning and that they can be kept secure throughout their life cycle. These efforts also aim to clarify for everyday consumers which products they can trust.

Organizations are working to build trust in leadership and emphasize the importance of cyber resilience enterprise-wide. In addition to this, there is growing cooperation between the public and private sectors to uplift organizations that do not have the resources on their own to achieve that same level of resilience, as well as efforts to make products more secure out of the box and for the duration of their usage. These factors work together to smooth out disparity among organizations with different demographics, and increase the capability of the ecosystem, benefiting all.

5

Building a better cyber ecosystem

Collaboration among organizations, suppliers, insurers and regulatory bodies is an essential factor for building a more secure cyber environment.



Key indicators for systemic cyber resilience include the quantity and quality of industry collaborations, the effectiveness and clarity of regulations, the maturity and accessibility of the cyber insurance market, and the extent to which organizations understand cyber risk coming from their own supply chains and third-party relationships.

When an organization finds common ground in its relationship with its suppliers, regulators, government agencies and industry peers, it creates a more resilient digital landscape. Conversely, an organization cannot truly be resilient if the partners on whom it relies are fragile.

5.1 Are cyber collaborations stalling or continuing to mature?

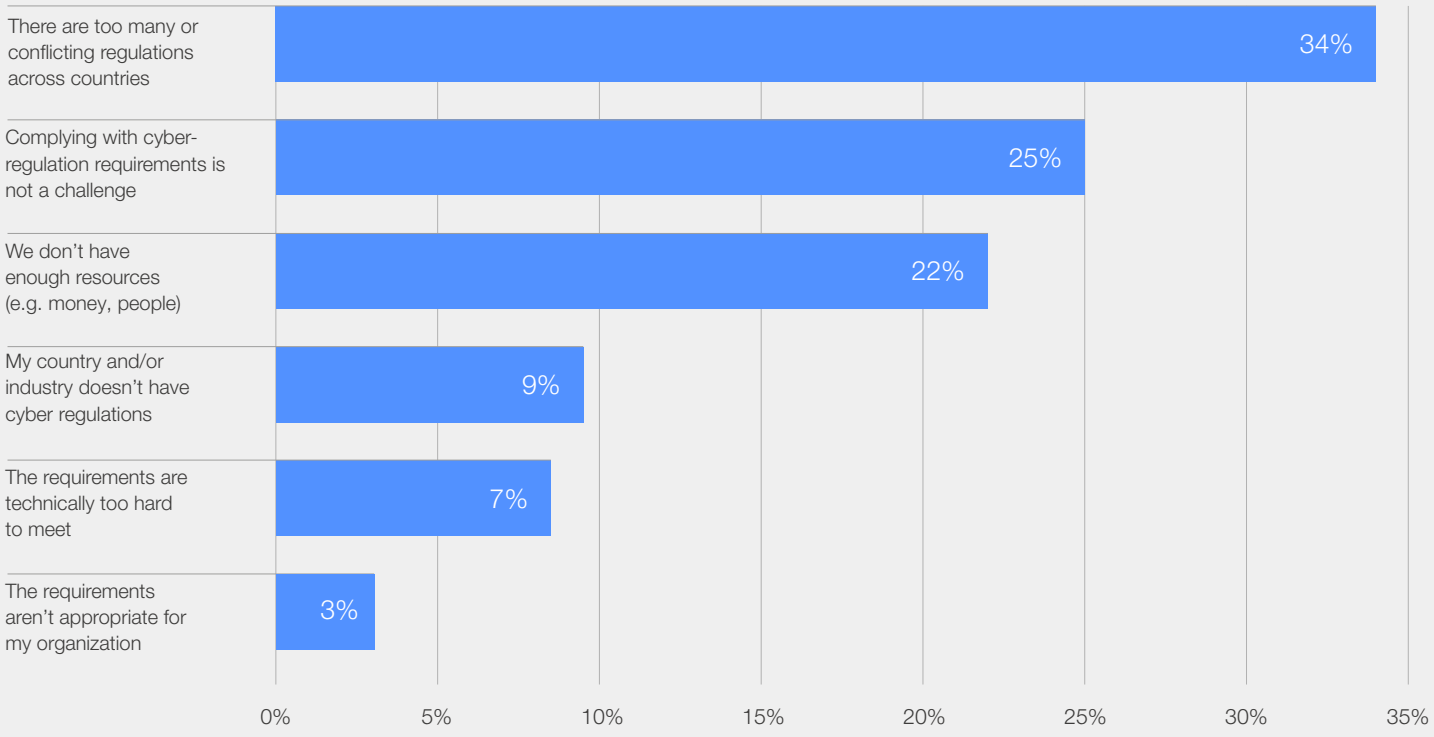
Unfortunately, only 23% of leaders are optimistic that industry and ecosystem collaboration will significantly improve in the next two years. Cyber leaders are marginally more optimistic that industry and ecosystem collaboration will become better (29%) in comparison to business leaders (17%). This could be because cyber leaders have more direct access to these collaborations and can see how they are growing in operational maturity.

This year's outlook shows that partners in an organization's ecosystem – each with their own perspectives and incentives – are both the greatest asset and the biggest hindrance to a secure, resilient and trustworthy digital future.

5.2 Effective regulation lifts all boats

Executive views on cyber regulation are a good example of the evolution of the perspective of both business and cyber leaders on public private interaction over the years. On the one hand, 60% of leaders from private organizations feel that cyber and privacy regulation effectively reduces risk in their organization's ecosystem, up from 39% in 2022. They are aligned with public leaders – 65% also agree with the statement.

FIGURE 12 **What are your biggest challenges in complying with regulations?**



Yet even though regulation is effective in uplifting the ecosystem, 34% of those leaders say their biggest challenge is that there are too many conflicting regulations across countries. However, only 7% say that regulations are technically too hard to meet. Not only is regulation valuable, but greater alignment across industries and geographies would make cyber and privacy regulation even more beneficial.

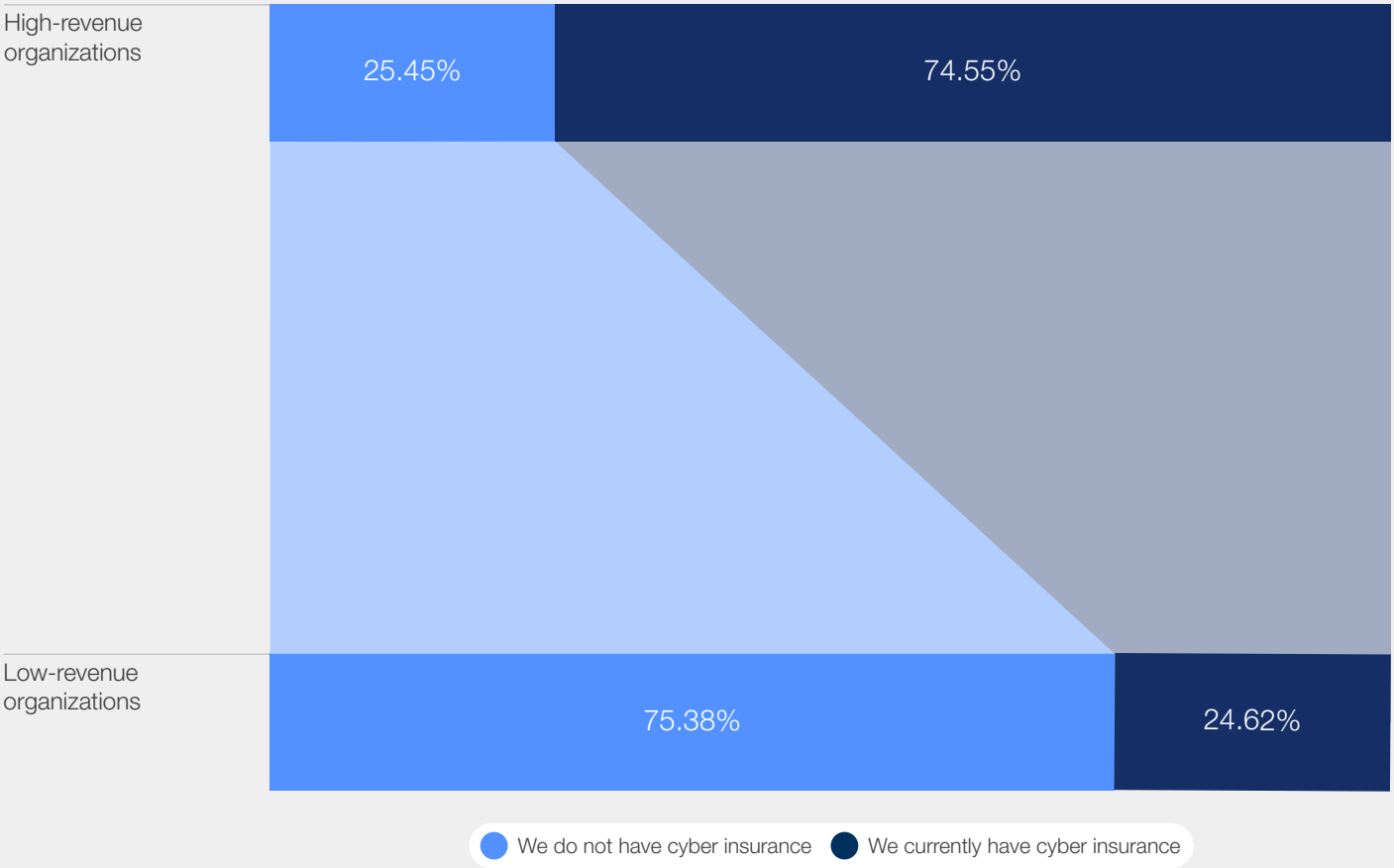
BOX 4 **The SCRE initiative**

The World Economic Forum Systems of Cyber Resilience: Electricity (SCRE) Initiative works towards tackling the challenges of fragmented and conflicting regulations. The SCRE community has recently provided a "Response to the White House's Request on Harmonizing Cybersecurity Regulations"[46] and in the past at the request of the European Commission also offered a response to the Commission's cybersecurity package, "Commentary in the Light of Recent Sophisticated Supply Chain Attacks".[47] The SCRE community has also put together a position paper, "Facilitating Global Interoperability of Cyber Regulations in the Electricity Sector",[48] to support regulators to build a more secure, resilient and standardized approach to cyber regulations globally.

5.3 The role of insurance

Similar to the role of regulatory bodies, the insurance industry is also instrumental in mitigating and containing risks throughout the ecosystem. Cyber insurance is a valuable tool for defraying the financial harm inevitable in any cyber-resilience strategy, and in many cases provides crucial support in ensuring sufficient and effective investment in cybersecurity. Yet the number of organizations that hold a cyber-insurance policy has dropped by 24% overall since 2022, with feedback from expert workshops in 2023 suggesting that, even for larger organizations, insurance is sometimes not economically viable and that security budgets can be more usefully spent elsewhere. The causes of this disparity become obvious when viewed through the lens of revenue.

FIGURE 13 **Organizations that report having cyber insurance by revenue**



There have been calls for greater transparency in the insurance industry, especially when it comes to methods of rate-setting and incentivizing cyber behaviours through reduced premiums. Collaboration both within the industry and with civil-society counterparts will be needed to address skyrocketing costs. Either way, collaboration between the industry's policy consumers and its providers to increase ecosystem resilience would benefit the market and contribute to the baseline cyber-resilience capability in these ecosystems.

As Davis Hake, the Co-Founder and Vice-President of Policy at Resilience Insurance, stated:

> **If insurance can transform more into a risk management solution, you're going to see cyber insurance as a driver for not only incentivizing companies to be safer, but as something that every company that wants to address this risk needs to have.**

5.4 Understanding cyber resilience in the supply chain

54%
of organizations have insufficient visibility into the vulnerabilities of their supply chain.

When it comes to the supply chain, which is one of the areas that demands the most collaboration, 54% of organizations fail to understand cyber vulnerability in their supply chain sufficiently – and it shows. Furthermore, 51% of leaders say that their supply-chain partners have not asked them for proof of their cybersecurity posture. It seems that many organizations do not know the extent of their supply-chain cyber risk because they do not ask.

Cyberattackers are taking notice of this weakness. The MOVEit attacks in June 2023 are a perfect illustration of the importance of knowing your supply chain. This one attack affected millions of individuals and thousands of organizations. Through the payment of ransomware funds, it was estimated to gain the group behind the attack, Cl0P, millions of dollars.

It was not just the payment of the ransom that Cl0P was pursuing: large amounts of personal identifiable data, including social security numbers, medical records and financial information were stolen during the attack.[49] For most organizations, a more comprehensive understanding of their supply chain, its vulnerabilities and its risk could have mitigated some of the colossal damage from this single attack.

The picture gets sharper when organization size is included in the analysis. Some 71% of the smallest organizations by annual revenue have not been asked to prove their cyber posture by their supply chain partners in the past 12 months. The picture is reversed for the largest organizations by annual revenue: 71% have been asked for proof in the past 12 months.

As Christophe Blassiau, Senior Vice-President, Cybersecurity and Product Security, Global CISO and CPSO, of Schneider Electric, stated:

> **The cyber maturity gap between large corporations and medium/small companies is constantly widening, creating a systemic supply-chain security risk. Global companies must have a larger play in raising the bar for their smaller partners to prevent them from becoming threat vectors.**

41%
of organizations that suffered a material impact from a cyberattack said it originated from a third party.

Curiously, even the 64% of executives who believe that their organization's cyber resilience meets (but does not exceed) its minimum requirements to operate say they still have an inadequate understanding of their supply-chain cyber vulnerabilities. The question that follows is, can an organization truly meet its baseline standard of cyber resilience if it is partially oblivious to where and how its ecosystem puts it at risk?

In the end, one result of an ecosystem that is often under-informed about its risk, under-insured and sceptical about the future of collaborative progress is this: 41% of the organizations that suffered a material incident in the past 12 months say that a third party caused it.

To begin to tackle this issue, the World Economic Forum Systems of Cyber Resilience: Electricity (SCRE) Initiative (the first of its kind) published a report defining cybersecurity-related roles and responsibilities throughout the electricity industry's value and supply chain, based on consensus among major stakeholders in the industry.[50]

Conclusion

The struggle to maintain high-quality – or even adequate – cyber-resilience capability is fast becoming a zero-sum game.

The ability to cultivate best practices, to compete for sufficient talent and, in some cases, simply to afford the right tools and services, is increasingly determining which organizations win and which lose out. As a result, the organizations most lacking can least accomplish it. A secure supply chain requires all organizations to meet a minimum viability for a truly secure ecosystem, but the inequity that exists today makes it vulnerable.

Yet it does not have to be this way and there are many reasons to be optimistic about the near future. Prudent cyber-resilience practices – the fundamentals that cyber professionals and prescient business executives have learned are wise – are slowly but surely working. Nonetheless, something must still change the current trajectory

Otherwise, as seen throughout 2023, early adoption of new technology by leading-edge organizations, the struggle by those on the underside of the curve to keep pace with foundational capabilities for trust and security, and fragmented incentives within digital ecosystems will accelerate digital disparity in the coming years.

Furthermore, the interconnection of the digital economy makes it inevitable that the negative effects will compound, affecting everyone. Therefore, everyone needs to work together to encourage sustainable capability for the future – including developing the right priorities and organizational culture while providing for equitable access to talent, technology and security tools. Raising systemic resilience – all organizations closing the inequities that divide and improving the resilience of what connects – is not only the most pressing requirement, it is the greatest responsibility.

Appendix: Methodology

The primary dataset used as the foundational research was a 23-question survey with eight demographic questions, the Global Cybersecurity Outlook Survey, which was launched in June 2023 and ran until October 2023. The World Economic Forum received 204 survey participants from 49 countries. Once the dataset was normalized using the eight demographic questions to determine the qualifications of the participants, the dataset was left with 199 qualified participants. Each of the 199 participants fully completed the survey.

As additional qualitative data, the Forum performed 14 one-on-one interviews with C-suite executives, asking adjacent or supplemental questions to probe further into the survey data collected.

In October 2023, a 90-minute workshop was held with 37 executives, focused on the themes identified within this report. This data was used as qualitative data within the report. Additional quantitative data was collected in the form of a two-question poll posed to the attendees.

The Forum's Annual Meeting on Cybersecurity was held on 14–16 November 2023. Several sessions were held, and qualitative data was gathered from the 140-plus executives that attended the event. During the closing plenary, quantitative data was gathered in a form of a two-question poll for the audience.

Contributors

Lead Authors

Gretchen Bueermann
Knowledge Lead, Centre for Cybersecurity, World Economic Forum, Switzerland

Michael Rohrs
Security Senior Manager, Accenture, USA

World Economic Forum

Sean Doyle
Lead, Cybercrime Atlas Initiative, Centre for Cybersecurity, Switzerland

Tal Goldstein
Head of Strategy, Centre for Cybersecurity, Switzerland

Campbell Powers
Data Fellow, Switzerland

Accenture

Taylor Browder
Security Manager, USA

Lauren Stockton
Security Senior Analyst, USA

Acknowledgements

World Economic Forum

Filipe Beato
Lead, Centre for Cybersecurity

Joanna Bouckaert
Community Lead, Centre for Cybersecurity

Akshay Joshi
Head of Industry and Partnerships, Centre for Cybersecurity

Giulia Moschetta
Research and Analysis Specialist, Centre for Cybersecurity

Natasa Perucica
Project Lead, Centre for Cybersecurity

Luna Rohland
Community Coordinator, Centre for Cybersecurity

Kesang Tashi Ukyab
Lead, Cyber Resilience, Electricity

Additional acknowledgements

Bushra Alblooshi
Senior Consultant, Research and Innovation, Dubai Electronic Security Center, UAE

Hoda Al Khzaimi
Director, Centre for Cybersecurity; Founder and Director, EMARATSEC, New York University Abu Dhabi, UAE

Ajay Bhalla
President, Cyber and Intelligence Solutions, Mastercard, United Kingdom

Christophe Blassiau
Senior Vice-President, Cybersecurity & Product Security, Global Chief Information Security Officer and Chief Product Security Officer, Schneider Electric, France

Kris Burkhardt
Chief Information Security Officer, Accenture, USA

Paolo Dal Cin
Global Lead, Accenture Security, Italy

J. Michael Daniel
President & Chief Executive Officer, Cyber Threat Alliance, USA

Dorit Dor
Chief Technology Officer, Check Point Software Technologies, Israel

Cathy Foley
Chief Scientist, Australian Government, Australia

Janus Friis
Chief Digital Risk Officer, PensionDanmark, Denmark

Öykü Işık
Professor, Digital Strategy and Cybersecurity, IMD Business School, Switzerland

Yurie Ito
Founder and Executive Director, CyberGreen Institute, USA

Davis Hake
Co-Founder and Vice-President of Policy, Resilience Insurance, USA

Rotem Iram
Co-Founder and Chief Executive Officer, At-Bay, USA

Ciaran Martin
Professor of Practice in the Management of Public Organisations, Blavatnik School of Government, University of Oxford, United Kingdom

Lindiwe Matlali
Chief Executive Officer, Africa Teen Geeks, South Africa

James Nunn-Price
Senior Managing Director – Growth Markets Security Lead, Accenture, Australia

Kunal Purohit
Chief Digital Service Officer, Tech Mahindra, India

Abhay Raman
Senior Vice-President & Chief Security Officer, Sunlife Insurance, Canada

Giovanni Salvi
Data Intelligence Manager, World Economic Forum, Switzerland

Andreas Schmitt
Global Manager, Cyber Underwriting, Zurich Insurance, Switzerland

Vikram Sharma
Founder and Chief Executive Officer, QuintessenceLabs, Australia

Leo Simonovich
Vice-President & Global Head of Industrial Cyber and Digital Security, Siemens Energy, USA

Mark Swift
Group Chief Information Security Officer, Trafigura, United Kingdom

Akhilesh Tuteja
Global Cyber Security Practice Co-Leader, KPMG, India

Wendi Whitmore
Senior Vice-President, Unit 42, Palo Alto Networks, USA

Aleksandr Yampolskiy
Chief Executive Officer, SecurityScorecard, USA

With thanks to the Members of the Global Future Council on Cybersecurity and Chief Information Security Officer Community.

Endnotes

1. Gartner, “Gartner Identifies Three Factors Influencing Growth in Security Spending”, 13 October 2022: https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i.
2. Organisation for Economic Co-operation and Development, “OECD Economic Outlook, Interim Report September 2023: Confronting Inflation and Low Growth”, 12 September 2023: https://www.oecd-ilibrary.org/sites/1f628002-en/index.html?itemId=/content/publication/1f628002-en.
3. The category of smallest organizations by annual revenue in the 2024 GCO data is <$250 million.
4. In general in this report, “business leaders” refer to CEOs, chairs, presidents and board members, while “cyber leaders” refers to CISOs, CSOs and other security focused leaders.
5. Gartner, “Gartner Identifies Three Factors Influencing Growth in Security Spending”, 13 October 2022: https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i.
6. OECD, “OECD Economic Outlook, Interim Report September 2023: Confronting Inflation and Low Growth”, 12 September 2023: https://www.oecd-ilibrary.org/sites/1f628002-en/index.html?itemId=/content/publication/1f628002-en.
7. The category of smallest organizations by annual revenue in the 2022 GCO data is <$500 million, and the largest organizations by annual revenue in the 2022 GCO data are +$5.5 billion.
8. SecurityScorecard, “Cyentia Institute and SecurityScorecard Research Report: Close Encounters of the Third (and Fourth) Party Kind”: https://securityscorecard.com/research/cyentia-close-encounters-of-the-third-and-fourth-party-kind/.
9. Trey Herr et al., “Buying Down Risk: Cyber Poverty Line”, Atlantic Council, 3 May 2022: https://www.atlanticcouncil.org/content-series/buying-down-risk/cyber-poverty-line/.
10. United Nations, “Widening Digital Gap between Developed, Developing States Threatening to Exclude World’s Poorest from Next Industrial Revolution, Speakers Tell Second Committee”, 6 October 2023: https://press.un.org/en/2023/gaef3587.doc.htm.
11. World Economic Forum, “Cybercrime Prevention Principles for Internet Service Providers”, 23 January 2020: https://www.weforum.org/publications/cybercrime-prevention-principles-for-internet-service-providers/.
12. Gretchen Bueermann and Daniel Dobrygowski, “From Deepfakes to Social Engineering, Here’s What to Know about Elections, Cybersecurity and AI”, 8 November 2023: https://www.weforum.org/agenda/2023/11/elections-cybersecurity-ai-deep-fakes-social-engineering/.
13. Ibid.
14. Ibid.
15. A malware family is a group of applications with similar attack techniques.
16. Fortinet, “Global Threat Landscape Report”, August 2023: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2023.pdf.
17. United States House Committee on Science, Space and Technology, “Support Grows for the National Quantum Initiative Reauthorization Act”, 13 November 2023: https://science.house.gov/2023/11/support-grows-for-the-national-quantum-initiative-reauthorization-act.
18. World Economic Forum, “Global Cybersecurity Outlook 2022”, January 2022: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.
19. Economic Times, “Beware: Cybercriminals Using ‘Limitless’ AI Tools Like FraudGPT or WormGPT for Frauds”, 31 July 2023: https://economictimes.indiatimes.com/news/india/beware-cybercriminals-using-limitless-ai-tools-like-fraudgpt-or-wormgpt-for-frauds/articleshow/102277128.cms.
20. Snir Kodesh, “When MFA Isn’t Actually MFA”, Retool, 13 September 2023: https://retool.com/blog/mfa-isnt-mfa.
21. Ibid.
22. Emily Cahill, “What’s the Difference Between Phishing, Smishing and Vishing?”, Experian, 20 March 2022: https://www.experian.com/blogs/ask-experian/phishing-smishing-vishing/.
23. Goldman Sachs, “Generative AI Could Raise Global GDP by 7%”, 5 April 2023: https://www.goldmansachs.com/intelligence/pages/generative-ai-could-raise-global-gdp-by-7-percent.html.
24. Gemma Roden, Marjorie Chinen and Diego Angel-Urdinola, “Unleashing the Metaverse for Skills and Workforce Development”, World Bank, 12 September 2023: https://blogs.worldbank.org/education/unleashing-metaverse-skills-and-workforce-development.
25. Ipek Ozkaya, Anita Carleton, John E. Robert and Douglas Schmidt, “Application of Large Language Models (LLMs) in Software Engineering: Overblown Hype or Disruptive Change?”, 2 October 2023: https://insights.sei.cmu.edu/blog/application-of-large-language-models-llms-in-software-engineering-overblown-hype-or-disruptive-change/.
26. Splunk, “The CISO Report”, 2023: https://www.splunk.com/en_us/pdfs/gated/ebooks/the-ciso-report.pdf.
27. Ian Shine, “These Are the Jobs that AI Can’t Replace”, World Economic Forum, 17 May 2023: https://www.weforum.org/agenda/2023/05/jobs-ai-cant-replace/.

28. The International Information System Security Certification Consortium, or ISC2, is a non-profit organization that specializes in training and certifications for cybersecurity professionals.
29. ISC2, "How the Economy, Skills Gap and Artificial Intelligence Are Challenging the Global Cybersecurity Workforce", 2023: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4.
30. Ibid.
31. Fortinet, "2022 Cybersecurity Skills Gap Survey", 2022: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf.
32. Help Net Security, "Many Adults Want to Reskill for Cybersecurity Careers", 11 September 2018: https://www.helpnetsecurity.com/2018/09/11/reskill-cybersecurity-careers/.
33. World Economic Forum, "Future of Jobs Report 2023", May 2023: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf.
34. Statista, "Requirement of University Degree for Cybersecurity Jobs Worldwide from 2021 to 2022, by Region": https://www.statista.com/statistics/1322395/cybersecurity-university-requirement-worldwide/.
35. World Economic Forum, "Principles for Board Governance of Cyber Risk", March 2021: https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/.
36. Sarah Braithwaite, "ALPHV: Hackers Reveal Details of MGM Cyber Attack", University of Hawai'i-West O'Ahua, 24 October 2023: https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/alphv-hackers-reveal-details-of-mgm-cyber-attack/.
37. Fortinet, "2023 State of Operational Technology and Cybersecurity Report", 2023: https://www.fortinet.com/resources-campaign/secure-ot/2023-state-of-operational-technology-and-cybersecurity-report-2.
38. World Economic Forum, "Principles for Board Governance of Cyber Risk", March 2021: https://www.weforum.org/publications/principles-for-board-governance-of-cyber-risk/.
39. Fortinet, "Global Threat Landscape Report", August 2023: threat-report-1h-2023.pdf (fortinet.com).
40. Accenture, "The Cyber-Resilient CEO", October 2023: https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-The-Cyber-Resilient-CEO-Final.pdf.
41. Minister for Home Affairs and Minister for Cyber Security, "Small Businesses to Receive Cyber Security Boost", 20 November 2023: https://ministers.treasury.gov.au/ministers/julie-collins-2022/media-releases/small-businesses-receive-cyber-security-boost.
42. European Cybersecurity Competence Centre and Network, "About Us": https://cybersecurity-centre.europa.eu/about-us_en.
43. Directorate-General for Communications Networks, Content and Technology, "The ECCC and NCC-BE Join Forces to Raise Cybersecurity Awareness", 10 November 2023: https://cybersecurity-centre.europa.eu/news/eccc-and-ncc-be-join-forces-raise-cybersecurity-awareness-2023-11-10_en.
44. United States Attorney's Office, Northern District of California, "Former Chief Security Officer of Uber Convicted of Federal Charges for Covering Up Data Breach Involving Millions of Uber User Records", 5 October 2022: https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach.
45. US Securities and Exchange Commission, "SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures", 30 October 2023: https://www.sec.gov/news/press-release/2023-227.
46. World Economic Forum, "Response to the White House's Request on Harmonizing Cybersecurity Regulations", 23 October 2023: https://www.weforum.org/publications/response-to-the-white-houses-request-on-harmonizing-cybersecurity-regulations/.
47. World Economic Forum, "European Commission Cybersecurity Package: Commentary in Light of Recent Sophisticated Supply Chain Attacks", June 2021: https://www3.weforum.org/docs/WEF_Commentary_in_light_of_recent_sophisticated_supply_chain_attacks_2021.pdf.
48. World Economic Forum, "Facilitating Global Interoperability of Cyber Regulations in the Electricity Sector", 17 November 2023: https://www.weforum.org/publications/facilitating-global-interoperability-of-cyber-regulations-in-the-electricity-sector/.
49. Resilience, "2023 Mid-Year Cyber Claims Report", 2023: https://unlock.cyberresilience.com/2023_midyear_claims_report.
50. World Economic Forum, "Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain", November 2020: https://www.weforum.org/publications/cyber-resilience-in-the-electricity-ecosystem-securing-the-value-chain/.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org