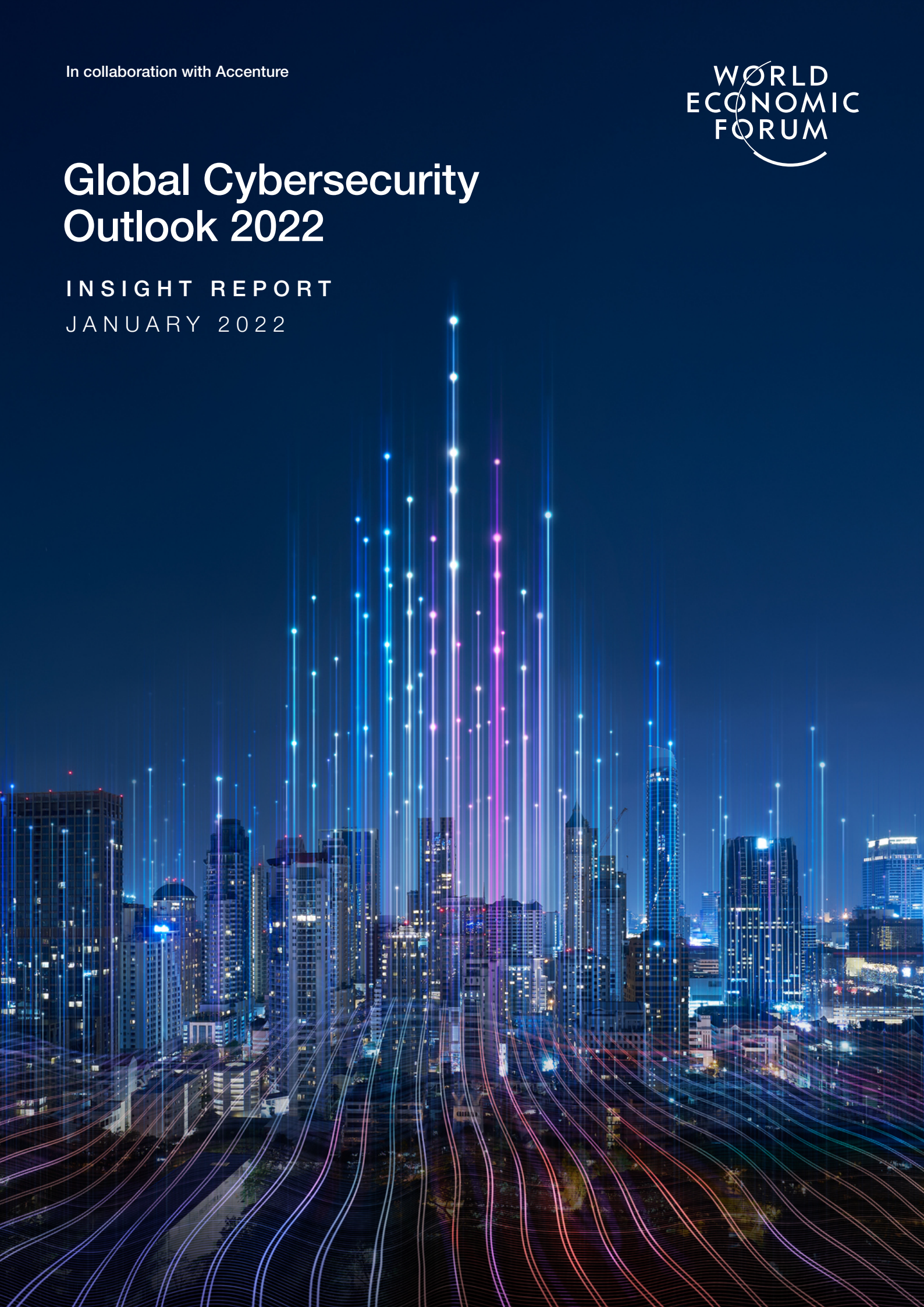
In collaboration with Accenture

WORLD ECONOMIC FORUM

Global Cybersecurity Outlook 2022

INSIGHT REPORT

JANUARY 2022



Cover: @Quardia/Gettyimages

Contents

Preface

Jeremy Jurgens
Managing Director
World Economic Forum

As human behaviour and interaction continue to be shaped by increasingly ubiquitous technologies, organizations must continuously adapt their capabilities to deal with and prevent malicious actors from taking advantage of the shifting technological landscape. Cybersecurity must be prioritized in all domains of society and the economy if we are to unlock the true potential of the digital economy. Cybersecurity is not a separate technology but rather a foundational set of systems spanning technology, people and processes for the Fourth Industrial Revolution.

The accelerated shift to remote working during the COVID-19 pandemic coupled with recent high-profile cyberattacks have resulted in bringing cybersecurity top of mind among key decision-makers in organizations and nations. Despite the growing cognizance of cyber risks, decision-makers and cyber experts are often not on the same page in terms of prioritizing cybersecurity, integrating cyber risk into business strategy and integrating cyber leaders into business processes. Much still needs to be done to arrive at a shared understanding of how to strengthen cyber resilience.

Building cyber resilience is a core focus of the World Economic Forum Centre for Cybersecurity. We bridge the gap between cybersecurity experts and decision-makers at the highest levels to reinforce the vital importance of cybersecurity as a key strategic priority.

In 2021, the Centre engaged over 120 global cyber leaders to generate high-level insights on emerging cyber threats. Taking the global pulse on the state of cybersecurity is essential to clearly identifying the emerging risks and developing actionable solutions to address them. The aim of this report is to provide an in-depth analysis of the challenges that security leaders are dealing with, the approaches they are taking to stay ahead of cybercriminals and the measures they are implementing to enhance cyber resilience not only within their organizations but also within the wider ecosystem.

Cyberspace transcends borders. We therefore need to mobilize a global response to address systemic cybersecurity challenges. We hope the insights in this report will serve to foster collaborative approaches to building cyber-resilient ecosystems.

Foreword

Kelly Bissell
Global Lead, Accenture
Security, Accenture

The Global Cybersecurity Outlook will be an annual report highlighting the trends and progression as organizations begin to shift from a cyber-defensive posture to a stronger cyber-resilience position. As our cyber ecosystems expand and integrate, it is becoming more important to ensure all organizations can anticipate, recover and adapt quickly to cyber incidents. Security-focused leaders must be able to communicate their risk and mitigation strategies effectively and clearly to business leaders.

We surveyed 120 global cyber leaders from 20 countries across the World Economic Forum Cybersecurity Leadership Community and the Accenture Cybersecurity Forum, to gain a global perspective on how cyber resilience is being perceived and implemented, and how they can better secure our ecosystems, together. To build an ecosystem resilient enough to withstand and not falter in today's environment will need a unified approach.

As identified in our survey and workshops, leadership support is critical to adopting cyber resilience within an organization. Also identified, and equally important, is ensuring there are no communication or coordination gaps between cybersecurity and business leaders. Given that technologies are constantly shifting and evolving at a rapid pace, spurred by machine learning and automation advancements, combined with increasingly capable and affordable hacking resources available to cybercriminals, leaders must be united and synchronized in their cyber resilience initiatives.

In partnership with the World Economic Forum Centre for Cybersecurity, it is our goal to provide insights and solutions to build stronger ecosystems from which organizations can benefit, learn from and move into this highly connected and digital future with confidence.

Executive Summary

At the time of writing, digital trends and their exponential proliferation due to the COVID-19 pandemic have thrust the global population onto a new trajectory of digitalization and interconnectedness. One of the starkest and most troubling new consequences of our digitalized existence is the increasingly frequent, costly and damaging occurrence of cyber incidents, sometimes even paralyzing critical services and infrastructure. This trend shows no signs of slowing, notably as sophisticated tools and methods become more widely available to threat actors at relatively low (or in some cases no) cost.

Signs of increasing digitalization are everywhere. The International Telecommunication Union recently reported that fixed broadband access has increased significantly on all continents as a direct result of teleworking, distance learning, remote entertainment and telemedicine.[1] Most technologically advanced countries prioritized the expansion of digital consumer tools, fostering digital entrepreneurial ventures and investing in innovation across universities, businesses and digital authorities[2] whereas emerging economies prioritized increasing mobile internet access, training digital talent and generating investment in R&D and digital enterprises. This begs a question: How will smaller and less powerful countries protect themselves and their natural resources if they are not able to protect their digitally connected infrastructure? The cybersecurity poverty line question becomes even more pressing in the ever-increasing surge of connectivity.[3]

Considering these ongoing cyber challenges, the World Economic Forum Centre for Cybersecurity engaged the Cybersecurity Leadership Community consisting of 120 cyber leaders who are senior-most executives from private and public sectors representing 20 countries. The focus of the Centre for Cybersecurity's work was to gather data via a Cyber Outlook Survey and the Cyber Outlook Series (see Appendix) and analyse it to understand cyber leaders' perceptions, and the trajectory of cybersecurity and cyber resilience.

The results of the analysis shed light on valuable insights about the state of cyber and perceptions about the current path of cyber resilience.

Key findings include:

1. While many factors are driving cybersecurity policies forward, we identified through our survey that 81% of respondents believe that digital transformation is the main driver in improving cyber resilience. The accelerating pace of digitalization due to the COVID-19 pandemic and the shift of our working habits is pushing cyber resilience forward. As many as 87% of executives are planning to improve cyber resilience at their organization by strengthening resilience policies, processes and standards for how to engage and manage third parties.

2. Our research revealed three main and critical perception gaps between security-focused executives (chief information security officers), and business executives (chief executive officers). The gaps are the most visible in three areas:

   2.1 *Prioritizing cyber in business decisions*; while 92% of business executives surveyed agree that cyber resilience is integrated into enterprise risk-management strategies, only 55% of security-focused leaders surveyed agree with the statement.

   2.2 *Gaining leadership support for cybersecurity*; 84% of respondents share that cyber resilience is considered a business priority in their organization with support and direction from leadership, but a significantly smaller proportion (68%) see cyber resilience as a major part of their overall risk management. Due to this misalignment, many security leaders still express that they are not consulted in business decisions which results in less secure decisions and security issues. This gap between leaders can leave firms vulnerable to attacks as a direct result of incongruous security priorities and policies.

   2.3 *Recruiting and retaining cybersecurity talent*; our survey found that 59% of all respondents would find it challenging to respond to a cybersecurity incident due to the shortage of skills within their team. While the majority of respondents ranked talent recruitment and retention as their most challenging aspect, business executives appear less acutely aware of the gaps than their security-focused executives, who perceive their ability to respond to an attack with adequate personnel as one of their main vulnerabilities.

3. The threat of ransomware continues to grow. As many as 80% of cyber leaders stressed that ransomware is a dangerous and evolving threat to public safety. The survey confirmed that ransomware attacks are at the forefront of cyber leaders' minds, with 50% of respondents indicating that ransomware is one of their greatest concerns when it comes to cyber threats. Ransomware attacks are increasing in frequency and sophistication, and this ever-present threat is keeping cyber leaders up at night. Ransomware attacks are followed by social-engineering attacks as the second-highest concern for cyber leaders; number three on this list is malicious insider activity. A malicious insider is defined as an organization's current or former employees, contractors or trusted business partners who misuse their authorized access to critical assets in a manner that negatively affects the organization.

4. Small and medium-sized enterprises (SMEs) are seen as a key threat to supply chains, partner networks and ecosystems. In our research, 88% of respondents indicate that they are concerned about cyber resilience of SMEs in their ecosystem.

5. Cyber leaders have indicated that clear and productive regulations are needed, that would allow and encourage information sharing and collaboration. The value of partnerships is proven; over 90% of respondents report receiving actionable insights from external information-sharing groups and/or partners.

   This report uses a retrospective analysis of recent years to share the knowledge and concerns of cyber leaders with one goal: helping decision-makers prepare for the next generation of cyberattacks.

Below: @your_photo
Gettymimages

> **“Throughout the past year, we have received stark reminders that malicious cyber activity threatens our national and economic security and impacts the daily lives of individuals, communities and organizations around the world. The World Economic Forum’s Global Cybersecurity Outlook 2022 helps leaders understand the evolving threats we face and develop concrete solutions to enhance their own security and increase cybersecurity resilience worldwide.”**
>
> Alejandro N. Mayorkas, Secretary, US Department of Homeland Security, USA

> **“Looking ahead to 2022-2023, cybersecurity must be seen as a strategic business issue that impacts decision-making. To mitigate risks like ransomware and social engineering, organizations must ask not simply how they are protected, but how well – with an eye to strength, sophistication and efficacy.”**
>
> Nancy Luquette, EVP, Chief Risk and Compliance Officer, S&P Global, USA

Image: @Quardia/ Gettymimages

“The rise of supply chain threats and escalating ransomware attacks are the most pressing cyber challenges the international community needs to address. Business leaders must consider cybersecurity as a risk management issue and balance the trade-offs between security, usability and cost at the Board or C-suite level.”

David Koh, Commissioner of Cybersecurity and Chief Executive, Cyber Security Agency (CSA), Singapore

“The well-being of every person, organization and country depends on the application and security of digital technologies. If introduced and developed in a secure manner, they can bring stability, prosperity and would significantly raise the quality of life. However, if security is not prioritized, they can be the root cause of various kinds of problems. This is true of all progress, so our goal is not to shy away from it but to apply new technologies with security in mind and take the global community to fantastic new heights.”

Stanislav Kuznetsov, Deputy Chairman of the Executive Board, Sberbank, Russian Federation

Image: @Quardia/ Gettymimages

59%

Cyber leaders say cyber resilience and cybersecurity are synonymous with the differences not well understood

2%
Not confident in cyber resilience

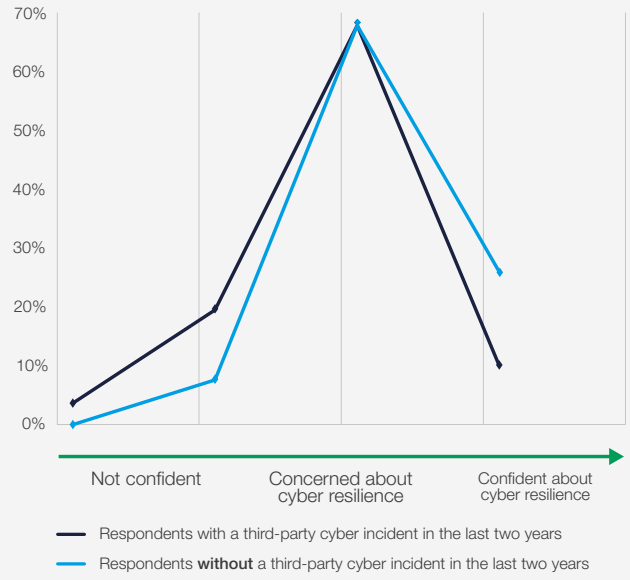
7%
Concerned about cyber resilience practices

74%
Perform cyber resilience practices with some inefficiencies

17%
Confident in cyber resilience

Over 90% of cyber leaders who say cybersecurity and cyber resilience are synonymous also believe they are resilient

Third-party cyber incidents reduce respondent confidence in their organization's resilience



Respondent confidence in their organization's cyber resilience in comparison to third-party resilience

Organizations affected by a third-party cyber incident in the past two years

55%
Have not been affected

39%
Have been affected

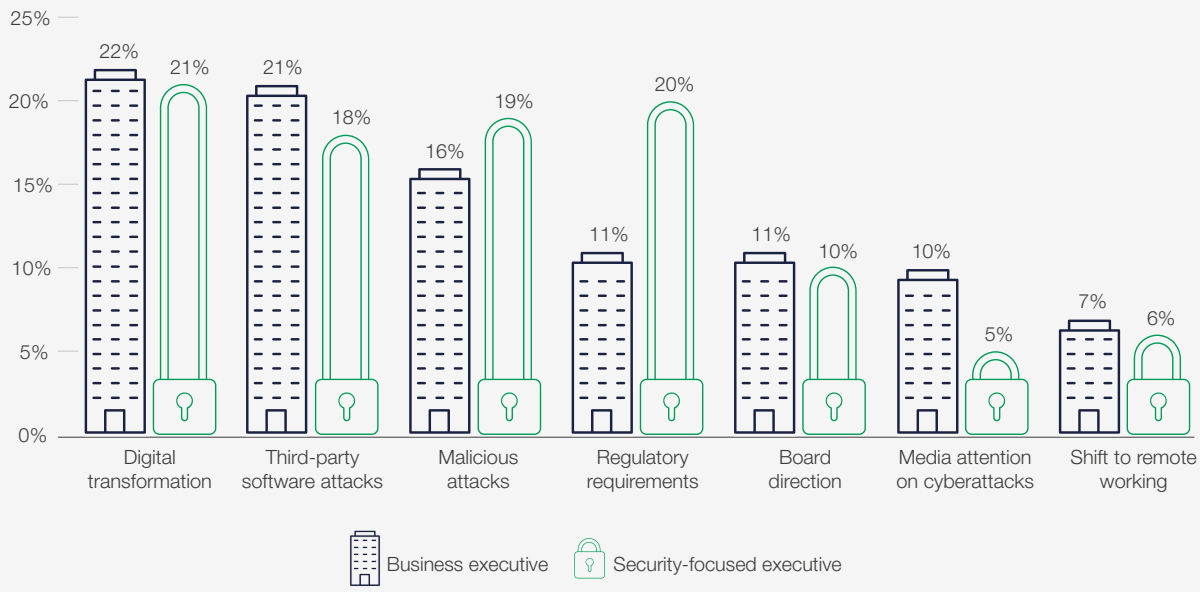
6%
Do not know

"Cyber resilience in my organization is integrated into enterprise risk management"

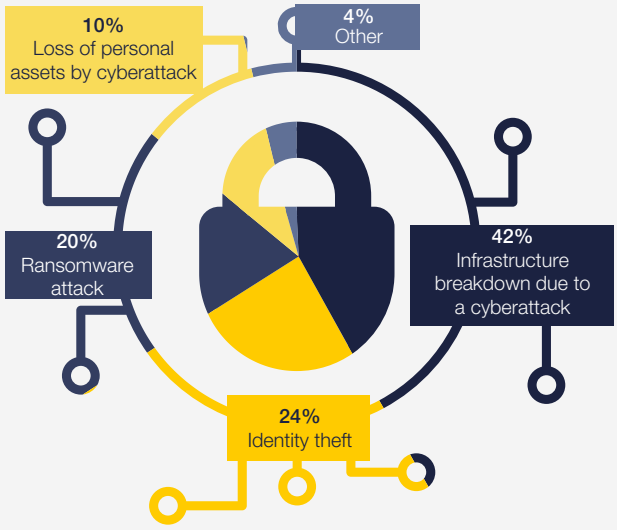
27%
Security-focused executives disagree with this statement

0%
Business executives disagree with this statement

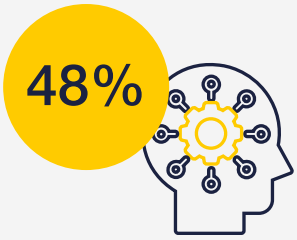
Business-focused and security-focused executives are aligned on what they believe will have the greatest influence on their organization's approach to cybersecurity next year



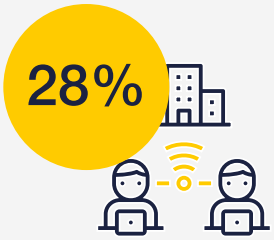
What are the personal cybersecurity concerns of cyber leaders?



What is expected to have the greatest influence on transforming cybersecurity in the next two years?



Automation and machine learning



Remote / hybrid work environment

1

Surveying the Landscape

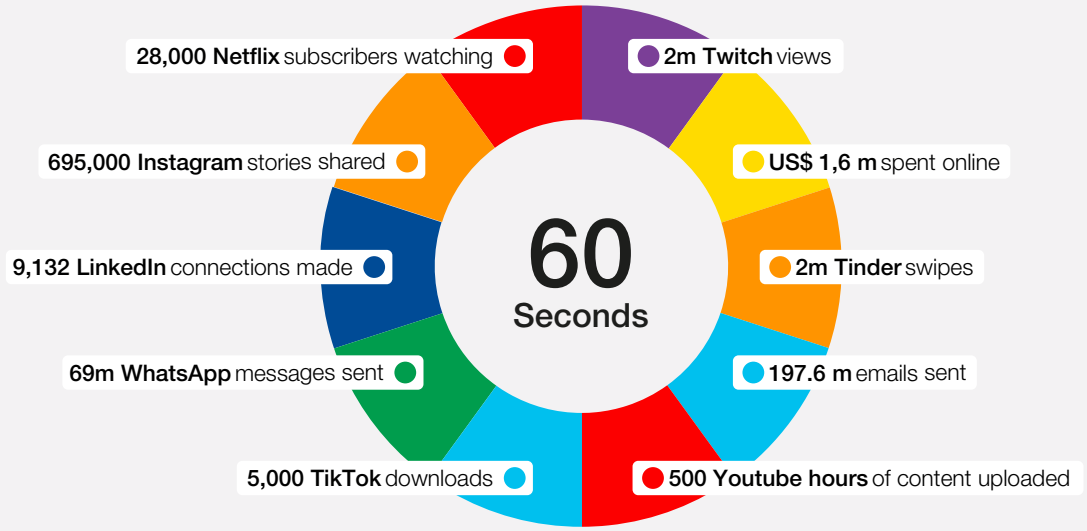
As the new normal continues to take shape, cyber breaches are becoming more frequent and more sophisticated.

Below: @matejmo/ Gettyimages

Most remarkably, recent changes have created an unprecedented increase in cyber dependence and technological innovation. As these dependencies continue to rise, the associated risks and threats now command the attention of all individuals and organizations who must take a more defensive position and seek clarity on their cyber presence and what they need to remain secure.

Substantial digital shifts can be seen in both personal and professional situations. Local businesses transitioning to e-commerce with their customers, online services are rising 50% in regions such as Africa, Latin America and China.[4] Organizations have rapidly accelerated the modernization of their technological capabilities using cloud services to quickly upscale to meet demand for remote access and collaboration. According to the OECD, most countries are reckoning with a drastic increase in network demand and changes in utilization habits since the onset of the COVID-19 pandemic. In Korea, operators have reported internet traffic increases of 13%, reaching 45% to 60% of their deployed capacity during the peak of the pandemic. In the US, internet service providers (ISPs) were granted approval by Federal Communication Commission regulators, reaching a commercial agreement with a satellite TV provider to borrow the company's unused wireless spectrum to add capacity and relieve congestion during months when most of the region's citizens were in isolation at the onset of the pandemic in 2020.

FIGURE 3 **Estimated amount of data created on the internet in one minute[6]**



Source: Loris Lewis via Allacces

As dependence on digital technologies continues to surge at a rapid rate, so does cybercrime. Cybercriminals are seizing every opportunity to exploit vulnerabilities against people and organizations through technology. They are more agile than ever; swiftly adapting new technologies, tailoring their attacks using novel methods and cooperating closely with each other. More familiar or "traditional" organized crime, like the "mafia", are undergoing a digital transformation of their criminal operating tactics. Many illegal "mafia"-type organizations are paying hackers to support criminal activities, including extortion and drug trafficking.[7] Europol recently reported that the organized crime groups recruited hackers for phishing, social engineering attacks, SIM swapping and sending malware to victims to gain control of bank accounts. Hiring cybercriminals for service is becoming a widely used and open practice. Additionally, organized crime groups often fold cybercriminals into lawful business operations, further obfuscating visibility between legitimate and criminal actors. These so-called employees are often located around the globe, which hinders possible disruption of such groups by law enforcement.

The dark web[8] is teeming with hacking services that offer comprehensive skills, affordable pricing and quick engagement timelines. Cybercriminals, also known as "blackhat" hackers, can be hired to break into social media accounts, erase debts and even change students' grades.[9] Prices for these services are often relatively affordable, especially considering the probability of personal or institutional damage. Prices tend to vary depending on the complexity of the required hacking activities, the desired outcome and the victim's profile. It is relatively straightforward, however, to build an array of services with a budget of US$ 1,000 or less. Typical prices for services such as social media account hacking average US$ 230, while website hacking and changing school grades range from US$ 394 to US$ 526.[10]

1.1 A new generation of breaches

The cost of breaches to an organization is high, amounting to an average of US$ 3.6 million per incident.[11] Perhaps even more troubling is the growing trend that companies need 280 days on average to identify and respond to a cyberattack.[12] To put this into perspective, an incident which occurs on 1 January may not be fully contained until 8 October. One example of how long it takes to even get to know about attacks surfacing the networks is the recent Emotet malware. Although law enforcement disrupted the Emotet malware and its infrastructure in January 2021, news of the malware showing a return to the threat landscape through existing botnets was circulating in November 2021. Hence, it can be anticipated that Emotet's impact – or Emotet-like malware – will make a comeback in 2022. Additionally, rapid evolvement in threat actors' techniques and capabilities are also leading towards advanced multistage ransomware. Moreover, the race between attackers and defenders is challenged by the rate of newly discovered and published security vulnerabilities in the most popular software tools and systems.

Breaches also apply pressure, reflect negative financial performance and stock price. One analysis using the NASDAQ found that, 14 market days after a breach becomes public, the average share price bottoms out and underperforms the NASDAQ by -3.5%. After six months, the average share price performance falls -3.0% against NASDAQ performance.[13]

The media plays a significant role in informing the public about cybersecurity issues. The dangers inherent in these types of cyberattacks and events, a formerly obscure topic, are becoming a more common subject in household conversation. Cyber news coverage has increased overall, but it spikes and wanes around major events.[14] As cyberattacks get more coverage and become more visible to average citizens and users, the result is often a newfound sowing of doubt in the minds of consumers, damage to company reputation and a trail of victims (both institutional and individual) suffering long-lasting consequences. Additionally, cybersecurity-related stories in the news are becoming more in-depth, reflecting a renewed interest in understanding this nuanced and complex topic more thoroughly. Concerns over the security of computers and networks are no longer limited to cyber experts alone, they are front-page news, part of political debate and on the agenda in board rooms globally.

Although most companies recover post-breach, some must shut down their business operations. Even those that recover from an incident pay a very high price both financially and in terms of reputation. Our research supports that ransomware attacks are on the minds of cyber leaders. When asked, "What type of cyberattack is your organization most concerned about?", respondents identified, in order of magnitude:

FIGURE 4 **Top three cyberattacks organizations are most concerned about**

"In the short term, we need to get ransomware under control. Poor cybersecurity makes too many of us easy targets. And the prevalence of cryptocurrencies makes it too easy for the criminals to collect their ransoms. Solving this will require changes on a variety of fronts. We need to better secure our networks, so we're not so easily victimized by this crime, obviously. But we need more regulation of cryptocurrencies, so criminals can't so easily hide their transactions. We need law enforcement to aggressively identify, charge and arrest the worst offenders. And we need global partnerships to eliminate the safe havens where these criminals can operate. Ransomware is a crime well-optimized to the Internet age; we need defense to up their game as well."

Bruce Schneier, Lecturer in Public Policy, John F. Kennedy School of Government, Harvard University, USA

Ransomware attacks saw a significant increase in the first six months of 2021, with global attack volume increasing by 151%.[15] The United States Federal Bureau of Investigation (FBI) has warned that there are now 100 different strains of ransomware in circulation globally. It is unlikely that this issue will diminish in pace or severity any time soon. There were on average, 270 attacks per organization in 2021, a 31% increase over 2020.[16] Cost is a major issue for organizations.

In fact, 81% of survey respondents contend that "staying ahead of attackers is a constant battle and the cost is unsustainable", compared with 69% in 2020.[17]

Even when it comes to personal cybersecurity, cyber leaders around the globe have listed ransomware, identity theft and critical infrastructure failure among their top personal cyber risk concerns.

FIGURE 5 **Top three cyberattacks cyber leaders are most personally concerned about**

Some of the solutions to the increasing threat of ransomware attacks are: employee cyber training (61%); offline backups (58%); and cyber insurance (57%).[18] Organizations should also seek out a platform-based cybersecurity solution that stops known ransomware threats across all attack vectors. This requires a layered security model that includes network, endpoint and data-centre controls powered by proactive global threat intelligence.

Increasingly, organizations are beginning to accept that cyber incidents will inevitably happen – adversaries are growing in number and appear to have increasingly sophisticated technologies at the ready. What is needed now is more than sophisticated protection. What is needed now is to improve the capacity to bounce back quickly from a cyber incident. This begs the question: How resilient are you?

1.2 The transition to cyber resilience

Corporate support for cyber resilience is getting stronger and more ubiquitous. Our survey shows more than 84% of respondents agree that "cyber resilience is considered a business priority for my organization with support and direction from leadership."

FIGURE 6 **Cyber leader confidence**

Say they are confident in their cyber resilience and have cyber resilience integrated into their enterprise risk management strategies

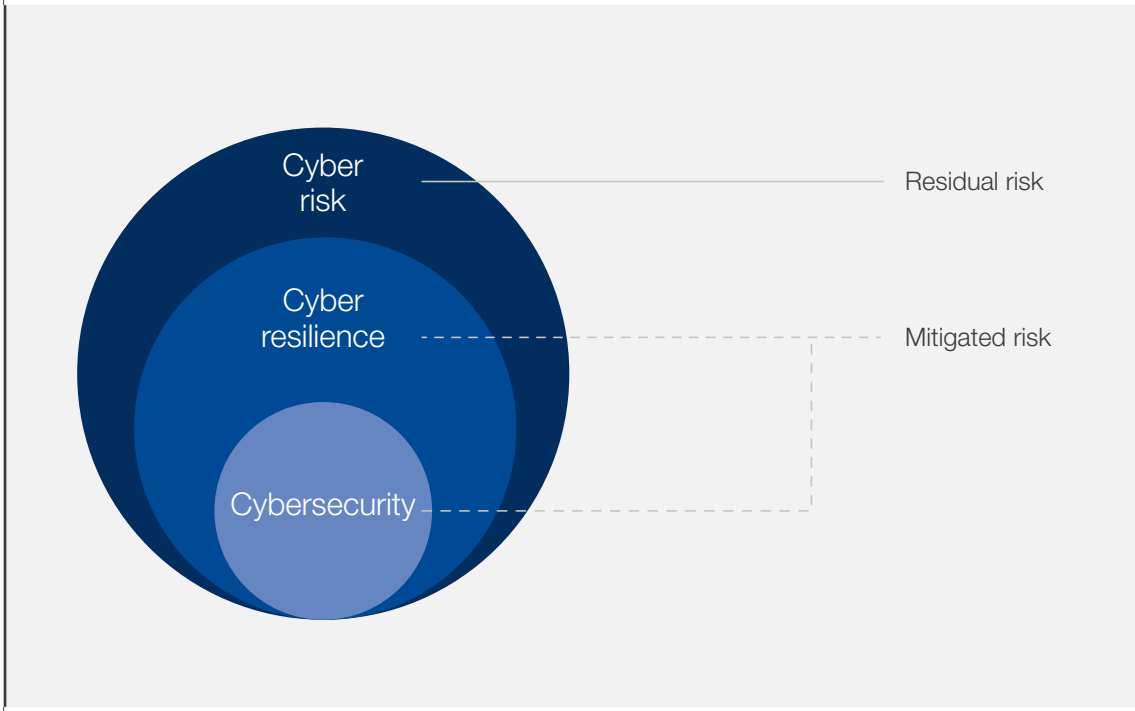
Sixty-seven per cent of cyber leaders indicate that they perform common cyber-resilience practices, though they acknowledge that some inefficiencies exist. Only 19% of cyber leaders feel confident that their organizations are cyber resilient. A high percentage (87%) of executives are responding internally to build more cyber resilience by strengthening resilience policies, processes and/or standards for how to engage third parties. About two-thirds (61%) will re-architect technical trust relationships and controls with their third parties (e.g., network connections, identity and access management for users, etc.). This data is very encouraging. We observe a real-time shift in mindset from cybersecurity to cyber resilience; that is, not only defending against cyberattacks, but also preparing for swift and timely incident response and recovery when an attack does occur.

Insurance is one of the solutions to reduce the impact of a cyber incident. It is one of the most widely used remedies: 71% of respondents currently have cyber insurance, either to limit financial liability for specific cyber incidents, and/or to benefit from incident response and cyber professional services made available through an insurance carrier. Moreover, 74% of respondents who show confidence in their cyber-resilience practices carry cyber insurance, compared to the 45% without coverage, and are concerned about their state of resilience. However, the level of maturity of the cyber-insurance markets differs widely across countries. In some regions it is standard practice, in others it is only emerging as a solution. Moreover, the cyber-insurance industry is undergoing a major shift. Due to emerging ransomware attacks and their volume, the average 2021 cyber insurance premium increase is 180%.[19]

Nonetheless, our survey suggests that there is still much to be done to establish the distinction between cybersecurity and cyber resilience; 59% of respondents indicate that cyber resilience and cybersecurity are synonymous, with their differences not well understood. With cyber resilience still being a relatively new concept to executive thinking, there is currently a lack of clarity as companies begin to discuss cyber resilience more frequently.

For the purposes of this report and in general, we define cyber resilience as **the ability of an organization to transcend (anticipate, withstand, recover from, and adapt to) any stresses, failures, hazards and threats to its cyber resources within the organization and its ecosystem, such that the organization can confidently pursue its mission, enable its culture and maintain its desired way of operating.**[20] We are at a crossroads, a point at which cyber resilience has become the defining mandate of our time – beyond foundational security controls – to anticipate future threats, withstand, recover from cyberattacks, and adapt to likely future digital shocks.

FIGURE 7 | **Relations between cyber risk, cyber resilience and cybersecurity**



This focal shift to cyber resilience will be a crucial development and objective in the next two years. Cyberattacks are inevitable, and at the core of any future-proof cybersecurity strategy stands resilience. Leaders must assume incidents are more likely than ever and that adversaries are now more capable of compromising or breaching systems or organizations. There will always be weakness and flaws in the system, operational environments and supply chains that adversaries will be able to exploit. There is a distinct imbalance between protecting a network and attacking it, and this imbalance continues to grow as more effective hacking resources become available at a significantly lower cost. But without continuous investment and commitment to cyber resilience, organizations will be more vulnerable to cyberattacks and thus more likely to endure reputational, financial, operational and safety impacts.

These developments have caused a profound reset and adjustment to the traditional expectations of cyber-risk management and its approaches. Survey respondents make clear that the rapidly changing digital landscape and the accompanying threats call for a transformation of how organizations, state authorities and individuals conceptualize and implement operational cyber resilience and develop preparedness and readiness tactics to combat the next generation of risks.

Below: @Milan_Jovic/ Gettyimages

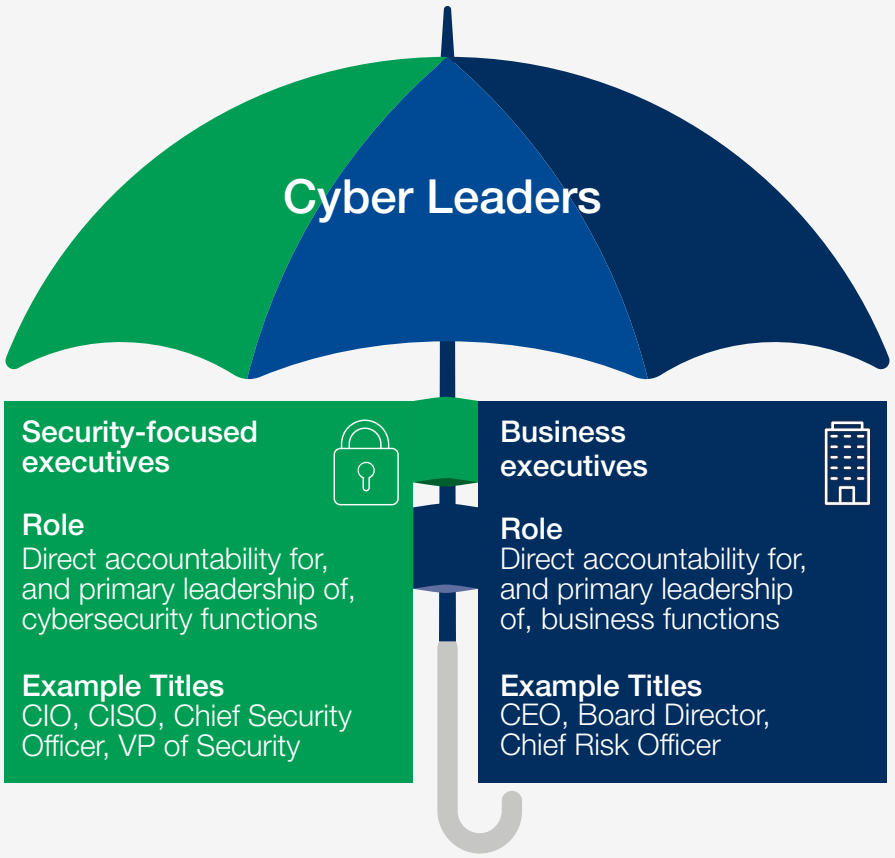
2

Bridging the Gap: Cyber and business

Cyber leaders are increasingly finding themselves in a precarious position as the gap between business and security leaders widens.

Adversaries are capitalizing on low-risk, high-reward opportunities during the pandemic, driving cybersecurity leaders to work tirelessly to protect their organizations from succumbing to persistent cyber threats. Cybersecurity teams need to be prepared and equipped to face evolving threats, defend and adapt within budget and, most importantly, retain talent. Cyber leaders must attune to new technological advancements and have visibility into both their own networks and the extended networks of their supply chains and third-party ecosystem. As the mandate of cybersecurity leaders evolves, the ability to juggle enabling and protecting critical business functions while absorbing anticipated disruptions and shocks from cyber incidents will be paramount.

FIGURE 8 **Cyber leaders: Security-focused and business executives**

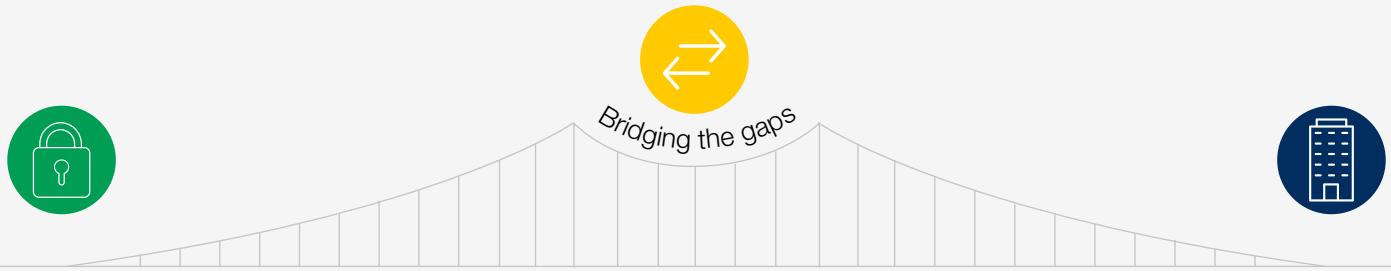


Note: Designations are based on primary role alignment and are not intended to imply lack of involvement, influence, leadership or accountability for business or cybersecurity functions, respectively.

The survey indicates that whereas about 85% of cyber leaders agree that cyber resilience is a business priority for their organization one of their most prominent challenges is to gain decision-makers' support when prioritizing cyber risks, against a plurality of other risks. These discordant results indicate that highlighting cyber resilience as a business priority alone is necessary but insufficient. It is up to cybersecurity leaders to drive the efforts, and then to corporate leadership to prioritize and integrate their proposals into broader business strategy.

Our research revealed three main gaps between a security-focused executive (e.g. chief information security officer), and a business executive (e.g. chief executive officer). In this chapter, the differences in perception and understanding of cyber resilience and operational cyber requirements will be explained from the standpoint of these two key corporate leadership roles.

FIGURE 9 **Three gap areas between security-focused and business executives**



Recommendations for security-focused executives		Recommendations for business executives
Develop a deep understanding of critical business operations Translate cyber risks into business impact	**Prioritizing cyber in business decisions**	Elevate cybersecurity and cyber resilience in business strategy Include security-focused executives into the corporate governance process
Ensure regular communication between cyber and business operations teams Become a strategic partner with business executives Understand the organization's risk appetite and align security strategy accordingly	**Gaining leadership support**	Provide sufficient cybersecurity budgets Frame cybersecurity as a strategic investment and business enabler Empower security-focused executives with the authority to protect business operations
Focus on retention. Take care of and protect cyber teams Communicate talent shortages and risks with leadership Drive initiatives for organic growth of security staff and skills within the organization	**Recruiting and retaining talent**	Ensure adequate compensation and incentives for cyber teams Accelerate HR process for recruiting and onboarding cyber talent Focus on career advancement and progression for cyber teams

2.1 Prioritizing cybersecurity in business decisions

To build the most efficient and business-friendly cyber programs, security-focused executives need to cultivate a deep understanding of critical business operations throughout the organization, including:

- A horizontal understanding of functions that are core to the organization's mandate and require the most attention and protection.[21]
- A vertical understanding, which encompasses cybersecurity principles and measures to implement that protect business operations and address intolerable risks.[22]

To acquire and sustain this knowledge, security-focused executives must regularly interact with different business units involving multiple stakeholders in the cybersecurity strategy development. Simultaneously, their peers from different business units should involve security-focused executives in various business conversations to ensure that cybersecurity is not an afterthought in an organization. Yet, security professionals feel they lack a strong voice when it comes to business decision-making. As Randy Herold, Chief Information Security Officer, Manpowergroup Inc. noted, "Cyber leaders are not consulted throughout business decisions which results in less secure decisions and security issues later on." These regular conversations and relationship-building between security and business executives will ensure that cyber-risk management becomes an integral part of daily decision-making.

Survey findings point to a pronounced and troubling disconnect between the views of cyber and business leaders on collaboration between and within organizations and the way forward when it comes to cyber-resilience practices and their efficacy.

FIGURE 10 **Differences in perceiving cyber resilience as a business priority**

To avoid these gaps, both executive groups need to create better two-way communication: including space to educate business executives on cyber risk and for business executives to inform and align with security-focused executives on business decisions and operations. It is nigh impossible to protect something that isn't fully understood, especially the core business priorities, and business executives cannot expect security-focused executives to perform without empowerment. The Forum's Centre for Cybersecurity is leading the Cybersecurity Risk Governance body of work focusing on developing tools for boards to continue fostering leaders' awareness, supported by a community of cyber-aware leaders to champion cybersecurity as an organizational priority, and develop the tools necessary for leaders to govern these new risks.

2.2 Gaining leadership support

One major challenge for security-focused leaders globally is gaining their organizational decision-makers' support. Leadership support includes primarily:

- Providing sufficient budget to meet cybersecurity priorities and needs
- Authorizing and empowering high levels of decision-making for security focused leaders
- Integrating security leaders in business decisions
- Aligning cybersecurity with organizational business objectives
- Including a security-focused leader on the board or appointing a board member whose personal KPIs (key performance indicators) would include cyber resilience.

> **"The increasing digitalization across governments and in the private sector poses existential risks to the world's digital economy. Cybersecurity leaders require the right skillset, tools and partnerships to assess these risks and to build resilient digital economies."**
>
> Albert Antwi-Boasiako, Acting Director-General, Cyber Security Authority (CSA), Republic of Ghana

This progress requires business executives to be fluent in cybersecurity and for security executives to demonstrate the criticality of cybersecurity as a business enabling function. Security professionals must identify and share weaknesses and gaps that could render organizations vulnerable and illuminate cyber-risk blind spots to executive leadership. Both sides need regular dialogues to ensure that cybersecurity is included in everyday business decisions. Even with the initial agreement on the importance of cyber resilience, sustained attention and support from decision-makers is difficult to achieve. While 92% of business executives surveyed agree that cyber resilience is integrated into enterprise risk-management strategies, only 55% of security-focused leaders surveyed agree with the statement.

FIGURE 11 **Differences in perceiving the integration of cyber resilience into enterprise risk management**

It is crucial to better understand this misalignment between high-level acknowledgement of cyber issues, its cohesion with business priorities and a perceived lack of actionable operational tools when it comes to strategy.

The misalignment of perception between security-focused executives and business leaders extends to aligning priorities with the Board of Directors. Increasing scrutiny and expectations from the Board of Directors is becoming a reality of business-risk oversight. "Organizations should have a cyber-aware board member who can probe and challenge the organization on cyber matters", according to Kelly Bissell, Global Lead, Accenture Security, Accenture.

In 2018, a major security breach occurred at a company in the hospitality industry headquartered in Delaware, US, where nearly 68% of Fortune 500 companies are incorporated.[23] A class action lawsuit against the company was filed and upheld, signalling cybersecurity is an area of consequential risk that spans modern business sectors. In her

deciding opinion, Vice Chancellor Lori W. Will of the Delaware Court of Chancery stated that it was necessary to "increasingly call upon directors to ensure that companies have appropriate oversight systems in place [when it comes to cyber risk]."[24] The cyber risks affecting the corporation's "mission critical" component was a focus of Delaware courts in assessing potential oversight liability, particularly where a board has allegedly failed to implement reporting systems or controls to monitor those risks.[25]

Regulations and court decisions are shaping the future of cybersecurity, but is that enough? Comparing data between security-focused and business executives, when asked about their organization's approach to cybersecurity, security-focused executives were twice as likely as their business counterparts to place regulations as the top influence when managing their approach to cybersecurity, indicating that shaping future regulations may be key to better encouraging collaborative cyber policies.

FIGURE 12 **Differences in perceiving regulatory influence on cybersecurity**

11% of business executives believe that regulations will be the leading influence on the organization's approach to cybersecurity

20% of security-focused executives believe that regulations will be the leading influence on the organization's approach to cybersecurity

> **"Given the ever-increasing cyber threats and the evolving cyber and privacy regulatory environment, cybersecurity must shift towards cyber resilience ensuring a quick recovery in case of an incident. That will enable trust and value creation – key pillars for sustainable innovation."**
>
> Christophe Blassiau, Global CISO, Schneider Electric, France

According to the survey, 72% of respondents do not agree that "cyber and privacy regulations are effective in reducing my organization's cyber risks." In addition, 60% of boards do not believe that cyber and privacy regulations are effective in reducing their organization's cyber risks. It might be a sign for policy makers and state leaders to innovate when incentivizing better cybersecurity. Regulators do not operate in a vacuum, so it is important for organizations to collaborate with regulators on innovation and to raise insights and challenges as a partner to the regulatory process.

Decision-makers should look beyond compliance requirements to enable their cyber leaders to drive cybersecurity performance and position it as a competitive advantage, thereby preventing and mitigating a potential cyberattack, and balancing security and business operations to allow the business to thrive and deliver its services. As Jim Alkove, Chief Trust Officer, Salesforce, frames it, "Business leaders must implement a cybersecurity strategy with an eye towards what's needed to build a trusted enterprise, not just to meet minimum requirements from a legal or regulatory perspective. Consider the expectations of all stakeholders – customers, employees and partners included – and work to achieve, if not exceed, those measures."

2.3 Recruiting and retaining talent

Looming ever larger for organizations across every industry is a shortage of cybersecurity professionals. It is no exaggeration to say that the dearth of staff security positions is a major threat to business continuity and even to national defense. When asked whether their organization had the skills needed to respond and recover from a cyberattack, our survey found that 50% of all respondents would find it challenging to respond due to the shortage of skills within their team, and less than 25% of companies with 5,000 to 50,000 employees, "have the people and skills [they] need today". Many respondents shared that they rely on third parties to support them a cyber incident occurs.

FIGURE 13 **Skills and talent currently available to cyber leaders to counter cyberattacks**

6%
Are missing critical people and skills

6%
Rely on third parties and external resources

37%
Have the people and skills they need today

47%
Have training and skill gaps in some areas

Retention and work-life balance are also amplifying factors to the talent shortages. Working in cybersecurity can be extremely stressful and taxing. Recent research exposed high senior security personnel staff turnover, with CISOs and the C-Suite citing average tenures for CISOs of just over two years (26 months). More than 88% of security-focused executives report being "moderately or tremendously stressed." Among them, 48% say work stress has had a detrimental impact on their mental health.[26] Often, these gaps come down to things like recruiting and retaining human capital.

We need innovative solutions to provide opportunities for more people to choose cybersecurity as their career path. The private and public sectors are stepping up to respond to this challenge. For example, the Forum's Cybersecurity Learning Hub democratizes access to cybersecurity skills by providing free and career-oriented modules that give people a route towards in-demand roles.[27]

Below: @AzmanJaka/ Gettyimages

2.4 Action: the importance of partnerships

Cyber leaders acknowledge the need for collaboration and a common platform for a more robust cybersecurity and a resilient ecosystem. As Ken Xie, CEO of Fortinet, reports:

"In a world that is so deeply interconnected by digital technology, cybersecurity and global security are the same thing. No single organization, public or private, can have a complete view of the entire cyber landscape. Senior leadership must insist organizations share information to put the pieces of the puzzle together. Otherwise, we will be flying blind."[28]

According to the World Economic Forum Cyber Outlook Series,[29] the main goal for cyber leaders is to develop trust and forge partnerships within their ecosystem. The value of partnerships is proven; over 90% of respondents report receiving actionable insights from external information sharing groups and/or partners.

FIGURE 14 **The importance of information sharing**

Say information sharing groups provide actionable insights

Cyber leaders also noted that effective collaboration between private- and public-sector leaders is key to ensuring national cyber resilience. A noteworthy 85% of respondents agreed that they would be willing to be more transparent and to cooperate with law enforcement if it led to greater punishment of cybercrime. Thus, increased partnering with law enforcement should be considered in overall public-private collaboration strategies.

The goal of public-private partnerships is to:

- Increase understanding of cyber environment
- Enhance resilience, in the whole or in parts of the ecosystem
- Create societal resilience

Both private- and public-sector leaders agree that closer cooperation between the sectors is needed for a more cyber-resilient society. To start, cyber leaders indicated that limiting regulatory restrictions and legal boundaries preventing information sharing and focusing on capacity building should be priority areas for tighter public-private collaboration.

However, where to start is the issue. Cyber leaders shared their concern that before focusing on global public-private cooperation across different industries and governments, it is important to foster public-public cooperation across different governments. That means there need to be global frameworks and standards for security and the sharing of digital evidence.

Today, technology is a strategic business enabler that is essential to effective business operations. Yet, too often the people and functions that protect that technology are viewed as a cost rather than an investment. This widens the gaps, creates inefficiencies and undermines cyber resilience. To bridge these gaps, executives should work together in a more seamless and strategic manner. Each should become fluent with the others' objectives, priorities, limitations and risks within the context of the broader organizational mission, and those ecosystems and communities that the organization serves.

3

Securing the Ecosystem

Much value is generated through today's hyperconnected digital world, but it introduces even more threats if the ecosystem is not secured effectively.

Below: @maxkabakov/ Gettyimages

People and organizations have more access than ever to data. Sharing that data through widely used Application Programming Interfaces (APIs) is transforming how we collaborate across organizations and national borders. Aside from the top-line value at the surface level, which fuels business growth and improves efficiencies, there are underlying and sometimes unforeseen consequences of the increasing digital connectivity. They introduce multiple entry points for cybercriminals to exploit. This challenge has become particularly prevalent during the onset of the COVID-19 pandemic, when much of the workforce started working remotely full time whenever possible depending on the type of work performed and the infrastructure available. Almost overnight, any employee, executive or third-party supplier in a company's ecosystem represented a potential threat.

Cyber incidents in a borderless digital ecosystem cause far-reaching effects across environments, exacerbating potential harmful consequences and representing greater challenges to damage control efforts. It is often said that "a chain is only as strong as its weakest link". A company is only as secure as the safeguards and countermeasures of its most vulnerable contact point. Cyberattacks on other organizations in the digital supply chain can negatively impact downstream businesses and their operations. An example of such an attack affecting the whole supply chain was perpetrated by the REvil ransomware group in 2021, wherein they exploited a vulnerability in a remote monitoring and management software platform. The attack disrupted as many as 1,500 companies worldwide, including a Swedish grocery retail chain, which forced a temporary closure of more than 800 stores.[30] This was one of the largest ransomware attacks in history, which resulted in a complete shutdown of certain businesses.

Third-party attacks are on the rise. In the last several years, indirect attacks – successful breaches coming into an organization through third parties – have increased from 44% to 61%.[31]

Cyber leaders are justifiably highly concerned about vulnerabilities in their supply chain and other third-party partnerships. Our survey found that almost 40% of respondents have been negatively affected by a third-party vendor/supply chain organization cybersecurity incident. Nearly half (44%) of the surveyed CEOs indicated that software supply chain attacks will have the greatest influence on their organization's approach to cybersecurity in the future. Many do not trust that their vendors are ready for the challenge: 58% of respondents feel that their partners and suppliers are less resilient than their own organization.

Companies, governments and individuals alike must now be more aware of these threats, and their response involves three sets of actions:

1. Mapping their network thoroughly, including all the endpoints

2. Focusing their resources not only on prevention but also on the resilience

3. Strengthening relationships across the ecosystem in which the business operates

Below: @alexsl /Gettyimages

3.1 Ecosystem vulnerability

FIGURE 15 **Cyber leaders and third-party incidents**

Have been adversely affected by a cyber incident stemming from a third party within their ecosystem

Growth in network connectivity has resulted in increasing the size of the cyberattack surface, thereby making organizations more vulnerable to compromise. One analysis found high-risk vulnerabilities in 84% of companies, combined with publicly available exploits on the darkweb to around 60% of those vulnerabilities.[32] The black market on the darkweb for Common Vulnerabilities and Exposures (CVEs) is thriving: with nearly 50 new CVEs released per day in 2020, the pressure on security teams to prioritize and deploy timely patches has never been greater.[33]

In the digital ecosystem, small and mid-size enterprises (SMEs) connected to an organization's network represent most vulnerabilities and are increasingly a target of cyberattacks. In many cases, they are seen by hackers as more exploitable and with fewer resources committed to their defense. As of 2020, 55% of SMEs have experienced a cyberattack. In our survey, 88% of respondents expressed concern over the resilience of SMEs within their ecosystem. In addition to that, 40% of respondents admitted that in the last two years they experienced an attack in their digital ecosystem that affected their organization in a negative manner.[34]

> **"Organic and inorganic growth of organizations has resulted in increased complexity and exposure to cyber risks, making organizations even more vulnerable to compromise. We have not been particularly successful in automating asset and data visibility as well as threat reduction at scale. Especially vulnerable are the SMEs in our digital supply chains and ecosystem. As a global community we need to make sure that we provide solutions for the SMEs to better protect themselves against current and future cyber threats and shift the burden to the makers of technology rather than the users."**
>
> Jaya Baloo, Chief Information Security Officer (CISO), Avast Software, Netherlands

3.2 The importance of resilience

Even the most protected and resource-rich organizations cannot fully avoid cyber disasters. It is impossible to reach complete security in the cyber domain so the focal objective of cyber leaders must shift to reinforcing cyber resilience to the utmost – the ability to anticipate and quickly recover from both malicious and non-malicious disruptions. Cyber leaders and their teams will increasingly be judged by how quickly business operations are restored and how seamless and timely the incident response process was after a successful cyberattack. Robert Silvers, US Department of Homeland Security (DHS) Undersecretary for Strategy Policy and Plans underscores this: "companies are not judged by whether they were hit by a cyberattack, but by the character of their response."[35]

3.3 Success through transparency and trust

Trust is at the core of the ecosystem partnerships and system-to-system relationships that exist today. An organization may feel confident or secure in their own network, within their walls, but lose faith in their ecosystem's resilience once they have been negatively impacted by a third-party vendor cybersecurity event. How can trust be established or re-established and maintained?

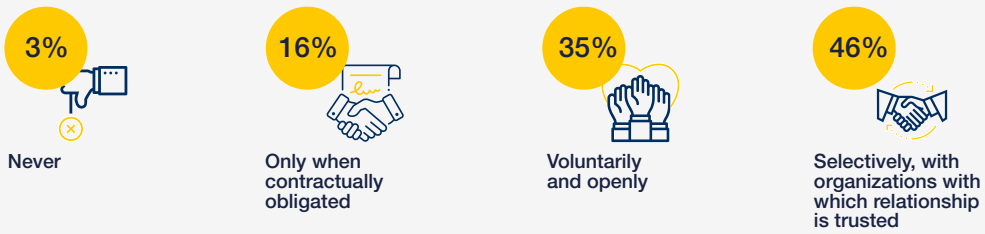
Accountability and visibility in the ecosystem are essential ingredients for success but are often missing. During the Cyber Outlook Series, cyber leaders emphasized the difficulties associated of establishing accountability within the ecosystem. They have also shared some solutions to resolve this challenge:

1. Encourage business leaders to take part in tabletop exercises, i.e. practice a cyber incident response. This approach heightens awareness of issues and risks that may jeopardize the operative success of incident response and underscores the importance of teamwork and learning from peers both inside and outside one's organization or industry. Business leaders participating in such inclusive exercises, including tabletop exercises and beyond, will acquire broader clarity on the importance of the implemented cybersecurity capabilities as well as on how to measure the effectiveness of incident response capability.

2. Establish a mechanism for better visibility into the digital ecosystem. Clear visibility of an organization's ecosystem interlocks is vital when onboarding third parties, IOT devices and other information and data exchanges. At the highest level, leaders are looking for optimal transparency and visibility – learning from one another's successes and failures. Strong collaboration and partnerships will build meaningful trust and allow for actionable information-sharing to create a more resilient ecosystem. This visibility should encourage a development of a minimum-security baseline and requirement across the ecosystem.

3. Enable more effective information sharing within the ecosystem. Cyber leaders acknowledge the importance of information sharing. More than

FIGURE 16 **Are cyber leaders sharing information about their cyber-resilience practices and capabilities across the ecosystem?**



35% of respondents confirmed that they share information openly and voluntarily, and another 45% do so with others with whom they have established relationships. The infrastructure for information sharing still needs to make possible and encourage a culture of disclosure and sharing. When asked what protections need to be in place for cyber leaders to be more comfortable about sharing data within their ecosystems, they replied:

- maintaining anonymity and usage agreements (44%)
- requiring information disclosure agreements (43%)
- legal protections against civil or criminal lawsuits (39%)

FIGURE 17 | **Incentives for voluntary disclosure of cyber incidents**

44%
Maintain anonymity

43%
Disclosure agreements

39%
More legal protections against lawsuits

21%
Direct access to law enforcement

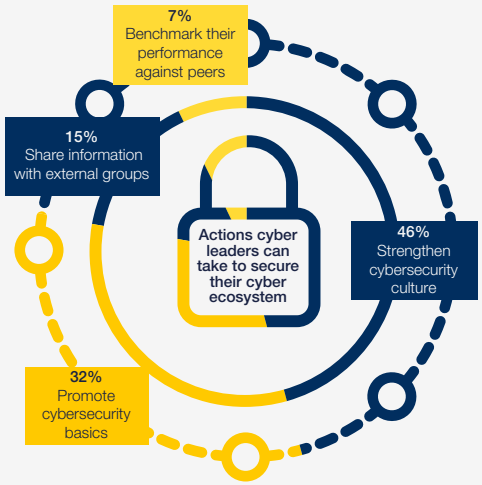
Fundamentally, transparency and trust are borne out of strong ecosystems, and a firm foundation for the type of sharing that builds and encourages resiliency. A strong ecosystem comprises policies and practices that allow leaders, employees and peers to cast aside doubts about the confidentiality, security and competitiveness of the information they choose to disclose when it comes to both internal and external engagement.

Innovation in the cyber industry will play an important role in securing our digital future. Entrepreneurs and investors are focusing on R&D to shape solutions to ongoing security problems such as ransomware and zero-day exploits. Investment in cybersecurity start-ups and its ecosystem can lead to high ROI as well as play a key role in the strategy to strengthen cyber resilience, serving both, operations and cyber strategy.

How do current approaches to the resilience of an ecosystem need to shift in the near term to remain viable? According to the survey, when asked how their organization is currently changing or planning to change its approach to managing cyber resilience across its ecosystem in the coming year, the overwhelming majority of respondents (over 87%) will focus on strengthening resilience policies, processes and/or standards for how to engage and manage third parties.

The World Economic Forum Centre for Cybersecurity is leading a Cyber Resilience Index initiative, aiming to improve transparency and visibility across the digital ecosystem. This cross-industry, multistakeholder community collaboration is working to develop a framework to guide cybersecurity and business leaders in translating cyber-resilience principles, strategic goals, objectives and best practices to assess and advance their organization's cyber resilience.

FIGURE 18 | **Actions to secure the ecosystem**



Each participating member holds the power to help or harm, weaken or strengthen their cyber ecosystem. It is the responsibility of everyone to recognize their cyber role based on their position in the ecosystem to reduce the likelihood and risk of disruption, influence their workforce culture, and show and encourage trust and transparency. This trust and transparency will be the foundation of any ecosystem's resilience.

Conclusion

As digitalization continues to proliferate and new technologies are introduced cyber risk will inevitably grow.

Frontier technologies like AI, robotics, quantum computing, the ever-evolving adoption of the internet of things (IoTs), cloud computing, blockchain and remote working/distance learning models represent the future of our digital world. The potential cyber risks and vulnerabilities of these new technologies should be on minds of every leader when considering technology adoption and implementation.

Nearly half (48%) of the World Economic Forum's Cyber Outlook survey respondents say that automation and machine learning will introduce the biggest transformation in cybersecurity in the short-term future. Indeed, leading cyber expert Bruce Schneier, Lecturer in Public Policy, John F. Kennedy School of Government, Harvard University, USA, agrees that techniques from artificial intelligence will permeate all aspects of cybersecurity, both in attack and defense.[36] According to him, these techniques will almost certainly upend the traditional imbalance between attack and defense. The problem is that we do not know how, and we do not know when.

The advantage of traditional computers is that they excel at speed, can process an enormous amount of data, and never tire or get bored. Humans, on the other hand, are great at thinking and reasoning. What AI will do is push computers more and more into those traditionally human realms. But here's the thing about AI: its development is intermittent, and its progress is non-linear. Things that we thought were hard for a computer end up being easy, and things we thought were easy for it end up being hard. It's impossible to know for sure until the breakthroughs occur, especially when trying to predict a couple of years or a decade into the future.[37]

One of the most pressing risks in the longer term is quantum computing. Quantum computing could crumble the current encryption on which most enterprises, digital infrastructures and economies rely. This is a critical risk that could introduce more harm than benefits if the risks are not addressed in a timely manner at the national and global levels.

Although public- and private-sector stakeholders are determined to achieve higher cyber resilience levels, their efforts are often hindered by various organizational, technical and regulatory barriers. Overcoming these barriers will require a holistic, systematic and collaborative multistakeholder approach.

While we cannot fully prepare for various potential scenarios on how technology is and will influence and change our lives or become a potential venue to be exploited, the challenges pointed to herein are something we need to at least think about. The less we are surprised by these developments, the better off we will be as a society. At this stage of mass digitalization, it is imperative that leadership better incorporate cybersecurity and cyber resilience in their thinking and analytical process of potential cyber threats and understand various scenarios to prepare for potential cyber disasters while identifying incentives to improve cyber resilience.

The World Economic Forum Centre for Cybersecurity is working with multistakeholder communities to enhance cyber resilience by developing and scaling forward-looking solutions and promoting effective practices across digital ecosystems.

Appendix

Methodology

Insights for Global Cybersecurity Outlook 2022 were gathered from four sources: First, a survey of global cyber leaders; second, Cyber Outlook Series sessions conducted by the World Economic Forum throughout 2021; third, the team held multiple interviews with experts and bi-lateral meetings; fourth, data has been collected from reports, research and articles published by the World Economic Forum and reputable third parties. Combination of all these efforts, the World Economic Forum's team has consulted with 120 global cyber leaders.

Cyber Outlook Survey

The World Economic Forum (hereafter 'the Forum') Centre for Cybersecurity and Accenture generated a survey comprising 24 questions. The questions focused on cybersecurity and cyber resilience progress, foresight, challenges and perceptions. The survey was administered to global leaders within two primary groups: the Forum's Cyber Leadership Community and the Accenture Cybersecurity Forum.

The survey was anonymous and non-attributable to the respondent or their respective organizations. Demographic questions were asked in the survey and included: Industry, ranges of number of employees in the respondent's organization, annual revenue ranges of the respondent's organization, country where the respondent's organization is headquartered, and the respondent's job title. There were a total 79 responses from 20 countries and 14 industries.

Except for one free-form text response and seven sentiment responses (ranging from 'strongly disagree' to 'neither agree nor disagree' to 'strongly agree'), all survey questions provided the respondent with a list of pre-populated answers from which they could select. Where appropriate, a text box labelled "other" was available to permit addition of responses not included in the pre-populated responses. Five questions asked the respondent to rank their responses, which also permitted the respondent to create and rank their own unique response using a text box input.

Cyber Outlook Series

The Forum Centre for Cybersecurity hosted Cyber Outlook Series sessions throughout 2021 with the goal of creating opportunities for unique peer-level exchanges on key cybersecurity issues among members of the Cybersecurity Leadership Community. During 2021 sessions, the Forum actively engaged more than 120 members of the Community. The members take ownership of the Series by providing input to the topics, shaping the agenda and engaging actively in the sessions, resulting actionable insights shared in this report. Throughout the Series, participants were encouraged to contribute their ideas and responses using a chat capability within the meeting platform. Following every session of the Series, responses were consolidated and analysed to develop insights and themes for this report.

The Cyber Outlook Series is held under the Chatham House Rule, consequently no information in this report is attributed to a specific member of the Community.

Acknowledgements

Our sincere thanks to the members of the Cybersecurity Leadership Community for their active contribution to this report. We also extend our gratitude to the external experts who agreed to be interviewed as part of this study, as well as to colleagues around the world who provided perspectives. They include:

Edward Blomquist
Senior Manager, Accenture, USA

Pedro Caruso
Managing Director, Accenture, USA

Jacky Fox
Managing Director, Accenture, Ireland

Jim Guinn
Senior Managing Director, Accenture, USA

Michael Rohrs
Senior Manager Accenture, USA

Lauren Stockton
Project Analyst, Accenture, USA

Jaya Baloo
Chief Information Security Officer, Avast Software, Czech Republic

Arina Pazushko
Head, External Affairs, BI.ZONE, Russian Federation

Dmitry Samartsev
Chief Executive Officer, BI.ZONE, Russian Federation

Yael Nagler
Corporate Cyber Risk Expert, The Cantellus Group, USA

Summer C. Fowler
Adjunct Faculty, Heinz College, Carnegie Mellon University, USA

David Koh
Commissioner of Cybersecurity and Chief Executive, Cyber Security Agency (CSA), Singapore

Albert Antwi-Boasiako
Acting Director-General, Cyber Security Authority (CSA), Republic of Ghana

Ken Xie
Founder, Chairman of the Board and Chief Executive Officer, Fortinet, USA

Sandra Wheatley Smerdon
Senior Vice President, Threat Intelligence, Marketing and Influencer Communications, Fortinet, USA

Bruce Schneier
Lecturer in Public Policy, John F. Kennedy School of Government, Harvard University, USA

Marene Allison
Chief Information Security Officer, Johnson & Johnson, USA

Randy Herold
Chief Information Security Officer, ManpowerGroup, USA

Nancy Luquette
EVP, Chief Risk & Compliance Officer, S&P Global, USA

Bruce Byrd
Executive Vice President and General Counsel, Palo Alto Networks, USA

Ryan Gillis
Vice President, Cybersecurity Strategy & Global Policy, Palo Alto Networks, USA

Jim Alkove
Chief Trust Officer, Salesforce, USA

Noura Alajmi
Head of Cybersecurity Awareness and Behavior Management, Saudi Aramco, Saudi Arabia

Bandar Almashari
Head of Global Security Operations, Saudi Aramco, Saudi Arabia

Hisham Alsuwayied
Head of Cybersecurity Governance, Saudi Aramco, Saudi Arabia

Sarah Alzamil
Head of Endpoint Security, Saudi Aramco, Saudi Arabia

Stanislav Kuznetsov
Deputy Chairman of the Executive Board, Sberbank, Russian Federation

Christophe Blassiau
Global CISO, Schneider Electric, France

Alejandro N. Mayorkas
Secretary, US Department of Homeland Security, USA

Tim Maurer
Senior Counselor for Cybersecurity to the Secretary, US Department of Homeland Security, USA

Filipe Beato
Lead, Centre for Cybersecurity, World Economic Forum, Geneva

Sean Doyle
Lead, Centre for Cybersecurity, World Economic Forum, Geneva

Contributors

World Economic Forum

LEAD AUTHOR
Algirde Pipikaite
Lead, Strategic Initiatives, Centre for Cybersecurity

Gretchen Bueermann
Research and Analysis Specialist, Centre for Cybersecurity

Akshay Joshi
Acting Deputy Head, Centre for Cybersecurity

Jeremy Jurgens
Managing Director

Accenture

Kelly Bissell
Global Lead, Accenture Security

Carlos Aguirre
Security Manager

Taylor Browder
Security Consultant

Jim Pruitt
Principal Director

Endnotes

1. Katz, Raul, and Jung, Juan. 2021. The Economic impact of broadband and digitalization through the COVID-19 pandemic. International Telecommunication Union. https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.COV_ECO_IMPACT_B-2021-PDF-E.pdf (link as of 1/12/21)
2. Chakravorti, B., Bhalla, A., and Chaturvedi, R. S. 2020. Which economies showed the most digital progress in 2020? Harvard Business Review. https://hbr.org/2020/12/which-economies-showed-the-most-digital-progress-in-2020 (link as of 1/12/21)
3. The cybersecurity poverty line is the umbrella term designating organizations or nations that need to establish or enhance their cybersecurity posture. It can also be referred to as a threshold for what is considered the lowest line of cyber defense.
4. United Nations Conference on Trade and Development. 2021. How Covid-19 triggered the digital and e-commerce turning point. United Nations Conference on Trade and Development. https://unctad.org/news/how-covid-19-triggered-digital-and-e-commerce-turning-point (link as of 23/11/21)
5. Organisation for Economic Co-operation and Development. 2020. Keeping the Internet up and running in times of crisis. Organisation for Economic Co-operation and Development. https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/#figure-d1e110 (link as of 23/11/21)
6. Jenik, Claire. 2021. Statista. https://www.statista.com/chart/25443/estimated-amount-of-data-created-on-the-internet-in-one-minute/ (link as of 12/1/2021)
7. Franceschi-Bicchierai, Lorenzo. 2021. How the Mafia Is Pivoting to Cybercrime. Vice. https://www.vice.com/en/article/epne4j/how-the-mafia-is-pivoting-to-cybercrime (link as of 23/11/21)
8. The dark web is that part of the internet that is not visible to search engines and requires the use of an anonymizing browser called The Onion Router (Tor) to be accessed. It is where cybercriminals gather, exchange information, sell and buy illegal items and services.
9. Bischoff, Paul. 2021. The cost of hiring a hacker on the dark web: report. Comparitech. https://www.comparitech.com/blog/information-security/hiring-hacker-dark-web-report/ (link as of 23/11/21)
10. Ibid
11. Cost of a Data Breach Report 2021. 2021. IBM. https://www.ibm.com/security/data-breach (link as of 23/11/21)
12. IBM Security. 2020. Cost of a Data Breach Report 2020. IBM Corporation. p.5. https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf (link as of 23/11/21)
13. Bischoff, Paul. 2021. How data breaches affect stock market share prices. Comparitech. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/#NASDAQ_benchmark_validation (link as of 23/11/21)
14. Boholm, Max. 2021. Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995-2019). Journal of Cybersecurity, Volume 7, Issue 1, 2021. https://academic.oup.com/cybersecurity/article/7/1/tyab016/6321976#270960794 (accessed 23/11/21)
15. He, Terry, et al. 2021. Mid-Year Update Sonicwall Cyber Threat Report. Sonicwall. https://www.sonicwall.com/2021-cyber-threat-report/?elqCampaignId=14431&sfc=7013h000000Mm0SAAS#form (link as of 1/12/21)
16. Bissell, Kelly, et al. 2021. State of Cybersecurity Resilience 2021. Accenture. p.5. https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf (link as of 23/11/21)
17. Ibid.
18. Fortinet. 2021. The 2021 Ransomware Survey Report. Fortinet. https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-ransomware-survey.pdf (link as of 10/12/21)
19. Ibid.
20. Ron Ross; Victoria Pillitteri; Richard Graubart; Deborah Bodeau; Rosalie McQuaid. 2021. NIST Special Publication 800-160 Vol. 2, Revision 1. NIST. https://csrc.nist.gov/glossary/term/cyber_resiliency#:~:text=Definition(s)%3A,NIST%20SP%20800%2D160%20Vol (link as of 10/12/21)
21. Koh, David, and Luquette, Nancy 2021. How to succeed in an increasingly risky cyber environment. World Economic Forum. https://www.weforum.org/agenda/2021/07/how-to-succeed-in-an-increasingly-risky-cyber-environment/ (link as of 23/11/21)
22. Ibid.
23. Firemen's Retirement System of St. Louis v. Arne M. Sorenson, et al. (Marriott International, Inc.), p. 31 (Court of Chancery 2021) https://courts.delaware.gov/Opinions/Download.aspx?id=325170 (link as of 10/12/21)
24. Ibid.
25. Ibid.
26. Nominet Cyber. 2020. The CISO Stress Report. Nominet. p.7. https://media.nominetcyber.com/wp-content/uploads/2020/02/Nominet_The-CISO-Stress-Report_2020_V10.pdf (link as of 23/11/21)

27. World Economic Forum. 2020. Cybersecurity Learning Hub. World Economic Forum. https://www.weforum.org/projects/cybersecurity-learning-hub (link as of 10/12/21)

28. Xie, Ken. 2020. Four Key Challenges for cybersecurity leaders. World Economic Forum. https://www.weforum.org/agenda/2020/01/four-key-challenges-for-cybersecurity-leaders/ (link as of 23/11/21)

29. World Economic Forum. 2021, October 12. Cyber Outlook Series Workshop. Cyber Outlook Series, Geneva, Switzerland.

30. Klugerman, Yaffa. 2021. The 5 Most Notable Third-Party Data Breaches of 2021 (So Far). Panorays. https://panorays.com/blog/the-5-most-notable-third-party-data-breaches-of-2021-so-far/ (accessed 1/12/21)

31. Bissell, Kelly, et al. 2021. State of Cybersecurity Resilience 2021. Accenture. p.8. https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf (link as of 3/12/21)

32. Positive Technologies. 2020. Vulnerabilities on the corporate network perimeter. Positive Technologies. https://www.ptsecurity.com/ww-en/analytics/vulnerabilities-corporate-networks-2020/ (link as of 23/11/21)

33. Cyber Security Intelligence. 2021. For Sale – Dark Web Exploits. Cyber Security Intelligence. https://www.cybersecurityintelligence.com/blog/for-sale---dark-web-exploits-5756.html (link as of 1/12/21)

34. Downey, Brian. 2020. Why SMBs are high risk for cybersecurity threats in 2021. Connectwise. https://www.connectwise.com/blog/cybersecurity/why-smbs-are-high-risk-for-cybersecurity-threats-in-2021 (link as of 23/11/21)

35. Silvers, Robert. 2021, November 10. Decoding Ransomware: Leadership, Cryptocurrency and Cooperation 2 [Plenary session]. Annual Meeting on Cybersecurity, Geneva, Switzerland.

36. Schneier, Bruce. 2021, November. Phone Interview with Algirde Pipikaite, World Economic Forum.

37. Ibid.

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