Annual Meeting on Cybersecurity 2023: Key Takeaways

DECEMBER 2023

Images: Getty Images, World Economic Forum

Contents

Disclaimer
This document is published by the World Economic Forum as a contribution to a project, insight area or interaction. The findings, interpretations and conclusions expressed herein are a result of a collaborative process facilitated and endorsed by the World Economic Forum but whose results do not necessarily represent the views of the World Economic Forum, nor the entirety of its Members, Partners or other stakeholders.

Preface

Prevailing geopolitical uncertainty, a looming economic crisis and rapid advances in transformative technologies such as generative artificial intelligence (AI) have had a significant impact on cybersecurity. This is evidenced in the World Economic Forum report, Global Cybersecurity Outlook 2023, where the vast majority of cyber and business leaders think it “moderately likely” or “very likely” that global geopolitical instability will lead to a far-reaching, catastrophic cyber event in the next two years.

Adding to these challenges is a significant trust deficit worldwide, which has been growing hand in hand with the development of technologies. Those technologies have increased the interconnectedness of systems, humans and societies. Despite the interconnectedness, cyber inequity has been growing. It manifests in various forms, including disparities between large and small companies, developed and underdeveloped regions, end users and technology makers. The technology industry’s evolution has not kept pace with the need for increased security, with persistent vulnerabilities and malicious tactics continuing to pose threats.

To effectively prepare for and address cyber risks within the multiple transitions the world is going through, organizations need to develop strategies focused on systemic approaches to securing cyberspace. More than ever, sustained multistakeholder collaboration between organizations and society is needed to ensure shared resilience. Cyber leaders and executives at the highest levels also need to codevelop strategic foresight to steer effective decision-making to stay ahead of cyberthreats on the horizon.

To encourage dialogue and action on global solutions, the Annual Meeting on Cybersecurity 2023 convened in Geneva on 13-15 November. It brought together nearly 150 cybersecurity executives from various sectors, including business, government, law enforcement, international organizations, civil society and academia. The meeting featured 30 sessions across the three programmatic pillars – building cyber resilience, strengthening global collaboration and navigating cyber frontiers. This document offers a summary of key takeaways from the meeting for cyber leaders to act upon and share widely within their teams, as well as a call to action for chief executive officers to ensure a secure digital future.

Thank you for your continued engagement in the collective mission of securing cyberspace.

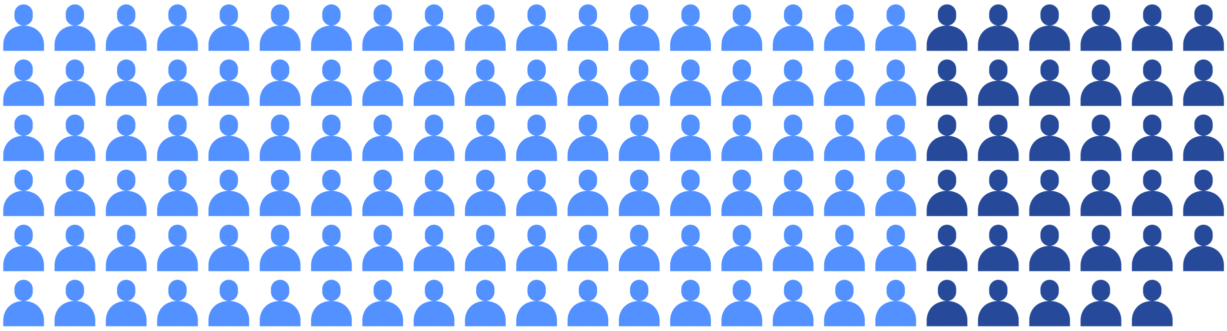
Key stats

3 days

30 sessions

143 participants

25% female participants



Quotes from attendees

“

Attending the Annual Meeting on Cybersecurity 2023 was not just an experience; it was an immersion into the ever-evolving landscape of digital innovation and cybersecurity. We are grateful for the opportunity to be a part of this transformative gathering, where each participant is a key player in the collective effort to secure our digital future.

Sami Khoury, Head, Canadian Centre for Cyber Security, Canada

“

This year’s Annual Meeting on Cybersecurity came at a critical juncture for cybersecurity: geopolitical dynamics place it even higher in the priorities of the domains that we need to strengthen. The Forum’s efforts to bring together government and business experts from across the world is a unique opportunity to discuss issues where global convergence is now urgent. Dealing with the use of artificial intelligence by malicious actors, exploring its potential for strengthening security and law enforcement require agreed solutions by the like-minded.

The EU continues to complete its regulatory ecosystem so as to create a cyber-shield based on preparedness but also operational capabilities built on ensuring security by design in all products and services but also seeking the best possible use of resources to address the skills gap and shortages of workforce. The answers to these problems can be found in global cooperation through agreed norms on technology use and reinforced intra-government as well as public and private sector cooperation.

Despina Spanou, Head of the Cabinet of the Vice-President for Promoting the European Way of Life of the European Commission

“

The Annual Meeting on Cybersecurity offers a venue for cybersecurity leaders to reflect on the latest opportunities, challenges and to collaborate towards strengthening global measures. This year’s meeting signified once again the importance of focusing on building a sustainable talent pipeline to develop a cybersecurity workforce capable of addressing the latest emerging threats.

Omar Al-Thukair, Director, Information Protection Department, Aramco Saudi Arabia

“

Sharing threat intelligence and cybersecurity insights among global private and public organizations plays a crucial role in protecting our world from sophisticated threat actors and advanced cyberattacks. The Annual Meeting on Cybersecurity 2023 provided a forum for the industry’s leading experts to come together and share knowledge on pressing issues such as AI. More importantly, it provided space to collaboratively develop solutions to make our rapidly-transforming world safer and better prepared to tackle the challenges of the modern threat landscape.

Wendi Whitmore, Senior Vice-President, Unit 42 (Cyber Consulting and Threat Intelligence), Palo Alto Networks, USA

> **The Annual Meeting on Cybersecurity 2023 underscored that covering cybersecurity fundamentals and addressing existing gaps vs evaluating the impact and risks posed by emerging technology, is still issue number one. We must continue down the path towards mastering the basics in order to eventually defend against future threats.**
>
> Grant Bourzikas, Chief Security Officer, Cloudflare, USA

> **This is one of the highlights of my calendar every year. To meet the top global cybersecurity professionals and discuss real-world challenges and where we as a collective can help.**
>
> Jacky Fox, Senior Managing Director; Lead, Accenture Security, Europe and Ireland

> **The Annual Meeting on Cybersecurity 2023 was an exceptional event that provided a comprehensive overview of the latest cybersecurity trends and challenges. I was particularly impressed by the quality of the speakers, the networking opportunities and the Global Collaboration Village, which provided an eye-opening look at the potential of the metaverse for collaboration and innovation.**
>
> Bushra AlBlooshi, Senior Consultant, Research and Innovation, Dubai Electronic Security Center (DESC), United Arab Emirates

A call to action for global leaders in Davos

The digitization of economies and societies has created greater global interconnectivity, unveiling vast opportunities for growth and innovation. This transformative shift is propelled by the continuous development and seamless integration of emerging technologies into pivotal processes, allowing organizations – both public and private – to derive significant benefits. However, this increased digital footprint also brings with it significant vulnerabilities that malicious actors seek to capitalize upon.

To ensure that the full benefits of digitalization are realized, it is crucial to strategically embed cybersecurity at the core of organizational operations. Cybersecurity is no longer a technological problem but a strategic leadership imperative. Building on discussions at the Annual Meeting on Cybersecurity, the community has identified five key priorities for leaders.

1 Gain a better understanding of your organization's cyberthreat landscape and associated key risks

Critical national infrastructure sectors are particularly at risk of being a target of cyberattacks in times of geopolitical conflicts and instability. This can have consequences for your organization.

2 Instil a culture of cybersecurity throughout the organization and set the tone from the top

Ensuring your executive team and employees are cyber-savvy will significantly reduce the cyber risks that your organization is facing, especially with cyberthreats becoming increasingly sophisticated.

3 Embrace a systemic approach to business continuity with an emphasis on cybersecurity

Define the material impact of cyber incidents on your business, assess the dependencies of your organization to third parties and understand the dependencies of your third parties on your own organization.

4 Promote the development of strategic collaboration lines on cyber resilience with key public organizations

Strong collaboration with stakeholders across government and law enforcement is key to enabling and empowering your chief information security officer to effectively respond in times of cyber crisis and will, in turn, help improve the resilience of your organization.

5 Focus on building, maintaining and nurturing the general public's trust in your organization

With new technologies developing at pace, digital trust is eroding. Organizations that focus on preserving that trust will maintain a competitive advantage in the digital era.

1 Key takeaways: building cyber resilience

Cyber resilience must be a leadership imperative for organizations in the digital age.

Cyber resilience is a systemic business issue that requires clear metrics

In the current landscape, marked by ever-evolving cyber threats, organizations and their chief information security officers should focus on resilience and adaptability. Chief information security officers should be both skilled at managing operational priorities and emergencies and at communicating to the board through "telling a story". Considering that merely deploying security measures is increasingly insufficient, organizations must also proactively deploy defensive strategies to counter today's cybersecurity threats effectively.

Cyber leaders should allocate more time to strategic planning, forging alliances and building trust beyond the confines of their organizations. An issue that persists is the ability to clearly articulate and translate cyber risks into business risks in a way that is understood by the C-suite and the board. To overcome language barriers, communication should be centred on business impact. Chief information security officers can further enrich discussions by sharing narratives from their peers and making use of collaborative efforts. That will help shift conversations from purely technical aspects to broader business perspectives.

Defining "what good looks like" for cybersecurity can help increase cyber resilience. Metrics serve as indicators of progress and introduce a more systematic and scientific dimension to the field of cybersecurity. Measurements empower leaders to make the right decisions. However, due to the current lack of global policies, standardized metrics are difficult to establish. Even the definition of some metrics varies between organizations, which – coupled with the challenge of gathering accurate cyber-related data to feed into metrics – adds to the complexity.

Cyber metrics should also help translate the operational view of cybersecurity into a business view. Understanding the risk appetite of the board is therefore crucial in order to establish what to report on. There is an opportunity to define a standard global framework for metrics and a set of definitions that can be tailored per industry. Boards should also consider familiarizing themselves with the topic to understand the impact of cyber metrics on their business.

The intricacies of securing critical national infrastructure and smart cities have to be thought of holistically

The concept of cyber resilience should extend beyond organizational or sector-specific considerations and encompass a broader societal perspective. Understanding interdependencies within the ecosystem and implementing contingency measures in the event of systemic cyber events is crucial.

This is especially true when dealing with critical national infrastructure (CNI) organizations, where an attack on one organization can have cascading effects across the entire ecosystem. Currently, CNI faces an escalating threat from nation-state actors amid the prevailing geopolitical instability. Unlike conventional attacks seeking financial gain, nation-state attacks often aim at disruption and destruction – which can have significant consequences. Establishing and encouraging public-private partnerships is imperative for safeguarding CNI. This will not only facilitate the sharing of information both before and after an incident but also create trust.

Beyond CNI, there is an even wider ecosystem that now needs to be considered for its cyber resilience capabilities: that of smart cities. Given the profound and continual digital transformation of smart cities, coupled with the increasing use of technology by citizens fuelled by the rise of the internet of things (IoT), cybersecurity must be a top concern in the journey to becoming a smart city. It extends beyond specific entities like critical infrastructure providers, smart building providers or governments digitizing their services. It also incorporates essential elements of citizens' trust in digital solutions, which is a cornerstone for a smart city's operational legitimacy.

A key challenge for cities' cyber resilience lies in navigating various levels of regulation, such as national versus state/local/municipal frameworks. This means that the consolidation of cybersecurity rules and requirements is complex. Establishing clear reporting thresholds for cyber incidents, including potential data protection and privacy violations and ensuring follow-through, is vital in maintaining citizens' trust in smart cities.

Third-party cyber risks are a growing ecosystem-wide concern that emphasizes the need for security-by-design

The cyber risks posed by third parties, especially supply chains, continue to be a key concern for organizations. Measuring and quantifying the cyber risks posed by third parties is not straightforward, and the information required to assess it can be limited. For example, some software are mandated by governments, some suppliers enjoy preferential status and cyber resilience of cloud-native solutions can be hard to assess. Against this backdrop, it is key for organizations to develop a strong understanding of their third parties, vendors and value chains to establish trusted collaboration channels – even before incidents occur. This will help them establish a common platform, ways of working and a standardized language to work together.

An industry in which the security of supply chains is particularly critical is the transport industry. Following a series of cyber incidents, there is growing recognition that the whole transport ecosystem should work together to materially increase cyber resilience – ports, maritime companies and vendors all need to break their siloes. During the meeting, cyber leaders from leading organizations in the transport ecosystem agreed on the need to join forces to exchange best practices and align on common standards/frameworks to bolster cyber resilience. The World Economic Forum has a longstanding history of running initiatives, such as the Cyber Resilience in Industries initiative, focused on systemic cyber resilience within a range of industries by mobilizing collective action and will, therefore, explore the opportunities to work with the transport industry on such matters.

Another issue – that extends beyond specific industries – is the practical implementation of security-by-design. For this to be successful, yet again, an ecosystem-wide approach is required – one that not only includes securing individual technical systems but also the infrastructure and hardware that supports them. The current economic model in cybersecurity puts almost all the responsibility and liability for security-by-design on the consumer. Therefore, incentivizing technology providers to improve the cybersecurity of their products from their development – and thus share the responsibility and liability – will require a concerted and collaborative public-private action.

The economic model for cybersecurity is also significantly geared towards large businesses and completely disadvantages small- and medium-sized enterprises, which do not always have the means to implement fit-for-purpose solutions. Governments and, more generally, the public sector have a key role to play in helping them achieve a minimum-security baseline.

2

Key takeaways: strengthening global cooperation

Multistakeholder collaboration is the key to address complex cybersecurity challenges.

Trust is a key differentiator as organizations seek to navigate cyber crises effectively

Conducting effective crisis management activities and ensuring business continuity are key objectives during a cyber crisis. Therefore, in the event of a crisis, it is crucial to know who needs to be in the room to drive and lead the response. Success while navigating a crisis hinges on trust.

Globally, there is a widespread erosion of trust among societies. This lack of trust is particularly acute in the technology field. This growing trust deficit is primarily a human issue, with policy- and technology-related issues playing a secondary role.

Therefore, organizations should focus on building credibility by showing their commitment to cyber resilience and establishing trusted relationships across the entire ecosystem. In the face of a crisis, it is these trusted relationships that are nurtured over time and collective efforts towards bolstering cyber resilience that will help organizations bounce back effectively.

Organizations that have the resources to invest in this domain should appoint a chief trust officer to focus on tackling this key issue that extends beyond cybersecurity itself.

Global collaboration on pragmatic regulations can help combat cybercrime

Organizations spend significant resources on demonstrating compliance against a variety of different cybersecurity regulations. Therefore, there is a general cross-sectoral consensus that better standardization of cybersecurity regulations worldwide would help increase cyber resilience overall while driving efficiencies from a resource standpoint.

While the public sector mandates information-sharing on incidents, full disclosure can, at times, be accompanied by liability considerations that generate fear and distrust. To effectively tackle those challenges, there needs to be closer collaboration between regulators and the private sector. Regulators should also focus on setting best practices and clear objectives for the regulations while inviting perspectives from the private sector. This would help build more pragmatic regulations. The Forum recently released its Response to the White House's Request on Harmonizing Cybersecurity Regulations in response to the call for information from the United States White House Office of the National Cyber Director on harmonizing cybersecurity standards and regulations across jurisdictions. It focused on addressing conflicts in cybersecurity requirements, identifying priority sectors and regions, evaluating international dialogues, reviewing ongoing global initiatives and exploring regulatory reciprocity.

A domain that particularly suffers from regulatory fragmentation is the response to cybercrime. Challenges associated with cross-border data flows often impede information sharing between countries. Cybercriminals, on the other hand, have no such restrictions and can therefore collaborate effectively. Delivering a compelling response to growing cybercriminal activity requires strong cross-border collaboration, particularly between financial institutions and law enforcement agencies. Developing progressive regulations that incentivize information-sharing practices for cybersecurity would significantly help fight cybercrime efficiently.

Tackling the talent shortage and promoting well-being are key to building a successful cybersecurity workforce

The cybersecurity talent shortage is a persistent challenge faced by organizations across industries and geographies. The deficit of cybersecurity professionals not only leaves organizations vulnerable to cybersecurity threats but also has broader implications for global economic growth and advancements in innovation as well as national security.

Despite the important shortage, there is a bias towards skilled hires, making it hard for entry-level professionals to break into the sector. This, in turn, limits the opportunities for less-experienced professionals to obtain the required know-how and practical exposure. Tackling this issue will require multiple approaches.

Firstly, more effort is needed to improve the branding of cybersecurity as a career choice. Greater emphasis should be placed on the rewarding career path, including the crucial role that cybersecurity professionals play in protecting organizations and society. To do so, among other things, organizations should use communication platforms to provide a comprehensive and easily understandable explanation of the various pathways available in cybersecurity. Mentorship programmes targeted at specific demographics are also an effective way to support individuals considering a career change into cybersecurity.

In addition to professional development, organizations should also pay greater attention to the well-being of their professionals and devise strategies for managing and overcoming burnout among the cybersecurity workforce. To succeed, the tone needs to be set at the leadership level by, for instance, promoting a culture that values a healthy work-life balance. Training programmes that focus on stress management as well as adequate opportunities for employees to recharge are some examples of how such a culture could be implemented. Conducting regular surveys to ascertain employee sentiment can also help provide valuable insights into the overall well-being of the staff. Finally, training the next generation of cybersecurity professionals should include teaching self-care and preserving mental well-being as an essential skill.

3

Key takeaways: navigating cyber frontiers

In a rapidly evolving technological landscape, cybersecurity can no longer be an afterthought.

Balancing the security of generative AI systems requires a multi-faceted approach

2023 has been the year of generative AI. Despite its promise, its widespread adoption across civil society, public and private organizations has raised concerns as cyberattacks have become increasingly sophisticated and targeted.

The responsibility for the security of generative AI systems has been discussed extensively. There should be economic drivers that incentivize the creation of safe, secure and responsible AI systems. Although the responsibility for security is often deferred to the developer of generative AI systems, part of the responsibility also lies on the end users. In a nutshell, developers should make sure the technology is as secure as possible when it goes to market, and end users should be able to use it in a safe and responsible manner.

Another concerning threat from generative AI systems is the heightened ease of generating misinformation and disinformation. Organizations will need to take appropriate measures to mitigate those risks. Growing concerns – such as voice interference through deepfake AI – can be tackled by implementing cybersecurity controls, providing training to increase digital literacy and risk awareness, and implementing authentication technologies, such as fingerprinting. It is important to consider multi-factor authentication (MFA) controls other than voice protocols because impersonation attacks are likely to rise in the future. Using AI technology to fight against AI-generated disinformation can also be effective and help differentiate between original and manipulated content.

Future-looking threats also require strong collaboration

Beyond generative AI, increasing attention has been given to space technologies. Low earth orbit (LEO) technology is critical for many services relied upon for daily life. Business and interpersonal communications, precise timing for banking transactions, healthcare technologies, agriculture and even weather reports all depend on LEO technology. Over the past 10 years, the cost to launch LEO technology has come down significantly, resulting in an increasing number of countries and organizations deploying their own LEO satellites. This makes both the geopolitical and the technical dynamics of governing their secure and responsible use even more complex. Considering there have already been significant cyberattacks on LEO satellites, it is key to ensure the systems are cyber-secure.

Looking towards the future of cybersecurity, the quantum threat is gaining prominence. This is evidenced by the Quantum Computing Cybersecurity Preparedness Act released by the US in 2022. Preparing for the quantum era can be achieved can be achieved by implementing an organization-specific quantum cyber-readiness programme – the Quantum Security initiative recently released its *Quantum Readiness Toolkit: Building a Quantum-Secure Economy*, which presents a set of guiding principles for organizations to navigate the quantum computing era securely. A cross-functional team of quantum experts, cybersecurity experts and possibly crypto evangelists should proactively plan for post-quantum cyber readiness within their organizations.

Cybersecurity will need to adapt to future trends

Although geopolitical and environmental concerns currently dominate the public discourse, cybersecurity is also a significant issue recognized globally. However, perceptions of its severity can vary, indicating the need for continued dialogue and education on this topic. Different age groups and stakeholders also perceive cyber risk differently, with private organizations ranking it higher than governments do.

When looking strategically at the future of cybersecurity over the next 5-7 years, a noteworthy consideration is the anticipated acceleration of technological and business model innovation. Organizations will need to ensure that speed does not come in the way of maintaining or building digital trust. Additionally, digital interoperability (integration) and digital sovereignty (fragmentation) will need to be balanced as nation-states grapple with both sides. Moreover, the ability to develop innovative technological solutions (e.g. generative AI) to detect, analyse and counter new cybersecurity threats will require enhanced collaboration.

Cyber capacity building – ranging from providing awareness and education, enhancing technological capabilities and building effective forms of collaboration on digital security matters – will be paramount for organizations and nations. Cybersecurity challenges and solutions of the future will have to be socialized beyond the traditional fora of cybersecurity experts and feedback sought from outside of the expert communities to ensure a robust analysis and action plan.

To better understand how technological, political, economic and environmental changes are impacting the future of cybersecurity for governments and organizations, the Center for Long-Term Cybersecurity at University of California, Berkeley, the Center for Naval Analyses' Institute for Public Research and the World Economic Forum's Centre for Cybersecurity released the white paper *Cybersecurity Futures 2030: New Foundations*, developed from a foresight-focused research initiative aiming to inform cybersecurity strategic plans around the globe.

Impressions

The Annual Meeting on Cybersecurity 2023 at a glance…

Contributors

Lead author

Joanna Bouckaert
Community Lead, Centre for Cybersecurity,
World Economic Forum
Joanna.Bouckaert@weforum.org

World Economic Forum

Filipe Beato
Lead, Centre for Cybersecurity
Filipe.Beato@weforum.org

Gretchen Bueerman
Research and Analysis Specialist
Centre for Cybersecurity
Gretchen.Buermann@weforum.org

Sean Doyle
Lead, Centre for Cybersecurity
Sean.Doyle@weforum.org

Tal Goldstein
Head of Strategy, Centre for Cybersecurity
Tal.Goldstein@weforum.org

Akshay Joshi
Head, Industry & Partnerships,
Centre for Cybersecurity
Akshay.Joshi@weforum.org

Giulia Moschetta
Research and Analysis Specialist,
Centre for Cybersecurity
giulia.moschetta@weforum.org

Natasa Perucica
Research and Analysis Specialist,
Centre for Cybersecurity
Natasa.Perucica@weforum.org

Luna Rohland
Community Coordinator,
Centre for Cybersecurity
Luna.Rohland@weforum.org

Victor Tuxans Pajares
Early Careers Programme,
Centre for Cybersecurity
victor.tuxanspajares@weforum.org

Kesang Tashi Ukyab
Lead, Centre for Cybersecurity
kesangtashi.ukyab@weforum.org

Acknowledgements

The Centre for Cybersecurity would like to thank all participants and partners for their valuable support and participation in the Annual Meeting on Cybersecurity 2023. For further information, please find the Centre for Cybersecurity's initiatives and partners on the website.

Production

Rose Chilvers
Designer, Studio Miko

Laurence Denmark
Creative Director, Studio Miko

Martha Howlett
Editor, Studio Miko

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