WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

Annual Meeting on Cybersecurity

Enabling Leadership for a Secure Digital Future

Geneva, Switzerland 12-13 November 2019

Contents

Foreword

Alois Zwinggi
Head of the Centre for Cybersecurity
World Economic Forum

As the international organization for public-private cooperation, the World Economic Forum is leading a global effort to drive systemic change on the most pressing cybersecurity issues. We believe that this change will have the greatest impact if the private and public sectors work on solutions together

Cybersecurity has rapidly become both the safeguard and the key enabler of socio-economic innovation, prosperity and stability. Security and digital trust are vitally important as industries transition towards data- and technology-driven business models and governments are challenged by the policy and regulatory implications and the acceleration of the Fourth Industrial Revolution.

At the second World Economic Forum Annual Meeting on Cybersecurity held in Geneva Switzerland on 12-13 November 2019, over 160 leaders and experts in cybersecurity strategy, policy regulation and technology aimed to advance three overarching priorities for a secure and sustainable digital future: Strengthening global cooperation for digital trust and security, securing future digital networks and technology, and building skills and capabilities for the digital future.

Meeting participants included highest-level corporate executives, government and policy leaders, and experts representing 18 countries, 10 international organizations, over 20 specialized agencies and 86 private-sector businesses with a broad cross-industry profile.

The global borderless nature of cyberspace offers economies and societies tremendous and unprecedented opportunities for sharing solutions, innovation, operational collaboration and continuous capacity-building. In the ubiquitous proliferation of connected digitalization driven by 5G, cloud services, artificial intelligence, the internet of things, physical convergence and biometric identification opportunities can materialize and flourish on the condition that cyberspace is optimally understood, secure and trustworthy.

Despite the well-acknowledged need for building digital trust at multiple levels – across countries for the stability of cyberspace, between corporations and users on the security of their data, and on new technologies that can be leveraged to this end – at this meeting we heard that “we don’t have time for trust”. The speed and volume of cyber challenges, threats and vulnerabilities are accelerating faster than the opportunities, to a point where “today, not only has the speed and volume of technological development outpaced the regulators, it is now outpacing its creators”. The growing economic and social costs of unbridled technological change, cyberattacks and malicious acts are increasing inequalities, causing technological and geopolitical rifts and throttling much of the world to a “cyber poverty line”.

It is the responsibility and duty of global leadership in government, business, civil society and academia to effectively harness the power and steer the promise of the Fourth Industrial Revolution and its ecosystems of digital networks to a secure digital future – one that yields maximum benefit for the greatest number while reducing to a minimum the collateral ills, threats and dangers to economies, societies and individuals.

Today’s challenges call for new modes of global leadership and collaboration. This meeting and all our activities on the Platform for Cybersecurity and Digital Trust seek to enable leaders at all levels to practice cybersecurity as a public good, incorporating security by design and default.

Leveraging the multistakeholder capabilities of the World Economic Forum we will be sharing 10 key messages from the cyber community with participants of our Annual Meeting 2020 in Davos in January to facilitate concerted leadership on the technical and operational challenges and the policy and strategic decisions of our day for our future.

Ten Messages for Global Leaders in Davos

To drive cybersecurity and digital trust as enablers of technological and economic sustainability and cohesive societies, over 160 global cybersecurity leaders and practitioners from the public and private sectors meeting at the Forum's Annual Meeting on Cybersecurity propose the following priorities:

1. In the Fourth Industrial Revolution, where ubiquitous connectivity and digitalization underpin socio-economic progress and prosperity whereas cyberattacks are increasing in frequency and sophistication, it is the responsibility of **public- and corporate leaders to take ownership of the challenge** to ensure global cybersecurity and digital trust.

2. Board and C-Suite executives need to **gain a better understanding of the cyber risks** to which their organization is exposed and of their cyber readiness, to be able to take more informed investment and resourcing decisions to enhance preparedness and resilience to attacks.

3. Both public and private organizations need to **improve their cyber crisis management**, develop holistic response and recovery plans, including a crisis communication plan strategy, to limit economic, reputational and legal consequences.

4. Leaders need to **create a culture of cybersecurity** from the entry level to the top leadership of an organization – creating awareness is no longer sufficient. Regular training and practical exercises can make a real difference.

5. Leaders may need to **rethink organizational structures and governance** to enable a more robust cybersecurity posture and break silos.

6. Innovation in cybersecurity and rapidly evolving technologies, such as AI, identity management and quantum computing, **call for greater investment** to stay ahead of cybercriminals who are adopting such technologies even faster and to their advantage.

7. **Global cooperation across the public and the private sectors is vital.** Among the dimensions to be prioritized are information-sharing, business cooperation with law enforcement agencies, and skills and capacity development, particularly in emerging economies.

8. Maintaining an **open and secure internet** requires collaborative effort between the public and private sectors. The Internet Service Provider Principles agreed upon at this Annual Meeting on Cybersecurity are a major step towards reinforcing safety and trust in cyberspace.

9. **Trusted and verified cybersecurity ratings** are required to assess and improve understanding of an organization's cybersecurity posture and how it ranks with peers. Cybersecurity should be one element of a broader scorecard to evaluate for organizational resilience.

10. The World Economic Forum and its Platform for Shaping the Future of Cybersecurity and Digital Trust provide a **neutral, trusted and globally recognized platform to facilitate cooperation** and deliver tangible impact on the systemic challenge of global cybersecurity.

Børge Brende in the Opening Plenary: Making Global Cooperation Work

Shi Xiansheng in the Opening Plenary: Making Global Cooperation Work

Jason Mallinder in the Opening Plenary: Making Global Cooperation Work

Jim Alkove in the Opening Plenary: Making Global Cooperation Work

Gabi Dreo Rodosek in the Opening Plenary: Making Global Cooperation Work

Rob Wainwright in the Opening Plenary: Making Global Cooperation Work

Enhancing Global Cooperation for Trust and Security

Promoting dialogue and accelerating new models of effective cooperation at the technological, operational, legal and policy levels between stakeholders across the ecosystem. How can we ensure trust and robust decision-making?

Cybersecurity is one of the most strategically important issues in our globalized world. Where trade makes up 40% of global GDP and 40% of a product's content is manufactured in other countries, the notion of decoupling no longer works. And yet, the world is becoming more fragmented. This has serious implications for companies and countries in their efforts to effectively adapt to the phenomenal speed and breadth of technological change in order to optimize the benefits while protecting against rising vulnerabilities and threats.

Government and business leaders invest billions in cybersecurity but this is not adequate to address the magnitude of cyberattacks which have increased by 67% over the past five years. Business and political leaders traditionally focus on defending their own companies or jurisdictions, which is not effective in a borderless cyberspace and, collaterally, cyberthreat surface.

Broadening the horizon

Success will depend on a change in the mindset of leaders across governments and industries, as well as a change in organizational culture. First, attention must move from enterprise to ecosystem parameters. Moving to an ecosystem model requires building dynamic cooperation among all cybersecurity stakeholders – governments, companies, industries, law enforcement agencies, academia, civil society and cyber technology experts – who share experience and develop standards and best practices collaboratively. Examples exist in the financial services industry and public utilities, like electricity, where the highest levels of leadership have begun working together to solve common cybersecurity problems.

Beyond leadership, further challenges remain. Trust lies at the heart of stakeholder willingness to share and is too often lacking, especially, when sharing is perceived as a threat to an entity's competitive advantage or security. At the same time, communities have different needs and requirements that determine what, why and when they will share. There are different sharing cultures and perceptions of risk between East and West that influence openness to sharing. Today there are no visible, economically-driven incentives to such sharing. Instead of relying on goodwill, which underlies person-to-person relationships, the challenge is to create incentives on the basis of an economic model of two-way exchange that drives rational behaviour between countries and institutions to share information and best practices. Current bilateral or limited multilateral information sharing, while useful, falls short of reaching the global scale needed to combat constantly evolving cyber sophistication and threats.

Meanwhile, across industries and sectors, cybercrime's risk profile is changing. For every 1,000

cyberattacks or breaches, only three arrests are recorded. The gap in global enforcement cannot change without resolving the gap between security and incident response efforts led by the private sector, and cybercrime investigation and prosecution led by law enforcement agencies (LEA). There is a pressing need to adapt new models of public and private cooperation in this field at the global level, taking into consideration the nature of the threat, the international operations of private-sector actors and the limits of national law enforcement processes. There are some instances of productive LEA and private-sector cooperation but to date there is no scalable, replicable regional and international cooperation across the public-private security ecosystem to enable effective global enforcement. The World Economic Forum, building on its neutral and global platform, can mobilize a group of leading public-private actors in a dedicated partnership that would explore new ways of working together against global cybercrime.

Bridging the gap between technology and policy-making is another priority. In the Fourth Industrial Revolution, where digital and social systems are integrally connected, policy-makers are compelled to learn, to get up to speed about the technology that is progressively dominating our lives, as never before. This reality is further compounded by the numerous existing processes and initiatives – multilateral, government and private sector-led – that aim to address cybersecurity challenges internationally and require the attention of policy-makers, corporate executives and technologists, but often have a siloed scope. The fragmented and complex overall landscape of existing architectures has a high potential for gaps and inefficiencies in global cooperation. Several participants pointed to the strong need to raise leadership awareness of these global initiatives and identify where there is over- and under-resourcing of efforts to inform a realignment towards those that are improving cooperation at scale, globally.

One key challenge for governments is to ensure that cybersecurity provisions in laws and regulations are drafted according to principles that apply to and encompass all sectors. The technology industry and more broadly the private sector are urged to spearhead the drive to enhance understanding of cyber technology, expand and strengthen global cooperation on cybersecurity. As one crucial step, CISOs could strive to build consensus within government by endorsing cybersecurity as a priority, by design and by default

Jean-Yves Art, Despina Spanou, Hannes Grassegger and Stephane Duguin in the session Keeping it Real: Tackling Digital Misinformation

– because when data breaches spill people's personal details into the public realm, trust in the system rapidly evaporates. What's needed are coherent, well-balanced and agile policies combined with general and effective consumer education to bolster trust in the digital economy.

Multistakeholder collaboration is the most effective way of addressing cyberthreats and will have to accelerate to keep up with cyber criminals and the speed of technological change. The challenge is not only in educating stakeholders on cyber technology and setting up platforms and processes for cooperation, but more fundamentally, in building the requisite trust to incentivize sharing. The Forum is an effective and recognized platform for bringing key stakeholders together to develop trust-building mechanisms and cooperation on information-sharing that are crucial to achieving the reality of a global community equipped with the expert understanding, tools and processes needed to successfully protect from malicious intent while improving innovation, new technologies and services.

Sharing in the Absence of Trust

Combating cybercrime effectively relies on an ecosystem of stakeholders willing to share information across industries, geographies, and the public and private sectors. Trust, which drives the sharing culture, is not always achievable. In an environment where "$1.6 billion a year is being laundered and only 1% is being saved, we have to find innovative ways to share across borders," said one panellist. Homomorphic encryption, which allows computation on encrypted data without ever seeing the data content, is one example of a new technology that can enable sharing in the absence of trust.

Tim Maurer in the session Cybersecurity and Digital Trust: Strengthening Global Architectures

Heli Tiirmaa-Klaar in the session Cybersecurity and Digital Trust: Strengthening Global Architectures

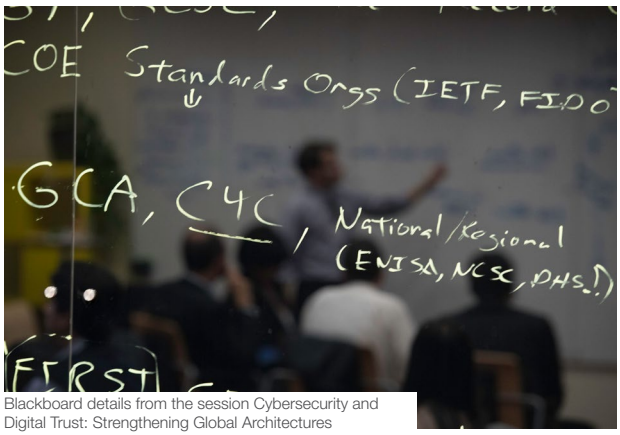
John Lynch, Seamus Tuohy and Vishal Salvi in the session Collateral: Shaping Cybersecurity Through Non-Cyber Policies

Enhancing Global Cooperation for Trust and Security

Jennifer Elliott in the session Collateral: Shaping Cybersecurity Through Non-Cyber Policies

Neal Pollard in the session Collateral: Shaping Cybersecurity Through Non-Cyber Policies

Kai Hermsen in the session In Data We Trust?



Blackboard details from the session Cybersecurity and Digital Trust: Strengthening Global Architectures

Claudio Guarnieri in the session Security that Counts

Sol Echeverria in the session Security that Counts

Sandra Joyce in the session Beating Cybercrime: Partnering to Close the Global Enforcement Gap

John Lynch in the session Beating Cybercrime: Partnering to Close the Global Enforcement Gap

Thomas Harvey in the session Beating Cybercrime: Partnering to Close the Global Enforcement Gap

Chris Gibson in the session Beating Cybercrime: Partnering to Close the Global Enforcement Gap

Craig Jones in the session Beating Cybercrime: Partnering to Close the Global Enforcement Gap

Securing Future Digital Networks and Technology

Promoting solutions to acute cybersecurity challenges in the Fourth Industrial Revolution and ways to incentivize the development of secure technologies. How can we build cybersecurity into technologies, corporate and public policies from the get-go?

Securing future digital networks demands leadership and cooperation – not just smarter technology. Leaders need to understand the tech in order to cooperate effectively.

Securing Industry 4.0

Today, industries are benefitting from new levels of digitalization and connectivity. Physical things and cyber systems are becoming increasingly connected – from assets to people and data – by harnessing technologies including biometrics, artificial intelligence, machine learning, autonomous vehicles, blockchain and the industrial internet of things (IIoT).

Technological advances are creating tremendous opportunities for improved operational efficiencies, customer experience and quality of life. The opportunities that IIoT capabilities can generate for several industries, including aviation, electricity, automotive or healthcare, are unprecedented.

With the new heights of efficiency enabled by increasing digitalization and connectivity come new frontiers of vulnerability. Rapid cyber capability breakthroughs also create new potential attack vectors at an equally fast pace.

Due to their complexity, cyber-attacks on critical national industries (CNI) may be more difficult to detect and control, and generate cascading effects resulting in economic losses, industrial disruption and, in some cases, human casualties.

Beyond security, cyber resilience requires a focus on protecting critical functions, in addition to assets. Cybersecurity challenges remain underestimated. It is essential that public- and private-sector leaders engage in a collaborative and risk-informed approach globally, by sharing practices, insights and threat intelligence, to ensure a secure and resilient ecosystem.

To enable public-private collaboration and dialogue across industries, the World Economic Forum has spearheaded several industry-specific initiatives – in electricity, aviation, financial services, investment. Some of the systemic industry challenges being addressed are securing a highly interdependent supply chain, building a coherent approach to risk management across the value chain, building a culture of cyber resilience and fostering dialogue with policy-makers to influence policy development.

Opportunities and risks of future technologies

Our highly interconnected digital networks are only as strong as the weakest link – and the threats to these systems are posed by

the very technologies that drive them. Artificial intelligence (AI) gives attackers the ability to mimic and distort reality in a way that threatens defences that depend on human judgement. AI can now fake biometrics such as voice, based on just five seconds of target recording. AI-powered attack algorithms operate at such speed and scale they risk overwhelming cybersecurity approaches. Malware developers will exploit AI to produce stealthier attack tools, then employ AI to extract more value from the data they steal.

Hyperconnectivity – driven by 5G/6G and the proliferation of the internet of things (IoT) – is expanding the attack surface, especially in terms of vulnerabilities. As we migrate our digital stacks to the Cloud, the target we present to the criminals expands.

Quantum computing is considered the next opportunity (and threat). Although experts think its impact is 5-10 years out, quantum has the capacity to radically reduce the time it takes to destroy the algorithms on which many secure systems depend.

Stepping Up Large-Scale Cyber Defence

There are three main ways to attack a digital network: through hardware, such as routers; through vulnerable code in software; or through manipulating the flow of internet traffic itself. If telecommunications providers take collective action in all these areas, the internet will be a safer place for us all.

The scale of the problem is huge. Every month, BT – the UK's largest internet service provider (ISP) – prevents more than 100 million attempted malware connections. Yet UK police prosecuted just 8,214 individuals for fraud or cybercrime in the year to March 2017 (latest figures available). The risk-reward ratio for cybercriminals is skewed too far in their favour. We need to make it much harder for them to succeed.

The World Economic Forum is leading an initiative with BT, the Global Cyber Alliance and a number of other partners to define a set of principles to help ISPs around the world to understand better the types of actions that could have significant impact on high-volume cyberattacks. In November 2019 broad consensus was reached on these principles, which will be launched at the Annual Meeting 2020 in Davos. Meanwhile, more work is needed to engage governments and the public sector in formulating policy frameworks to provide the best incentives for ISPs to act securely. The challenge is to ensure the internet remains not just open, but safe.

Participants in the session Beyond 12345: No More Passwords

Meanwhile the world's 1,600-plus crypto currencies appear to offer cheap, quick ways to store, send and receive money across borders – especially for unbanked populations. But they also present a number of emerging risks, which our current cyber defences are not robust enough to tackle. Bitcoin's blockchain is distributed across five million computers, making it difficult to hack. Each block's information is anonymized, so it is hard to know who is adding blocks or upholding the chain, raising trust issues. In 2016, hackers attacked the blockchain code of DAO and siphoned off $50 million of crowd-funded assets. Everyone running the code could watch the criminals pick DAO's wallet in real time, but the vulnerability couldn't be patched unless everyone patched it.

Our current cyber defences are not robust enough to tackle these emerging risks. We haven't made enough progress on information sharing, systemic resilience or collaborative attribution. We need to act faster. We must combine the skills of security analysts with data scientists to integrate security into the design of AI and the IoT. The good news is these powerful new technologies can be used in defence as well as attack.

As 5G, 6G and the IoT drive hyperconnectivity, we no longer have days to fashion our responses to security breaches; we need to react in real time. AI and machine learning (ML) offer huge opportunities. Security Operations Centres are inundated with potential security breaches – AI will help them cut through the noise and focus on which threats really matter. AI tools can help with threat attribution, by detecting anomalies across ecosystems and tracking attack patterns that mimic human behaviour in a way that a human can't. One Fortune 500 company has improved its rate of attribution 10 times by using AI. But equally, AI's capacity for deep fakes will make attribution harder. We can use AI to detect if we're being attacked by AI – but it may lead to an "AI arms race".

As Cloud storage grows, the potential return on investment (ROI) for cyber criminals grows too. We need to keep revisiting the risk equation of handing over our data stacks. But the Cloud does offer us opportunities – to upgrade security when we move to the new environment, to establish more transparent processes, to map legacy controls to Cloud controls, and to enhance SIM standards. More needs doing, however, to harden our APIs and figure out how to remain resilient when the Cloud is attacked.

Quantum computing is experiencing a second revolution. Although it poses challenges to asymmetric encryption, the NSA has launched a search for quantum-resistant algorithms which should bear fruit by 2023. Quantum also provides positive opportunities. We can use it as a "change motivator", to conduct an inventory of data and data processes that are vulnerable. Quantum might have greater impact on identity, specifically on data integrity and confidentiality – potentially leading to the replacement of digital IDs. Companies need guidelines on how to make their IT and OT (operational technology) quantum-safe. Shareholders should expect large investments within the next decade to make this happen.

Better cooperation to overcome non-tech barriers

Fighting tech with tech is necessary, but not sufficient to keep our systems secure. Some of the biggest barriers to more robust cybersecurity are not faulty code or machine learning, but non-tech issues like fragmented regulation, poor information sharing and mistrust. Whether we are cyber experts or civil society, lawyers or law enforcement, private sector or politicians – it's time to crawl out of our silos and start cooperating.

The plethora of conflicting cybersecurity rules is a major obstacle. CISOs spend 40% of their time complying with regulations. Last year, 120 new cyber regulations were published in the US. There are nearly 90 frameworks governing AI alone. This proliferation of rules decreases the resilience of global systems, especially in finance, making life easier for cyber criminals.

For example, the US-based Financial Services Sector Coordinating Council has crunched 3,000 global regulations into a cybersecurity "profile" with 277 questions for international banks and 70 for smaller banks. Getting national regulatory bodies behind this push towards standardization is vital. Regulators and banks need to understand each other's red lines – which means more training, particularly in emerging economies. The financial industry should speak with one voice to avoid sending regulators mixed messages. Regulation can threaten innovation – we need sandboxes where companies can innovate safely while regulators develop appropriate levels of security. A shared global approach to regulating cybersecurity is badly needed. But some argue we don't have time to develop common standards – better that we focus on desired outcomes to avoid over-prescriptive regulation.

Public trust in the digital economy – slow to build, quick to lose – is a vital commodity. Data breaches from banks and social media have undermined trust in the security of personal data online. There has to be a better balance between privacy, personal consent and the innovations that amass and monetize our data. Boosting citizen awareness through regulations such as the EU General Data Protection Regulation is a start.

But we also need to take decisions. What is ethical behaviour in the AI context? Who takes legal responsibility for the consequences of AI-powered decisions? We still have the chance to be AI's master, not its slave. Information sharing is vital, but what should we share, when, how, who with? None of these pressing questions can be resolved without stronger global cooperation across public and private sectors.

Laura Deaner, Haiyan Song and Katheryn Rosen in the session Can the Market Fix It?

Einaras von Gravrock in the session Can the Market Fix It?

Nina Paine in the session Getting Priorities Straight: Cybersecurity Challenges in Financial Services

Participants in the session Crypto Currencies: Cutting through the Hype

Laurent Haug, Bertrand Perez and Christophe Nicolas in the session Crypto Currencies: Cutting through the Hype

Klaus Schwab in the session Crypto Currencies: Cutting through the Hype

Jeremy Grant in the session Cyber 2025: Preparing for Future Threats

Lutfey Siddiqi in the session Getting Priorities Straight: Cybersecurity Challenges in Financial Services

Reiko Kondo in the session Cyber-Resilience in the Fourth Industrial Revolution: From Critical Infrastructures to Critical Systems

Thomas Kropp in the session Cyber-Resilience in the Fourth Industrial Revolution: From Critical Infrastructures to Critical Systems

Khalid Al-Harbi in the session Cyber-Resilience in the Fourth Industrial Revolution: From Critical Infrastructures to Critical Systems

Marc Henauer in the session Cyber-Resilience in the Fourth Industrial Revolution: From Critical Infrastructures to Critical Systems

David Garfield in the session Cyber-Resilience in the Fourth Industrial Revolution: From Critical Infrastructures to Critical Systems

Mark Hughes in the session Cyber-Resilience in the Fourth Industrial Revolution: From Critical Infrastructures to Critical Systems

Yasser N. Alswailem in the session Stepping Up Large-Scale Cyber Defence

Salim Al Ruzaiqi in the session Smart Cities: A Prism of Cybersecurity Challenges

Haiyan Song in the session Smart Cities: A Prism of Cybersecurity Challenges

Maria Vello in the session The Promises and Perils of Zero Trust Technologies

David Lau in the session Smart Cities: A Prism of Cybersecurity Challenges

Ian Levy in the session Securing Next-Generation Networks


Pär Gunnarsson in the session Securing Next-Generation Networks


Laura Deaner in the session Chasing the Silver Bullet? Innovation in Cybersecurity


Sam Curry in the session Chasing the Silver Bullet? Innovation in Cybersecurity


Floris van den Dool in the session Chasing the Silver Bullet? Innovation in Cybersecurity

Vikram Sharma in the session Chasing the Silver Bullet? Innovation in Cybersecurity

Bob Xie in the session Rethinking Supply Chain 4.0 Security

Markus Braendle in the session Rethinking Supply Chain 4.0 Security

Philipp Amann in the session Cyber 2025: Preparing for Future Threats

Participants in the session Beyond 12345: No More Passwords

Building Skills and Capabilities to Secure Our Digital Future

Promoting human capital development, knowledge transfer and the adoption of best practices for leaders in cybersecurity. How can we build talent and leadership momentum for cybersecurity?

In recent years, the culture of cybersecurity has made significant advances in becoming increasingly incorporated into business, civil society and government. The number of governments that have adopted a national cybersecurity strategy has increased exponentially, while there are also more concerted efforts towards better regulation with security and privacy-by-design standards. Company boards are also increasingly making cybersecurity an integral part of their operations. Similarly, academia is advancing on research for new cybersecurity solutions, and civil society at large is developing a progressively better understanding of the cybersecurity landscape and contributing to the relevant policy dialogues. As one participant noted: “Cybersecurity is an issue that concerns everyone. We’re all in this together.”

Call for more scalable capacity-building solutions

While the digital revolution is heralded for increased efficiency and reduction of costs, the potential offset of those benefits by the associated security risks puts an additional burden to all stakeholders across sectors to have the capacity to build and maintain the security of systems and data. The lack of critical mass in skills and capacities across national institutions, corporations and civil society highlights the need to make skills-building and knowledge-sharing far more prominent in the cybersecurity ecosystem.

This involves bringing together different communities and partners, while appropriately financing and supporting training, implementation of best practices and sharing of lessons learned - including negative experiences. As one participant put it: “We have learned far more from bad mistakes than anything else, so sharing them with others might not only help them, but all of us now and in the future.”

A proactive, scalable and sustainable approach for addressing the cybersecurity capability deficit, beyond ad hoc activities, is to think in terms of cybersecurity “ecosystems” development. A whole-of-ecosystem approach at a local level ranges from identifying the right stakeholders in a city or a region while supporting research, skills and talent development, diversity and inclusion and fostering innovation. A global network where diverse partners can create impact by joining forces and contributing with respective resources and expertise could significantly contribute to addressing this gap. The World Economic Forum could be the ideal platform for such comprehensive action.

More broadly, the effort of promoting digital transformation as a key enabler of socio-economic prosperity must, particularly in not “cybersecurity mature” countries and regions, needs to develop in parallel with the incorporation of security. Moving forward in achieving the

Sustainable Development Goals, we need to start building a comprehensive international development agenda that mainstreams cybersecurity and takes into account the global cyber skills shortage.

A holistic cybersecurity culture

Within organizational culture, the time has come to acknowledge cybersecurity as a business-enabling function to be managed like any other risk management issue. An organization's cybersecurity posture has a direct impact on its capacity to operate and generate value – and could be vital to its very existence. Leaders are encouraged to create a culture of cybersecurity throughout their organization – from entry level to top leadership.

Yet, numerous companies still fail to ensure appropriate security measures in their overall operations and governance, extending to both customers and suppliers. As one case in point, the number of businesses that do not bother with passwords more elaborate than "admin" is "staggering", one participant noted. Major progress has been made in certain companies whose Boards clearly understand the importance of cybersecurity.

Smart Cities Reflect an Accelerated Form of Global Cyber Concerns

With the prism of all cybersecurity challenges accelerated in cities – where over 55% of the world's population lives – dealing with them at the local level may be a necessity and could help lead to more global solutions. The case of smart cities makes the convergence of old and new technologies palpable. Rapid transport systems can now be tracked in real time enabling travellers to know expected arrival or departure times. Car batteries can be charged at night with power then sold to the grid at peak times during the day. Hospitals can digitally share data, including accessing experts for instant diagnoses across the globe. All this can lead to far greater sustainability but also risk. Should a hacking incident disrupt power grids or computer access, then medical operations cannot be performed while trains will come to a halt. Security and safety by design need to be incorporated in all aspects of urban development.

But cybersecurity is still and by far insufficiently integrated into corporate and government culture. Board members and decision-makers still need to be better informed and updated on the benefits and risks of new technologies.

This also holds for the public-at-large. Most people, including the over 2.7 billion using social media world-wide, have little idea about cyber risks. Greater public awareness about cybersecurity needs to be placed high on the agenda. Governments, companies and civil society urgently need to invest in more effective outreach, and to involve all players as early as possible. Cyber resilience and security must always remain a vital concern of any operation, not a peripheral nice-to-have.

Moreover, with the recognized mismatch of talent throughout the industry, the private sector can also contribute to reducing the talent and gender gap. Companies can expand the pool of both cybersecurity experts and public interest technologists by pushing for changes in educational curricula from kindergarten through college and beyond. CISOs can increase diversity and inclusion, starting with addressing the gender gap by working on hiring policies and practices, also advocating that cybersecurity is an attractive career option for men and women alike, as well as for non-traditional backgrounds.

Trust and cooperation to tackle the capacity deficit

The private and public sectors should drastically improve their collaboration in a manner that first and foremost engenders trust through building cybersecurity capacity. Greater interaction means exploring how both sides can build on partner requirements, such as civil society concerns for protecting human rights defenders or ordinary citizens from threats, or businesses worried about being hacked. “The problem is that companies are seeking returns on their investment, while civil society is more outcome-based in its bid to protect communities,” said one participant. Not all forms of collaboration are created equal.

Corporate policies are also being increasingly defined by engaged employees. This includes leveraging company resources in the manner of “do no harm.” This could include providing funding, services or expertise in support of human rights groups, public interest journalism or educational initiatives. At the same time, companies need to understand that they are not marketing a product, but rather becoming part of civil society. The rules of the game have to be clearly defined, yet, as one participant pointed out: “This sort of ‘spiritual’ engagement can prove very powerful.”

Reaching out to youth is crucial for the future

In the race against the skills gap, the failure to engage with youth can be detrimental. “If we wish to see the future, we need to focus on education,” said one participant. For one, the international community is still failing to produce sufficient new talent to fill the three million jobs needed every year in the cybersecurity industry. While young people are indeed being trained in countries such as South Africa, India or Costa Rica, they are not necessarily finding employment. There has to be far broader involvement of the younger generation to better understand cybersecurity concerns. Cybersecurity has hardly been integrated into school curriculums around the world. And yet young people represent the main source for new talent.

Participants in the session Empowering Cybersecurity Leaders

Participants in the session Hard-Wiring Gender Parity in Cybersecurity

Participants in the session Empowering Cybersecurity Leaders

Dan Yerushalmi in the session Adding Some Mint: Inducing Behaviour Change

Nicolas Fischbach in the session Adding Some Mint: Inducing Behaviour Change

Elly van den Heuvel in the session Getting the Board on Board: Improving Cybersecurity Governance

Rosa Kariger in the session Getting the Board on Board: Improving Cybersecurity Governance

David Thornewill von Essen in the session Getting the Board on Board: Improving Cybersecurity Governance

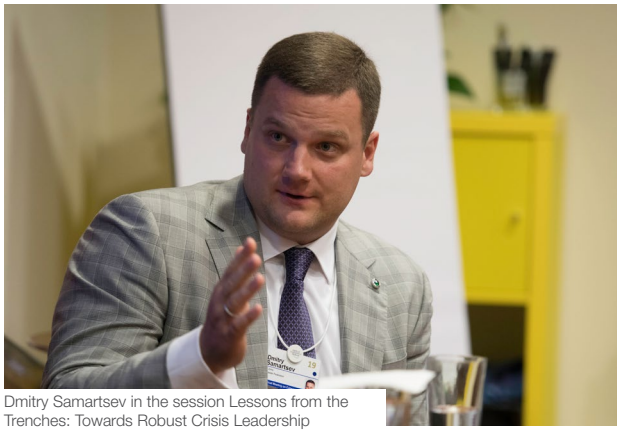
Participants in the session Getting the Board on Board: Improving Cybersecurity Governance

Building Skills and Capabilities to Secure Our Digital Future

Gabi Dreo Rodosek in the session Lessons from the Trenches: Towards Robust Crisis Leadership


Mark Swift in the session Lessons from the Trenches: Towards Robust Crisis Leadership

Brett Solomon in the session Driving Development: Cybersecurity and the Digital Dividend


Dmitry Samartsev in the session Lessons from the Trenches: Towards Robust Crisis Leadership

Sudheesh Babu in the session Lessons from the Trenches: Towards Robust Crisis Leadership

Philip Reitinger in the session What If Everyone Were a Cyber Professional?

Jim Alkove in the session What If Everyone Were a Cyber Professional?

Sandra Wheatley Smerdon in the session What If Everyone Were a Cyber Professional?

Participants in the session Tackling the Capacity Gap: Accelerating Cybersecurity Ecosystems

Ana Maria Montero in the Closing Plenary: Enabling Leadership for a Secure Digital Future

David Koh in the Closing Plenary: Enabling Leadership for a Secure Digital Future

Risto Siilasmaa in the Closing Plenary: Enabling Leadership for a Secure Digital Future

René Bonvanie in the Closing Plenary: Enabling Leadership for a Secure Digital Future

Klaus Schwab in the Closing Plenary: Enabling Leadership for a Secure Digital Future

Participants in the Closing Plenary: Enabling Leadership for a Secure Digital Future

Participants in the Closing Plenary: Enabling Leadership for a Secure Digital Future

Participants in the Closing Plenary: Enabling Leadership for a Secure Digital Future

Participants in the Closing Plenary: Enabling Leadership for a Secure Digital Future

Programme in brief

Tuesday
12 November

Enhancing Global Cooperation for Trust and Security

Securing Future Digital Networks and Technology

Building Skills and Capabilities to Secure our Digital Future

09.15 - 10.15 Plenary
Opening Plenary: Making Global Cooperation Work
From climate change to global trade - international cooperation is seeing a particularly hard time. How can we gear up to make cybersecurity an exception to that rule?

Børge Brende, President, World Economic Forum
Alois Zwinggi, Head of the Centre for Cybersecurity, World Economic Forum
Jim Alkove, Chief Trust Officer, Salesforce, USA
Gabi Dreo Rodosek, Executive Director, Research Institute CODE, Universität der Bundeswehr München, Germany
Jason Mallinder, Deputy Chief Information Security Officer; Global Head, Information Security, Credit Suisse, Switzerland
Shi Xiansheng, Deputy Director General, Bureau of International Cooperation, Cyberspace Administration of China, People's Republic of China
Rob Wainwright, Partner, Deloitte, Netherlands

10.30 - 11.15 Hub
Beyond 12345: No More Passwords
With “123456” still the most prevalent password globally, primitive authentication is the weakest link in cybersecurity at the current speed of technological acceleration and innovation. How can public and private entities revolutionize authentication to enhance effective security and improve the user experience?

Daniel Dubowski, Vice President - Business Information Security Officer, USIS, Equifax, USA
Andrew Shikiar, Executive Director & Chief Marketing Officer, FIDO Alliance, USA

10.30 - 12.00 Workshop
Cyber 2025: Preparing for Future Threats
The global cyberattack surface is both widening and deepening as artificial intelligence, next-generation networks and the internet of things (IoT) fundamentally alter the digital landscape and drive convergence with the physical world. How can the public and the private sectors prepare for the implications?

Sandra Joyce, SVP, Global Intelligence, FireEye, USA
Philipp Amann, Head of Strategy, European Cybercrime Centre, Europol, Netherlands
Nick Coleman, Global Cyber Security Risk Leader, IBM, USA
Yuval Elovici, Professor, Department of Software and Information Systems Engineering, Ben-Gurion University of the Negev, Israel
Jeremy Grant, Coordinator, Better Identity Coalition, USA
Jamie Saunders, Oxford Martin Fellow, University of Oxford, United Kingdom

10.30 - 12.00 xChange
Smart Cities: A Prism of Cybersecurity Challenges
With applications for IoT, big data and AI as well as the crucial role of digital technology in the delivery of public services and infrastructure, smart cities are prone to become the prism of future cybersecurity challenges. How can cities and their technology partners best prepare?

David Lau, VP Software Engineering, Tesla, USA
Salim Al Ruzaiqi, Chief Executive Officer, Information Technology Authority (ITA), Oman
Haiyan Song, Senior Vice-President and General Manager, Security Markets, Splunk, USA
Jean-Pierre Hubaux, Full Professor, School of Computer and Communication Sciences, Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland
Grant Waterfall, Global Cybersecurity and Privacy Assurance Leader, PwC, United Kingdom
Laurent Haug, Swiss Correspondent, Wired UK, United Kingdom

10.45 - 11.45 Panel
Keeping it Real: Tackling Digital Misinformation
Digital misinformation, distortion and - increasingly - the manipulation of images are eroding trust in democratic institutions, media and digital technologies. Fact-checking data bases can only do so much to solve these challenges. What does it take to safeguard the integrity of data, political processes and the economy in the future?

Stephane Duguin, Head of the EU Internet Referral Unit and Head of Innovation at Europol, Europol, Netherlands
Hannes Grassegger, Technology Reporter, Switzerland
Despina Spanou, Director, Digital Society, Trust and Cybersecurity, European Commission, Brussels
Kirstine Stewart, Head of Shaping the Future of Media, Entertainment and Culture; Member of the Executive Committee, World Economic Forum; Young Global Leader

10.45 - 12.00 Roundtable
Empowering Cybersecurity Leaders
Strengthening fundamental cybersecurity leadership principles across government, industry and especially in small- and medium-sized businesses holds large potential for positive impact. How can the essential tenets of cybersecurity leadership be scaled faster to establish a robust security posture across markets and sectors?

Paige Adams, Group Chief Information Security Officer, Zurich Insurance Group, USA
Rosa Kariger, Chief Information Security Officer, Iberdrola, Spain
Katheryn Rosen, Managing Director, Technology and Cybersecurity Policy and Partnerships, JPMorgan Chase & Co., USA
Rob Wainwright, Partner, Deloitte, Netherlands
Troels Oerting Jorgensen, Chairman of the Advisory Board, Centre for Cybersecurity, Switzerland

11.30 - 12.15 Hub
What If Everyone Were a Cyber Professional?
What if offering promising career paths along with cutting-edge education and industry certification could help end the global cyber skills gap?

Jim Alkove, Chief Trust Officer, Salesforce, USA
Philip Reitinger, President and CEO, Global Cyber Alliance, USA
Sandra Wheatley Smerdon, Senior Vice President, Threat Intelligence, Marketing and Influencer Communications, Fortinet, USA

13.45 - 15.15 xChange
Beating Cybercrime: Partnering to Close the Global Enforcement Gap
Only three in 1,000 cyber incidents result in an arrest in the USA – a figure reflective of the global enforcement gap which is associated with the fundamental disconnect between cyber incident response and law enforcement. What new models of public and private cooperation can help to meet this persistent challenge?

Thomas Harvey, Global Head of Cyber Response & Intelligence, Banco Santander, Spain
Sandra Joyce, SVP, Global Intelligence, FireEye, USA
John Lynch, Chief, Computer Crime and Intellectual Property Section, Criminal Division, US Department of Justice, USA
Craig Jones, Cybercrime Director, International Criminal Police Organization (INTERPOL), Singapore
Philipp Amann, Head of Strategy, European Cybercrime Centre, Europol, Netherlands
Heather King, Chief Operating Officer, Cyber Threat Alliance, USA
Maria Vello, Chief Executive Officer, Cyber Defence Alliance, United Kingdom
Chris Gibson, Executive Director, FIRST, USA

13.45 - 15.15 Workshop
Chasing the Silver Bullet? Innovation in Cybersecurity
AI is expected to unlock up to $5.8 trillion of value in business, quantum computing may hold the key to new drugs and materials and cloud services revolutionize how we store and manage data. What are the opportunities and perils for cyber practitioners?

Sam Curry, Chief Security Officer, Cybereason, Inc, USA
Laura Deaner, Global Chief Information Security Officer, S&P Global, USA
Floris van den Dool, Managing Director, Accenture Security, Europe; Latin America Lead, Accenture, Netherlands
Vikram Sharma, Founder and Chief Executive Officer, QuintessenceLabs, Australia
Ruth Shoham, Executive Director, Strategy and Capacity Building, Israel National Cyber Directorate, Israel

13.45 - 15.15 Workshop
Security that Counts
Civil society actors working as frontline defenders of basic rights and values increasingly find themselves in the crossfire of digital threats. Partnering with business offers the opportunity to both gather insights about emerging threats and to ensure that these actors and organizations can continue to serve society. How can new partnership models between civil society and business be forged to implement more effective cybersecurity practices?

Claudio Guarnieri, Head of Security Lab, Amnesty International, United Kingdom
Philip Reitinger, President and CEO, Global Cyber Alliance, USA
Miguel Sanchez San Venancio, Global Chief Security Officer, Telefonica, Spain
Brett Solomon, Co-Founder and Executive Director, Access Now, USA
Seamus Tuohy, Director, Information Security, Human Rights Watch, USA

14.00 - 15.00 Panel
Lessons from the Trenches: Towards Robust Crisis Leadership
Cyber crisis leadership has become a competitive differentiator, demanding quick and stringent decision-making from senior leaders. How can organizations improve their crises preparedness and management?

Sudheesh Babu, General Manager & Head - Strategy and M & A, Cybersecurity & Risk Services, Wipro, India
Gabi Dreo Rodosek, Executive Director, Research Institute CODE, Universität der Bundeswehr München, Germany
Dmitry Samartsev, Chief Executive Officer, BI.ZONE, Russian Federation
Mark Swift, Chief Information Security Officer, Trafigura Group, Switzerland
Jennifer Schenker, Founder and Editor-in-Chief, The Innovator, France

15.30 - 16.15 Hub
In Data We Trust?
From machine learning to precision medicine, data is core to driving technological innovation. Yet, maintaining trust in the responsible use of data is a formidable challenge. What new governance models and technological approaches can help to enhance digital trust?

Bill Fryberger, Director - Information Security, Procter & Gamble, USA
Kai Hermsen, Global Coordinator for the Charter of Trust, Siemens, Germany

15.30 - 17.00 xChange

Can the Market Fix It?

Investors and insurers are increasingly taking investment or pricing decisions based on a company's security posture. In the ever-accelerating pace of technological advancement, what market incentives can effectively improve the cyber preparedness and resilience of organizations?

Laura Deaner, Global Chief Information Security Officer, S&P Global, USA
Einaras von Gravrock, Chief Executive Officer and Founder, CUJO AI, USA
Katheryn Rosen, Managing Director, Technology and Cybersecurity Policy and Partnerships, JPMorgan Chase & Co., USA
Haiyan Song, Senior Vice-President and General Manager, Security Markets, Splunk, USA
Jennifer Schenker, Founder and Editor-in-Chief, The Innovator, France

15.30 - 17.00 Workshop

Stepping Up Large-Scale Cyber Defence

Internet service providers are in the frontlines of reducing malicious traffic affecting millions of users daily - an entry point for low cost and high damage cybercrime. How can automated defensive measures and regulatory incentives enhance the resilience of networks and services against high-volume cybercrime?

Fabrice Clément, Chief Information Security Officer, Proximus, Belgium
Yasser N. Alswailem, Vice-President, Cyber Security, Saudi Telecom, Saudi Arabia
Marco Obiso, Head, Cybersecurity Division, International Telecommunication Union (ITU), Switzerland
Scott Stevens, Senior Vice President, Global Systems Engineering, Palo Alto Networks, USA
Kevin Brown, Vice President, Threat Intelligence & G.E.S Transformation, BT Security, BT, United Kingdom

15.30 - 17.00 Workshop

Cybersecurity and Digital Trust: Strengthening Global Architectures

Understanding the myriad of multilateral, government- and private sector-led cyber initiatives will help to address cybersecurity challenges concertedly and internationally. How might we create a shared narrative to address the fragmented global architecture?

Tim Maurer, Co-director of the Cyber Policy Initiative, Carnegie Endowment for International Peace, USA
Philip Reitinger, President and CEO, Global Cyber Alliance, USA
Heli Tiirmaa-Klaar, Ambassador at Large for Cyber Diplomacy, Ministry of Foreign Affairs of Estonia, Estonia
Knut Haanaes, Dean of the Global Leadership Institute, Member of the Executive Committee, World Economic Forum

16.15 - 17.00 Hub

The Promises and Perils of Zero-Trust Technologies

Zero-trust technologies promise to unlock the value of data without compromising its confidentiality. As zero-trust models are increasingly adopted, what do security practitioners need to watch out for?

Maria Vello, Chief Executive Officer, Cyber Defence Alliance, United Kingdom
Nadav Zafrir, Chief Executive Officer and Co-Founder, Team8, USA

17.15 - 18.00 Hub

Cryptocurrencies: Cutting through the Hype

Over 1.600 cryptocurrencies are on the market and recent hacks have shown they are not as safe and trustworthy as once hailed. With countries and companies increasingly adopting them, what is needed to understand the business impact and make cryptocurrencies more secure?

Christophe Nicolas, Senior Vice-President and Founder, Kudelski Security; Group Chief Information Officer, Kudelski Group, Switzerland
Bertrand Perez, Managing Director and Chief Operating Officer, Libra, Switzerland
Laurent Haug, Swiss Correspondent, Wired UK, United Kingdom

17.15 - 18.15 Roundtable

Driving Development: Cybersecurity and the Digital Dividend

To safeguard the benefits of digital transformation as a key enabler of socio-economic prosperity, cybersecurity capacity-building needs to be mainstreamed in international development efforts. How can this be achieved to ensure the sustainable and secure roll-out of digital technologies and services, particularly in emerging economies?

Chris Gibson, Executive Director, FIRST, USA
Ariel Nowersztern, Cyber Security Specialist, Inter-American Development Bank, USA
Ruth Shoham, Executive Director, Strategy and Capacity Building, Israel National Cyber Directorate, Israel
David Van Duren, Head Secretariat, GFCE, Netherlands
Brett Solomon, Co-Founder and Executive Director, Access Now, USA

Wednesday
13 November

Enhancing Global Cooperation for Trust and Security

Securing Future Digital Networks and Technology

Building Skills and Capabilities to Secure our Digital Future

09.00 - 09.45 Hub
Global Risks and Responses: The Cyber Community's View
The Global Risks Perception Survey is the source of the World Economic Forum risk data for its annual flagship Global Risks Report, harnessing the expertise of the organization's extensive network. How might the perception of global risks of the cybersecurity community differ from that of other respondents and how are the cyber risks going to influence global trends?

Heather King, Chief Operating Officer, Cyber Threat Alliance, USA
Thomas Kropp, Group Chief Information Technology (IT) Services Officer, Zurich Insurance Group, Switzerland

09.00 - 10.30 xChange
Getting the Board on Board: Improving Cybersecurity Governance
Effective cybersecurity governance is projected to protect more than $5 trillion in future revenue over the next five years. How do you get your company's board "on board" with cybersecurity?

Elly van den Heuvel, Secretary, Netherlands Cyber Security Council (CSR), Ministry of Security and Justice of the Netherlands
Rosa Kariger, Chief Information Security Officer, Iberdrola, Spain
David Thornewill von Essen, Global Chief Information Officer, IT GBS, CSI & Corporate Center, Deutsche Post DHL, Germany
Michael Siegel, Principal Research Scientist - Director of Cybersecurity at MIT Sloan, MIT - Sloan School of Management, USA
Steve Sparkes, Managing Director, Head of Cyber Security Technology, Bank of America, USA
Stefan Deutscher, Partner & Associate Director, Cybersecurity & IT Infrastructure, Boston Consulting Group, USA

09.00 - 10.30 Workshop
Getting Priorities Straight: Cybersecurity Challenges in Financial Services
Cybersecurity underpins confidence and trust in payment systems and financial services. In a period when international cooperation is under stress, how can leaders from the public and private sectors prioritize challenges and devise a global strategy for capacity building and cyber-resilience in financial services?

Jennifer Elliott, Deputy Division Chief, Financial Regulation and Supervision, International Monetary Fund (IMF), Switzerland
Tim Maurer, Co-director of the Cyber Policy Initiative, Carnegie Endowment for International Peace, USA
Nina Paine, Global Head, Cyber Partnerships and Government Strategy, Standard Chartered Bank, United Kingdom
Marcio Rodrigues Alves dos Santos, Head of IT Security Division, Central Bank of Brazil
Lutfey Siddiqi, Visiting Professor-in-Practice, London School of Economics and Political Science, United Kingdom; Young Global Leader

09.15 - 10.15 Panel
Securing Next-Generation Networks
5G-driven goods and services are forecasted to enable $12.3 trillion of global economic output by 2035, generating up to 22 million jobs. With the cyberattack surface slated to grow in tandem with these developments, how can trust and the readiness to protect the next generation of networks contain the inherent risks?

Gwenda Fong, Director, Strategy, Cyber Security Agency of Singapore (CSA)
Pär Gunnarsson, Vice-President and CSO, Group Security, Ericsson, Sweden
Ian Levy, Technical Director, GCHQ, United Kingdom
John Maddison, Chief Marketing Officer and Executive Vice President, Products, Fortinet, USA
Laurent Haug, Swiss Correspondent, Wired UK, United Kingdom

10.00 - 10.45 Hub
Hard-Wiring Gender Parity in Cybersecurity
Increasing numbers of women are engaging in cybersecurity in professional roles as data scientists, software developers and AI specialists. Yet, men still outnumber women in the sector by three to one. How can the cybersecurity workplace of the future be shaped by gender parity and equal prospects in seniority and salary?

Sol Echeverria, National Clusters Program Director, PROCOMER, Costa Rica
Jacky Fox, Managing Director, Accenture Security, Accenture, Ireland

10.45 - 11.45 Plenary
Cyber-Resilience in the Fourth Industrial Revolution: From Critical Infrastructures to Critical Systems
Strengthening cyber-resilience in critical government and business functions requires an ecosystem-wide approach to ensure that digitalization and connectivity yield their optimal benefits. How can new models of collaboration between governments and the private sector enhance cyber-resilience in the Fourth Industrial Revolution?

Khalid Al-Harbi, Chief Information Security Officer, Saudi Aramco, Saudi Arabia
Marc Henauer, Head, Reporting and Analysis Centre for Information Assurance, Melani, Switzerland
Mark Hughes, Senior Vice President and General Manager of Security, DXC Technology, USA
Reiko Kondo, Director, Office of the Director-General for Cybersecurity, Ministry of Internal Affairs and Communications of Japan, Japan
Thomas Kropp, Group Chief Information Technology (IT) Services Officer, Zurich Insurance Group, Switzerland
Henry Harrison, Chief Technology Officer, Garrison, United Kingdom

13.00 - 13.45 Hub

Adding Some Mint: Inducing Behaviour Change

In its day, adding mint flavouring to toothpaste resulted in behaviour change at scale along with new opportunities for marketing dental hygiene as a matter of beauty and health. What magic ingredient can trigger comparable sweeping improvement in user behaviour and practice in cybersecurity?

Nicolas Fischbach, Global Chief Technology Officer, Forcepoint, USA
Dan Yerushalmi, Chief Customer Officer, Check Point Software Technologies, Israel
Jennifer Schenker, Founder and Editor-in-Chief, The Innovator, France

13.00 - 14.30 xChange

Rethinking Supply Chain 4.0 Security

Managing third-party risks is becoming a significant challenge as supply chain attacks grow in frequency and sophistication, new vulnerabilities keep being discovered and everything-as-a service removes traditional security borders. How can industries rethink risk management in the age of supply chain 4.0?

Markus Braendle, Senior Vice-President, Head of Cyber Security, Airbus Defence and Space, Germany
Bob Xie, Director, Huawei Cyber Security Transparency Centre, Belgium
Stephen Boyer, Co-founder & CTO, BitSight, USA
James Goddard, Vice-President; Chief Information Security Officer, Kaiser Permanente, USA
Alexander N.M. Niejelow, Senior Vice-President, Cybersecurity Coordination and Advocacy, Mastercard, USA
Marc Henauer, Head, Reporting and Analysis Centre for Information Assurance, Melani, Switzerland

13.00 - 14.30 Workshop

Tackling the Capacity Gap: Accelerating Cybersecurity Ecosystems

More and more local ecosystem initiatives are seeking to tackle the shortfall of cybersecurity talent, estimated at nearly 3 million globally. How can multistakeholder partnerships elevate local best practices globally and spur innovation, economic and human capital development simultaneously?

Sandro Bucchianeri, Group Chief Security Officer, Absa Group, South Africa
Gabi Dreo Rodosek, Executive Director, Research Institute CODE, Universität der Bundeswehr München, Germany
Prerana Mehta, Chief of Ecosystem Development, AustCyber, Australia
David Van Duren, Head Secretariat, GFCE, Netherlands
Roni Zehavi, President, Global EPIC, Ireland
Marco Obiso, Head, Cybersecurity Division, International Telecommunication Union (ITU), Switzerland

13.15 - 14.15 Panel

Collateral: Shaping Cybersecurity through Non-Cyber Policies

Non-cyber policies - from trade and foreign investment to government procurement - are gradually influencing the security posture of corporations and countries alike. Similarly, corporate leadership must approach cybersecurity in relation to other strategic considerations such as finance, branding and innovation. What are the implications and impact of this interplay between cyber and non-cyber?

Jennifer Elliott, Deputy Division Chief, Financial Regulation and Supervision, International Monetary Fund (IMF), Switzerland
John Lynch, Chief, Computer Crime and Intellectual Property Section, Criminal Division, US Department of Justice, USA
Neal Pollard, Chief Information Security Officer, UBS, Switzerland
Vishal Salvi, Chief and Information Security Officer, Infosys, India
Seamus Tuohy, Director, Information Security, Human Rights Watch, USA
Lutfey Siddiqi, Visiting Professor-in-Practice, London School of Economics and Political Science, United Kingdom; Young Global Leader

14.00 - 14.45 Hub

What If Defeating Cybercriminals Can Be Trained?

What if cybersecurity trainings that bring together stakeholders across sectors and geographies can make cooperation the norm to defeat cybercriminals and decrease response time?

Craig Jones, Cybercrime Director, International Criminal Police Organization (INTERPOL), Singapore
Dmitry Samartsev, Chief Executive Officer, BI.ZONE, Russian Federation

14.45 - 15.30 Plenary

Closing Plenary: Enabling Leadership for a Secure Digital Future

Join the Closing Plenary for the key insights from the Annual Meeting on Cybersecurity to enable leadership for a secure digital future and develop concrete recommendations for global leaders.

Klaus Schwab, Founder and Executive Chairman, World Economic Forum
René Bonvanie, Executive Vice-President, Strategic Accounts, Palo Alto Networks, USA
David Koh, Chief Executive, Cyber Security Agency of Singapore (CSA), Singapore
Risto Siilasmaa, Chairman, F-Secure Corporation, Finland
Ana Maria Montero, Anchor, CNNMoney Switzerland, Switzerland

Acknowledgements

The Platform for Shaping the Future of Cybersecurity and Digital Trust would like to thank the following partners for their valuable support of the Annual Meeting on Cybersecurity

Founding Partners

Accenture
Fortinet
Palo Alto Networks
Salesforce
Saudi Aramco
Sberbank

Platform Partners

Absa Group
Aker
Amazon Web Services
Banco Santander
Bank of America
Boston Consulting Group
BT Group
Check Point
China Datang
Cisco
Cloudflare
Credit Suisse
Deloitte
Depository Trust & Clearing Corporation
Deutsche Post DHL
DXC Technology
Eisai
Equifax
EY
FTI Consulting
Generali
HCL Technologies
Hewlett Packard Enterprise
Infosys
Iron Mountain Information Management
Kudelski Group
Mahindra Group
Mastercard
Microsoft
PayPal
PwC
Saudi Information Technology Company
Saudi Telecom Company Group
State Grid Corporation of China
S&P Global
Total
UBS
Wipro
Zurich Insurance Group

Government and International Organizations

Europol
FIDO Alliance
Global Cyber Alliance (GCA)
International Telecommunications Union (ITU)
INTERPOL
Israel National Cyber Directorate (INCD)
Oman Information Technology Authority (ITA)
Organization of American States (OAS)
Republic of Korea National Information Resources Service (NIRS)
Saudi National Cybersecurity Authority
Swiss Reporting and Analysis Centre for Information Assurance (MELANI)
UK National Cyber Security Centre (NCSC)

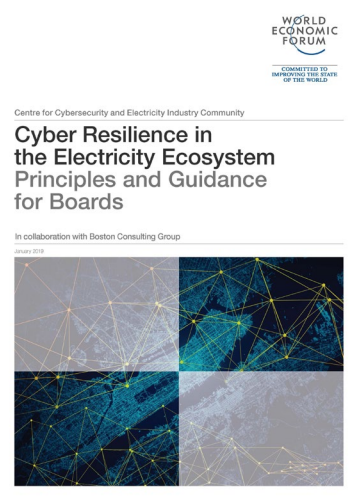
Read more

The Cybersecurity Guide for Leaders in Today's Digital World

Cyberattacks are one of the top 10 global risks of highest concern in the next decade, with an estimated price tag of $90 trillion if cybersecurity efforts do not keep pace with technological change. While there is abundant guidance in the cybersecurity community, the application of prescribed action continues to fall short of what is required to ensure effective defence against cyberattacks. The challenges created by accelerating technological innovation have reached new levels of complexity and scale – today responsibility for cybersecurity in organizations is no longer one Chief Security Officer's job, it involves everyone.

Incentivizing Responsible and Secure Innovation: Principles and Guidance for Investors

This report proposes an innovative focus on cybersecurity incentives for the investment community. Investors in innovation and technology-driven companies have a responsibility to ensure that cybersecurity is given priority in the early stages of product development. By ensuring cybersecurity from the outset – including features like security-by-design and security-by-default – investors can increase the likelihood of company success in the long term, promote more durable technology and improve overall cyber resilience. This report proposes principles for investors that will raise their internal cybersecurity awareness and offers a complete framework enabling investors to assess the cybersecurity preparedness of their target company



Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards

Cyber resilience is a challenge for all organisations, but, due to its vital role as a societal backbone, it is of particular importance for the electricity ecosystem. The power grid is an increasingly popular target for cyber threat actors: including hacktivists with the aim of causing civil unrest or state-sponsored groups performing espionage activities. Moreover, electricity organizations operate in an interconnected and interdependent environment where the consequences of a cyber attack on one can cascade to numerous others. Combatting this growing risk requires leaders to shift their thinking on cyber resilience.

Contributors

The Forum would like to thank the official writers of the Annual Meeting on Cybersecurity, **Dorit Sallis**, **Jonathan Walter** and **Edward Girardet**.

Editing and Production

Nina Vugman, Communications and Editorial Lead

Marco Aguilar, Marketing and Communications Lead

Photographer

Pascal Bitz

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