WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

World Economic Forum Centre for Cybersecurity

Annual Gathering of the Centre for Cybersecurity

Committed to securing our shared digital future

Geneva, Switzerland 26-27 November 2018

Contents

Foreword

Troels Oerting
Head, World Economic Forum Centre for Cybersecurity

The Centre for Cybersecurity's mission to shape the future of global cooperation on cybersecurity is more important than ever. Governments, businesses, academia, civil society and individuals of all ranks are recognizing the pressing need for public-private cooperation to meet the vital and accelerating security challenges in the realm of cyberspace. The geopolitical, technical, cultural and many other complexities challenging cybersecurity daily are of global magnitude. The World Economic Forum, its global network and platforms with emphasis on impartiality, neutrality and public-private cooperation, is an unparalleled convener for these shared efforts to understand the threats we face, shape global efforts to respond and build the necessary capacity and institutions to meet cyber challenges.

To succeed in shaping global cybersecurity, the Forum Centre for Cybersecurity is bringing together the foremost leaders and specialists on cybersecurity from business, government, international organizations and civil society. At the inaugural Annual Gathering of the Centre, more than 80 global CISOs from the world's leading companies, government ministers and high-level cyber officials from more than 20 countries, including the United States, People's Republic of China and the Russian Federation, worked together with us on the most pressing global cybersecurity issues.

We set out to establish the framework and priorities that will have significant and broad impact on improving cybersecurity globally. I am grateful for the frank and honest discussions, the hard work and recommendations that participants contributed to the work that lies before us. This is only the beginning, an ambitious start to work that we will build on throughout the year ahead and that will next be reviewed at the Forum's Annual Meeting 2019 in Davos, Switzerland, on 22-25 January.

At the Annual Gathering we discussed the challenges ahead and identified what we should prioritize together as key joint projects for delivery in 2019 and beyond. Consequently, this report reflects those discussions on the challenges. A forthcoming publication scheduled for January will focus on the solutions to the challenges and on the suggestions for joint projects aimed at their mitigation.

We look forward to partnering with you all to combine and multiply our forces to ensure that we build a powerful response to cyber-risks and threats and effectively defend global trust, innovation and security.

Thank you all for your valuable participation in the Annual Gathering, for your partnership and support of our objectives and efforts. I look forward to welcoming you to our next Annual Gathering on 29-30 October 2019 and to our fruitful collaboration in the meantime to improve the state of global cybersecurity.

Executive Summary

The objective of the first Annual Gathering of the Centre for Cybersecurity was to bring together leading high-level cyber specialists from business, government, international organizations, academia and civil society to address the most pressing cyber challenges in the world today.

The aim of the Centre is to facilitate global cyber security cooperation through three vectors:

- **Reduce** the attack surface – through efforts to identify, address and prevent vulnerabilities while raising the difficulty of conducting cyberattacks
- **Contain** current and future cyberattacks – through intensified cooperation and information sharing
- **Restrain** cybercriminals –by promoting deterrence and heightening the risks associated with participating in illegal cyber activities by means of reinforced collaboration between public and private partners on cybercrime investigation and law enforcement processes.

Frequently throughout the two-day discussions, Troels Oerting, Head of the Centre for Cybersecurity, and many participants from the public and private sectors affirmed that the World Economic Forum is in a unique position to facilitate global cybersecurity collaboration successfully. First, the World Economic Forum can harness its impartiality to bring together partners and decision-makers from all over the world, progressively yet rapidly developing the trust required to underpin global cooperation for impact. Second, the World Economic Forum has vast experience and acknowledged success in building public-private cooperation for nearly 50 years. Finally, the Forum and its partners can help to create a bridge between operational and commercial drivers, that can sometimes be in conflict in cyber-related discussions. Leveraging the Forum's unique accesses and global reach, the Centre can influence decision-making at the highest levels to help unlock previously intractable issues.

Oerting explained the three principle ways in which the Centre will build on the Forum's unique position to address cyber challenges:

1. **Understanding** the threat landscape and risks

   Discussions on top threats for awareness and action, the impact of disruptive technologies and potential future threats sought collective understanding of these issues to identify where the Centre for Cybersecurity's work could have the greatest impact. Sessions on sector-specific threats and challenges in the financial and aviation sectors explored shared risks from an industry perspective and the need for more targeted regulatory measures and environment.

2. **Shaping** global processes in the cybersecurity environment

   To identify which resources, relationships, policies and initiatives at a global level would make the most tangible improvements to security and trust in cyberspace,

> **For the World Economic Forum, the Centre for Cybersecurity has absolute priority. Cyberspace is the backbone of the Fourth Industrial Revolution. We must build trust into cyberspace to ensure the optimal functioning and benefits of this new technological transformation – and that requires the broadest possible multistakeholder collaboration.**
>
> **Klaus Schwab**
> Founder and Executive Chairman of the World Economic Forum

discussion focused on incentivizing secure and responsible innovation, working across the technology and investment communities. The focus extended to a large number of operational issues relating to cybercrime investigations and enhancing public-private cooperation in areas of cyber response.

3. **Building** the capacities required to enhance improve cybersecurity

   Seeking to build capacity and resilience in the cyber domain, issues on workforce needs, diversity and inclusivity-related challenges revealed areas the Centre can help to address for rapid improvement.

Across all the Annual Gathering workshops, the Centre sought to identify tangible outputs and areas of work to prioritize over the coming year. The message was clear – the support of all Centre partners and global cooperation efforts will be essential to the success of meeting the magnitude of global cybersecurity needs at the speed at which they are required.

It was also emphasized that all of the above initiatives would succeed only if the vehicles for improvement focused on the three main "influencers" of security: people, technology and processes.

The Centre has selected the following key directions for its work over the long term:

- **Analysing top threats and industry-specific risks** – to enhance prevention by raising awareness of these at senior levels and to initiate specific projects in response to any major gaps and on areas where the Centre's involvement can create the greatest impact

- **Promoting innovation and security** – exploring risk and opportunities in disruptive technologies and working with partners to leverage cutting-edge technologies to develop new platforms for cooperation

- **Guiding policy and governance** – promoting global initiatives and agreements to enhance collective trust and security in cyberspace by encouraging broader regulatory, due care and other alignment as well as harmonizing and incentivizing secure and responsible innovation

- **Enhancing operations** – promoting and facilitating required operational processes and cooperation between public and private partners, aiming to reduce cyberattacks and ensuring that responses across the community are more robust and effective

- **Reinforcing cyber resilience** – collectively enhancing and leveraging practices and tools to improve cyber posture and supporting the development of required resources and skills

As a global force multiplier for cybersecurity and cyber-resilience, the Forum's Centre for Cybersecurity is committed to working in a spirit of shared endeavour, inclusivity and diversity to shape and ensure secure and constructive cyber development and innovation globally.

We very much look forward to beginning our joint work together with those of you who want to form a "coalition of the willing" in order to make a real impact on cybersecurity. Our aims are to help protect responsible innovation and the development of the Internet's ability to make tomorrow better than today for all law-abiding citizens in our hyperconnected world; to make it possible to use and explore the Internet without being a target of crime.

Understanding the Threat Landscape

Digitalization is bringing unprecedented innovation, speed and convenience to the world. But as digital technologies advance in complexity and scale, the threat of cybercrime grows, as do the number and frequency of data breaches. They appear so often that the public is rapidly becoming accustomed to cyber-incident occurrence. “Complacency” is a dangerous development. In an interconnected world, cyberattacks against financial systems, energy infrastructure, healthcare operators and supply chains have the capacity to cause huge economic loss and widespread social instability. Understanding the range of cyberthreats and their implications is the first step to addressing the challenges of cybercrime.

Technological threats

The integration of automation, communications and networking in industrial environments is part of the **internet of things (IoT)**. Often, **information technology (IT)** and **operational technology systems (OT)** are managed separately within companies. Operational technology systems that were not designed for remote accessibility do not factor the risks of connectivity into their processes. Such systems may not be regularly updated. Alternatively, they may be updated without consulting operations. Access to personal and corporate data and sensor tampering to destroy data also present a security challenge. In all cases, the vulnerabilities of OT systems and the lack of coordination between the IT and OT divisions leave a company at risk of a cyberattack.

The use of IoT will exponentially increase in the next years: various forecasts suggests that more than 50 billion devices will be connected to the Internet by 2025 and most will operate without direct human interaction. This will magnify a new "front" in the attack vector landscape and also call for new tools to authorize and manage logic machine identity access.

Artificial intelligence (AI) takes human knowledge and trains a machine to use it better than people do. It is estimated that up to 90% of cyber practitioner jobs will be automated and AI can be empowered to strengthen cybersecurity operations. But if defensive tools can be automated so can offensive capabilities. Once a vulnerability is identified and malware is prepared to exploit it, it is easy to automate the exploitation of that vulnerability. As a result, an attack like Wannacry (2017) can be executed by three to five people with internet access. AI will also most likely lead to new types of crime and it must be anticipated that criminal orgnaizations and networks will start investing in "Adversarial AI" with the aim of optimizing and scaling attacks, exploring new attack vectors and manipulating legitimate AI tools to fraudulently change a result from corporate algorithms. Another threat from AI is the potential misuse of monitored and compiled information on human behaviour online, and also in the physical world through sensors and face-recognition tools. Likewise, other developments in this and similar areas could pose a threat to information integrity.

The rise of **blockchain technology** has created a whole new attack surface. Mostly the risks do not come from the blockchains, but the platforms and applications developed around them. There are three types: risks that are inherent to the technology, risks due to the intersection of this technology with others, and future risks such as quantum computing.

Blockchain is exposed to the traditional risks associated with any technology such as storage and management of public and private keys. There are endpoint vulnerabilities where back-end, off-chain systems can be hacked. Data manipulation before it is entered into the blockchain

system affects operations (“garbage in, garbage out”).

There are several dangers specific to blockchain technology: the 51% attack, bad code that may lead to exploitation of a flaw by cybercriminals, vulnerability to scams perpetrated by third parties, OP_RETURN, secure integration with other technologies or interoperability of blockchains, on-chain data that is immutable and may contain sensitive information, as well as vulnerabilities exposed by the DAO breach.

Despite the various security risks of distributed ledger technology, there is a preference for focusing on how the technology can be leveraged to enhance security of organizational operational processes. The first risk to be adressed should be the security implications of permissioned blockchains and quantum-resistant encryption.

Cloud-based threats and vulnerabilities will grow due to inadequate application of security standards to cloud computing.

Much of the responsibility for these incidents rests with cloud providers who often do not have the tools to detect abuses and prevent these from occuring. Data breaches due to weak authentication and identity management, lost data due to faulty infrastructure or malicious intrusions, and hijacked accounts are just some of the risks of cloud-based computing. But the saying that one can delegate work but not responsibility is also valid here. Companies outsourcing to cloud providers, which is a growing trend, need to ensure that their desired control regime is implemented by the individual cloud provider.

Supply chain management also constitutes an increasing threat to business, one that is frequently overlooked as a priority in the overall security strategy. Recently, hackers have been capitalizing on this and have accessed "target" companies through providers with significant access rights but insufficient control.

Generally, it was noted that horizontally many companies and other entities with huge digital assets share a number of cybersecurity challenges. There is also, however, a need for a more focused vertical probe into sectors that share similar threats and risks, such as aviation, shipping, healthcare, finance, smart cities, insurance, universities, among others.

There is a general increase in data security and online channel threats despite a strengthening of cybersecurity measures. Europol’s Internet Organized Crime Threat Assessment – IOCTA 2018 has identified a range of current and emerging trends across the range of disruptive technologies. Based on their findings, ransomware retains its dominance. Distributed Denial of Services (DDOS) plagues public and private organizations. Card-not-present fraud dominates payment fraud. Social engineering is still the engine of many cybercrimes. Darknet markets continue to facilitate illegal business and the production of CSEM.

Beyond technology

Identifying cyberthreats and implementing cybersecurity measures does not stop at technologies or actors. A lucid analysis of the threat landscape extends more broadly to company culture (processes, communications, governance), the substance of regulation, law enforcement and government policy, links between the public and private sectors, and relations between countries. These factors are integral to the cybersecurity ecosystem and must be understood in their totality as either heightening or mitigating cyber-risk, depending on the form they take.

The need to address basic cyber challenges through greater focus on cyber hygiene is another area of insufficient attention. The discussion concluded that focus on cyber hygiene is an absolute must and should be addressed as a priority, before more sophisticated attack vectors like APT.

Risks within the company

Within a company, IT-OT physical convergence can be a threat to cybersecurity. Information technology and operational technology are often two separate communities with their own management cultures, which leads to a lack of coordination and hampers unified standards for safety and reliability. Another issue pertains to legacy issues and obsolescence.

Do companies have a systematic process to transition from old to new systems that do not leave them vulnerable to attack?

A company that lacks well-implemented security best practices is more exposed to security breaches. For management to agree on cybersecurity measures requires first being able to quantify cyber risk and making a business case showing the value of the investment. At present it is difficult to monetize security measures and prove their value. This stands in the way of perceiving security as a competitive advantage rather than a cost.

A company is vulnerable if cybersecurity best practices are not built into its culture and reward system. Once the company has defined its approach to systemic cyber hygiene, is it effectively disseminated within the company? Ideally, cybersecurity is every employee's business and not just relegated to the IT department. The company should have a culture of information sharing on cyber-vulnerabilities and breaches without having to consult the legal department. There should be tabletop exercises that build muscle memory with continuous refresher trainings for management and employees. Incentive systems should be structured to reinforce cybersecurity best practices. This can be done by indexing a security metric to a quantitative score in performance evaluations.

Lines of reporting influence how effectively a company handles cybersecurity. Management may not recognize the importance of giving the CISO direct access to the top decision-makers. CISOs reporting to CEOs have more leverage and impact in sustaining overall cyber-hygiene and successfully handling cyber incidents. In the case of Maersk, the CEO handed control of the company to the CTIO during the crisis period, to give him all the tools needed to manage the incident.

Attention to the "Insider" threat is another area of paramount importance. Insider threats come in many shapes and forms, their vectors range from negligence and incompetence to malicious intention and action. The issues here are complicated and conceptually challenging, requiring the development of best practices for mitigation.

Beyond the company

Companies are embedded in a national and international cyber landscape that determines the level of cyber-risk and how effectively cyberthreats are controlled.

Investigating cybercrime

The boundless reach of cybercrime differs significantly from the contained space of traditional crime in the geographical space. The digital space has no borders and perpetrators can do a great deal of damage without physically entering a specific territory. Even locating the source of a crime can be difficult.

The nature of threat actors is changing. Modern cybercriminals are no longer just individual hackers but organized cybercrime groups with sophisticated business structures that are run like legitimate enterprises.

They have the resources to operate in a borderless playing field and perpetrate crimes that have a global impact. The challenge is to identify the actors behind the crimes and have adequate legal procedures to prosecute them.

Though it is generally accepted that information sharing and insight sharing would be beneficial to all parties, there are significant blocks to this undertaking. Views diverge on the subject of possible sharing products, depending on the organization's profile and interests (private-sector companies, national governments and lawmakers, Europol, Interpol). The international legal ecosystem is no longer fit for purpose and lacks an overarching legal framework for information exchange. There are also no checks on the accuracy and reliability of information. Until now, the law enforcement experience shows that sharing is complicated and slow, even with safeguards and control of information.

Adding to the risk landscape is the lack of dedicated law enforcement (LE) agencies with the necessary expertise to combat these groups. Today, the majority of cybercrime is not handled by the police, but by private-sector security companies that manage an enormous amount of data. Investigations can be hindered by the volume of information because of inadequate forensic tools and investigative skills. The biggest challenge is how to attract qualified people, particularly in the development world where problems are different. One size does not fit all, context-specific responses are needed.

Communication and coordination challenges

Cybercrime is a global phenomenon and cyber criminals have no nationality. Yet attempts to protect systems are still nationally-based. Cultural differences between public and private actors, and among nations add to the difficulty of communicating and developing effective tools to fight cybercrime. Technology companies find it hard to talk to policy-makers. Companies are often averse to sharing information because they fear that they will lose advantage over their competitors. Real-time information sharing between data protection authorities and cyber response entities is erratic. National and global cyber response entities lack systematic processes for exchanging information.

Lack of shared norms and trust

Two issues underlie these challenges. The first is the lack of collective norms. Stakeholders often have mismatched objectives and do not share a common understanding or set of norms concerning what they want to achieve. National actors have differing views of the world and varying solutions to problems. Generational divides, political and cultural systems also influence stakeholders' perception of scenario events and definition of solutions. This is reflected in the response to the question, "Who is supposed to lead the charge if things go really wrong?" Participants in Palo Alto argue that it will be the large firms. In Munich they see the solution in a citizen social movement. In Singapore, the government will be relied on to fix things.

Another major issue is the lack of trust among stakeholders, a far-reaching phenomenon that lies at the heart of the cybersecurity challenge. Working

together requires a high level of trust between individuals, private-sector companies and governments that may not exist in many parts of the world. How can we trust the government not to use the information we share with them against us? Do we risk increasing our rivals' competitive advantage by sharing information with them? Is it safe to share information with national authorities in countries where cyber breaches may be state-sponsored? These concerns can be very real constraints to extended global cooperation.

Cyberspace is the backbone of the Fourth Industrial Revolution – it must be trustworthy and secure if all the opportunities of that transformation are to be realized. Security flaws in digital technology are only one aspect of the challenge. The broader cybersecurity ecosystem within companies, between the public and the private sector, across government ministries and services, and within regions can either weaken or reinforce cyber-resilience. In the interest of a free and secure digital society, public authorities and the private sector must cooperate as widely as possible to build and foster swift and efficient information exchange and protection.


WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD


WORLD ECONOMIC FORUM

Shaping Global Processes

Shaping a more resilient cybersecurity environment

By 2022, over 60% of global GDP will be digitalized and global spending on security solutions will have exceeded US$ 120 billion. By 2025, 75 billion internet of things (IoT) devices will be digitally connected, vastly increasing the threat surface. Meanwhile, cyberattacks are accelerating in number and sophistication, affecting all parts of the economy, public sector and governance, targeting individuals through to critical infrastructure and big business. The spiralling vulnerability of our physical and virtual infrastructure to cyber attack is outpacing our efforts to keep it safe.

As digitalization speeds up, trust, cooperation and skills – the very things we need to fight cybercrime – are left behind. Conflicting dynamics and mismatches abound between the organizations that need to cooperate. Law enforcement agencies are not natural bedfellows with multinational corporations. Regulation is the enemy of openness. Lack of trust hampers information sharing. Speed of response, so vital for the commercial world, is at odds with the painstaking process of building a case for prosecution. Chasing criminals is important, but we also need to be out in front building resilience into tomorrow's systems.

Meanwhile, cyber attackers mock the international borders and bureaucracy that prevent more coordinated responses. They are nimble, swift and ruthless. Our response needs to be more than a match for them.

In the sessions that focused on shaping global processes, we aimed to identify which resources, relationships, policies and initiatives at a global level would make the most tangible improvements to security and trust in cyberspace. The focus extended to a large number of operational issues relating to cybercrime investigations and enhancing public-private cooperation in areas of cyber response.

Building a coordinated response to cybercrime

There was a powerful consensus around the urgent value of sharing timely information between different partners, along with the wider need to cooperate across sectors and borders. The private sector, governments and international organizations all need to cooperate. But within these broad groupings there are many different interests. These different agendas and ways of working lead to barriers, both real and imagined, that we must overcome to realize the full value of information sharing and cooperation in the fight against cybercrime.

A couple of recent case studies throw the issue into sharp relief, in particular the WannaCry ransomware attack and the attack on Danish shipping giant Maersk. Discussion of these well-known attacks highlighted the current lack of clarity around sharing of relevant information on threats, as well as information sharing between the public and private sectors after the incident. There was consensus that while information sharing and international cooperation are extremely valuable, they need to be more widespread.

Four major barriers to information sharing were identified:

- Borders
- Vested interests
- Regulation
- Trust

We will analyse each barrier in turn, consider possible solutions and necessary partners, and point to models around the world where these barriers are already being overcome.

Bots without borders

Like the *Terra Incognita* on ancient maps, where dragons and sea monsters once roamed, digital space is uncharted territory, borderless and virtually lawless. If we want to tackle the challenges of cybercrime, we need to change our mindset rapidly and completely from our current understanding of physical space to the digital space.

Cyberattacks are almost never direct – they generally affect more than one country. Unless we shine the light everywhere, we will only meet attackers on our own frontiers, by which time it's too late. Bots ignore borders and the only way to combat hostile malware is through international cooperation in collective prevention and defence. Yet measures to protect financial systems, for example, are still governed on a primarily national basis. Nation states still believe they control things they no longer control when it comes to cyber, such as maritime infrastructure. Borders prevent cyber and law enforcement agencies from thinking more globally. We will focus on the development of a global response to cybercrime that recognizes the collective risks to our shared infrastructure.

Vested interests and a possible Grand Bargain

The mismatch between government and regulators, working within a national border, and multinational corporations working across many borders, makes it hard for the two sides to talk to each other. Tech companies often struggle to communicate with policy-makers and government agencies. Expectations are currently very low – why should a private company waste time and effort going to law enforcement agencies when they get nothing in return? Cultural differences add to the difficulty. Finding a common language and purpose through a set of shared norms is a vital first step. But what do we want to achieve through our information sharing and cooperation?

Different people want different things. Law enforcement agencies are very focused on prosecuting suspects, so they need attributable information that can be used to build a case for trial. Businesses, on the other hand, are less interested in blame and more focused on recovering as quickly as possible. Every day of downtime that a multinational company suffers as a result of cybercrime costs millions. In the event of an attack, the private sector needs information in real-time, not some shiny report from a national computer emergency response team (CERT) 12 months later.

There are perhaps the makings of a "Grand Bargain" here – law enforcement agencies want as much information and data as possible from the private sector on cyber breaches so that they can build a case for prosecution with the required level of attribution. Meanwhile, the private sector wants to understand what is expected of it from law enforcement as well as receive information that can help – and this does not necessarily have to be sensitive intelligence –

ideally before a strike happens but most definitely very soon after it happens. This would allow CISOs to prepare for the worst, understand what is happening to them and craft a rapid recovery. Both sides have vested interests in sharing information, but for different reasons. Being transparent about the benefits of this trade and the principles that both sides will adhere to in the event of a cyber incident may just make it happen more swiftly and smoothly.

The Centre for Cybersecurity will work with public and private stakeholders over the coming months to develop just such a set of principles that could help each side better understand their respective roles in the event of an incident and will aim to facilitate multijurisdictional response. The Centre will also consider how to promote other initiatives, namely how to improve mutual understanding and cooperation between the public and private sectors.

Regulatory alignment

Regulations tend to destroy trust and are a major barrier to information sharing. One participant went as far as to say that the real risk to the global financial system comes from regulators. The plethora of recent cyberattacks has led governments around the world to react with knee-jerk regulation – well-intentioned no doubt, but the wrong response. Countries that develop new data protection and threat-led pen-testing regimes pose a real challenge for global companies operating in dozens of different jurisdictions. The multiplication of regulations only makes risks less transparent and data sharing far harder.

“Regulatory alignment” is the new battle cry. We need to create regulations based on principles, not prescription. When regulators get prescriptive they are simply drafting a “cookbook” for criminals. Regulations that are excessively detailed or technical look backwards, whereas regulations based on principles look to the future by providing flexibility and scope to react to the rapid pace of technological change. Partners in this process need to include regional and global regulators, cybersecurity agencies, banks and law firms.

Trust me – we’re on the same side

“How can we build the Fourth Industrial Revolution if we cannot trust cyberspace?” asks Klaus Schwab, Founder and Executive Chairman of the World Economic Forum. “For the Forum”, says Schwab, “the Centre for Cybersecurity has absolute priority”.

While much work is needed to build partnerships between and within public and private sectors, lack of trust remains probably the largest barrier to progress. Like the chicken and the egg, both trust and information sharing need to come first, but one can help the other.

Working together requires a level of trust between individuals, private-sector companies and governments that may not exist in many parts of the world, especially in emerging markets. How can we trust the government not to use the information we share with them against us? Companies need to be able to work with each other and with governments without fear that they’ll be blacklisted or that news of cyber breaches will be leaked to the media. Reputations that took decades to build can be shattered in days. Take aviation, for example, an industry that suffers disproportionately from any negative media impact. Despite being the safest way to travel, the public reacts instantly to any news of the slightest disruption and bad news quickly goes viral, hitting companies' bottom line as a result

Another concern is with B2B cooperation. Do we risk increasing our rivals’ competitive advantage by sharing information with them that they don’t already have? Participants in the gathering agreed that to succeed in improving cybersecurity, there cannot be competition. Actors in the cyber domain have a responsibility to include and inform others of risks and systemic threats.

But for this to happen, trust is crucial.

There are currently two main trusted ways of sharing information: 1. Parties that implicitly trust one another share information directly, and 2. Each party shares with a third party (mediator), so that each has only one interlocutor. Participants discussed that this second model could be replaced by trust-based technology, allowing all sensitive information to remain within the organization and maintaining control over what to share, with whom and when. This in itself, however, raises a range of cultural and legal challenges that would need to be addressed before such informaation exchange could take place. We will explore these issues further and work towards facilitating the development of a platform that could help to enable improved informaiton exchange.

What kinds of information should we share and who with?

Information, intelligence, analysis, insights, threat indicators – what do we need to share? For the most part, private-sector participants expressed that they are not interested in receiving sensitive intelligence, but are looking for information from public-sector agencies that they can combine with their own data to better inform assessment of cyber threat and improve response.

Insight differs from conventional intelligence or information in that it provides additional factual context and can be actionable. In the cyber context, it is often difficult for CISOs to measure when they are doing too little or too much – over- or under-reacting to information. This is where the value of insight comes into play.

Insights are not threat indicators and it is important to distinguish between the two. Insights include judgement about what to do with the information provided. The criterion for sharing could be – “I need to tell my CEO about this.” At this level, insights would be reported few and far between, perhaps 10 or 15 a year. The level at which insights

should be shared would need to find a sweet spot – few enough to be taken seriously, but regular enough to maintain momentum.

Insights could be used as valuable preventive tools but are currently confined within organizations. Such information could be enhanced by analysis from a carefully curated community of experts. Delegates to the gathering suggested that managing such an insight-sharing platform is an area where the Forum's Centre for Cybersecurity could really make a difference. The first step is to create a virtual circle of trust.

The Centre will work to consider how such a platform could operate across different sectors and needs. Key to this will be developing the necessary legal safeguards and reaching agreement on clear and transparent terms of reference for participation in any such platforms and on how information so obtained is used.

Existing models of cooperation in cybersecurity show the way ahead

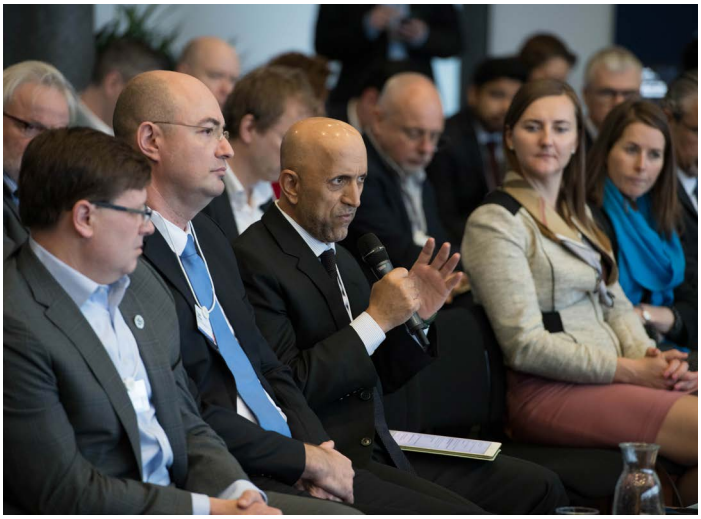
The Centre for Cybersecurity's ambition is to be a "do-tank" as well as a think tank, shaping prevention, protection and prosecution of cybercriminal activity and actors. A key strength of the Centre is as a global force multiplier for cyber resilience, enjoying the benefit of the Forum's power to convene the world's leading cyber experts and its direct access to the world's highest-level decision-makers at the Annual Meeting in Davos and through other Forum activities. The Centre aims to bring together public and private sectors, academia and international organizations.

Participants at the Centre gathering were, however, concerned about potential duplication of efforts with other platforms and the risk of information overload. They heard about a number of existing cyber cooperation and information sharing initiatives - for example, information sharing in the UAE financial sector through a cyber threat intelligence platform. Also mentioned was the Israeli Government development of "Cyber Net", a closed network that allows Israel's national CERT to connect with the cyber defence teams of public and private organizations across all sectors. Another example is Oman's work on hosting a regional cybersecurity centre for the 22 countries of the Arab League, following their consolidation of cyber initiatives.

The Centre has the opportunity to work with and learn from these existing models and from other countries such as Russia, where, despite accusations of cyberattacks originating from Russian sources, the government is seeking innovative solutions to address large-scale cybercrime affecting its businesses and citizens. The US meanwhile is seeking longer-term solutions by building more resilient networks across a range of ecosystems in the critical national infrastructure.

The Centre will also build on ongoing work being led by international organizations such as the European Commission, Europol and Interpol, also discussed at the Annual Gathering.

The one thing we can be sure of is that suspects never sleep – so whether we are into prevention, response or prosecution, we cannot afford to sleep either. We look forward to working with all our partners to align global policies and processes, build trust, and make it easier to deter and respond to cyber threats.



Building Cyber Capabilities

A global shortfall of 3.5 million cybersecurity jobs is expected by 2021. Against the backdrop of heightened cybersecurity threats and to create resilient societies, it is crucial for businesses and governments alike to close this gap, in both developed and emerging economies.

Developing greater diversity, gender balance and talent

Common themes mentioned relating to cybersecurity workforce development were the need to promote greater diversity, particularly gender, as well as attracting more talent. Currently, only 14% of the cybersecurity workforce in North America consists of women, while Europe ranks barely 7% and 5% in the Middle East. It is even less in Africa. The most difficult challenge is getting women to attain C-levels.

The gender question, however, is not a clearly defined one. As several participants pointed out, it needs to be dealt with carefully and sensitively. It should not be regarded simply as a male-female matter, but rather one of determining which issues need to be resolved and how best to respond.

The biggest challenge is marketing. How do we sell cybersecurity to potential talent pools, particularly to women? At the same time, some warn, companies should not indulge in making token appointments of women simply to fulfil quotas. What should be determined first are which measures will prove the most effective for integrating greater gender diversity, including responding to skills that are missing.

Much of this must happen at the executive level. Corporate leaders not only need to advocate for more women in the workforce but create more equitable working environments. The cybersecurity domain still harbours severe discriminatory attitudes. As some pointed out, certain companies feel the need to make a strong business case. They have to be convinced that it is worth their while to hire women. Nevertheless, executives need to make the effort to ensure that their organizations can help people (women or minorities) “grow”. This is where the Forum could make a significant difference by putting across the message more effectively to senior executives in the public and private sectors.

A new generation of cyberworkers in emerging economies

Given that Africa ranks as having the world’s third highest cybercrime rates, any form of cyber attack could severely threaten the livelihoods of small- or medium-sized businesses should they lose their online presence. It is therefore vital that populations in emerging economies become aware of the risks they are facing, but also of the possible solutions. They need to have access to affordable grassroots cyber expertise. As one participant put it, what economies like the African emerging market require is a new generation of cyber workers able to engage with schools and companies. But for this to happen, governments need to get involved by providing appropriate salaries and developing an encompassing approach that could also help alleviate unemployment.

In South Africa, for example, companies are developing new talent by investing in individuals. This is part of a deliberate effort to become more representative of society. The

problem is that, once trained - often at hight cost - people tend to leave for other companies offering better opportunities.

Yet, as another participant pointed out, expanding the cyber workforce does not mean seeking to elaborate or even impose a "one size fits all" approach. Training and awareness responses in North America and Europe, for example, may differ entirely from what is required in Africa. This is because many in Africa went straight to the smart phone phase missing out on computers and tablets. Many farmers and entrepreneurs rely on their Apps for access to livestock market prices or local business trends.

Conditions and remedies, including the creation of local or regional cyber job markets, may prove different in varying parts of the developing world. While North America, Europe and the Middle East may all be facing severe workforce shortages, countries such as Mexico, one of Latin America's most developed countries, have ample candidates.

Should cybersecurity capabilities be made more available cross-border?

Such geographical disparities raise the question as to whether cyber talent could – or should – be made available in a more cross-border manner. But which countries facing severe trained labour force shortages would be willing to issue visas? Clearly, this needs to be part of the discussion. The international community must decide how to promote or otherwise engage local cybersecurity capabilities designed to counter a "common" global enemy.

As a group, the Centre for Cybersecurtiy is in a key position to persuade policy-makers in both private and public sectors to embrace measures designed to produce skilled, new cyber professionals. Given that there is no shortage of public, corporate and academic leaders willing to pitch in, it is now imperative to mobilize adoption of more effective capacity-building measures and to take advantage of the global job pool.

Making cybersecurity attractive

As with other professions, such as the medical field, where doctors are trained in various medical disciplines, training according to various disciplines is applicable to the cybersecurity sector. Potential cyber workers need to understand that the possibilities are considerable as well as extremely varied. Particularly among young people we need to create a sense that cybersecurity is 'cool' and 'trendy'. The cyber industry is not just about dealing with hacking, but also providing the services that will help institutions operate more effectively as part of a broader "be prepared" approach. The public and private sectors in all their combinations need to contribute toward this talent development with more imaginative engagement. They also need to find ways of making training more available and to share the knowledge needed to achieve this.

Overall, this means creating a cyber skills network, a sort of new reference framework and global taxonomy based on international standards. In many parts of the world, such talent pools exist already. The problem is channelling them in the right direction. Hence, a skills network needs to emerge as one that is far better targeted, notably aimed also at people who may wish to change jobs or re-skill.

Such candidates could bring in far more relevant expertise, such as business experience, which might go hand-in-hand with their new cyber profession. Given that university graduates may have too much technical expertise and not enough social or entrepreneurial vision, individuals already endowed with mixed background capabilities could prove decisive in the event of a cyberattack and the impact it could have. An estimated 60% of companies tend not to survive a major hacking against their facilities. This suggests that appropriate cybersecurity precautions could have prevented their demise. At the same time, some may have been economically weak even before the incident.

Cyber-awareness: a corporate culture and a national effort

As emphasized by various participants at the Annual Gathering, the international community urgently needs to take effective action by expanding the cybersecruity workforce through a strategy of short, medium and long-term measures: Develop basic cyber awareness in schools to help companies embed an across-the-board cybersecurity culture from the C-level down.

Leadership at the executive level, for example, needs to take the time to clearly understand the risks and then ensure that everyone else in the company does the same. If discussions about cybersecurity are not constantly part of the daily conversation, these issues will not be perceived as being critical by people deeper within the organization.

One vital element of this overall framework is early education. Considered a starting point for a skills and public awareness pipeline, cyber professionals need to be present in schools. Most teachers have little idea about cybersecurity. Again, this is where the Forum could play a significant role, by persuading government leaders to support initiatives for enhancing cybersecurity visibility. But this needs to happen with private-sector involvement. Major funding could emerge through sponsorship, industrial expertise and other forms of support.

Students must be made aware of the need for cybersecurity, whether to guard against disinformation and hacking or about the importance of caution when positng anything online. Another purpose of these efforts is to reach out to girls, who are insufficiently included and supported in science and engineering. As one participant noted, many potential candidates are dispersed and cannot always find their way into a new career. "We must lower the walls to build human capital".


Topic: IN
RESPONSE KNOW-HOW
VS DATA
Mont Blanc C
Response


enisa
2 months interval


HOW CAN CAPACITY BE BUILT ACROSS CYBER RESPONSE
ENTITIES + LAW ENFORCEMENT TO ENSURE EFFECTIVE
INVESTIGATION + ENFORCEMENT CAN TAKE PLACE?
CHALLENGE
NEED
PARTNERS


WORLD ECONOMIC FORUM

The overall objective is to identify more efficient and expedient ways of creating a critical mass at every entry level for cybersecurity professionals. Select participants stressed the need to recognize that people want new opportunities and this is indeed what the cybersecurity sector can offer. Skills-related approaches with well-defined roles need to be elaborated, and fast.

Incorporating real-situation lessons learned into training

As part of overall training and awareness in the building-up of broader cybersecurity capabilities is the need to incorporate the experience, both positive and negative, of other companies and organizations. Credible information is considered imperative at all levels. This should be seen as a show of trust given that all companies and governments are concerned by the need for stepping up cybersecurity measures. Furthermore, it is something that companies, their partners and customers need to embrace. This includes small or medium-sized companies that cannot afford – or do not take on board – cybersecurity professionals. All need to have the sort of information that will enable them to incorporate proper online security, but also to know when a situation has become significant enough for them to seek outside help.

Many participants voiced a strong awareness of the need for feedback, learning the recovery experiences of others and how to capture and record learning experiences to incorporate them into recovery operations. As one participant noted, a cyber security specialist should not have to work on their own. They need to be able to rely on the support – and awareness – of all company employees. It is not simply a matter of training people with appropriate security capabilities but of ensuring that everyone knows what is at stake with a cyber breach.

A number of participants cited the Maersk case and the public manner with which it handled the June 2017 hacking of its cyber capabilities. This was considered a good example to follow as part of a collaborative sharing of information. These and other related incidents offer distinct "lessons learned" for what others can do if confronted with a similar situation. Valuable experience can not only help shape the training of cybersecurity professionals at all levels, but also encourage greater awareness about vulnerability, particularly among small companies which often tend to feel more immune from such threats.

Many, however, felt that remaining anonymous as part of the sharing process was preferential. Some suggested that the Centre should interview people anonymously, possibly for an annual "experience" report or video, and thus delve deeper into their hacking woes without revealing sensitive information. Such an approach could benefit everyone and dramatically help reinforce cybersecurity capabilities.

Acknowledgements

The World Economic Forum would like to acknowledge and thank the partners of the Centre for Cybersecurity for their support.

Founding Partners

Accenture
Fortinet
Salesforce
Sberbank

Partners

Check Point Software Technologies
Deloitte
Equifax
Zurich Insurance Group

The Forum also wishes to thank the writers of this report:

Edward Girardet
Dorit Probst
Jonathan Walter

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