OECD*publishing*

ROLES AND RESPONSIBILITIES OF ACTORS FOR DIGITAL SECURITY

OECD DIGITAL ECONOMY PAPERS

July 2019 **No. 286**

OECD
BETTER POLICIES FOR BETTER LIVES

This document contains a summary of the discussions held at the inaugural event of the OECD Global Forum on Digital Security for Prosperity, at the OECD headquarters in Paris, France on 13-14 December 2018. It was discussed by the OECD Working Party on Security and Privacy in the Digital Economy (SPDE) on 6-7 May 2019 prior to being declassified by the OECD Committee on Digital Economy Policy on 1-2 July 2019 and prepared for publication by the OECD Secretariat.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/SPDE(2019)4/FINAL

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Foreword

This report provides a summary of the Inaugural Event of the OECD Global Forum on Digital Security for Prosperity ("Global Forum") held on 13-14 December 2018 at the OECD Headquarters in Paris, France. It was drafted by Laurent Bernat and Andras Molnar, of the OECD Secretariat. Speakers reviewed the draft and provided input and corrections.

The event was sponsored by the French Ministry of European and Foreign Affairs, the French National Cybersecurity Agency (ANSSI), the Korean Ministry of Science and ICT and TÜV SÜD. It gathered 240 experts and 50 speakers from governments, businesses, civil society, the technical community and academia of 40 countries. They examined the roles and responsibilities of actors for digital security, with a focus on good practice for the governance of digital security risk in organisations, and how to improve digital security of technologies throughout their lifecycle.

The event organising team included Andras Molnar, Suguru Iwaya and Alice Weber, of the OECD Secretariat. Hugo Sicurani also carried out initial research to prepare the event.

The Global Forum was launched in 2018 to foster sharing of experiences and good practice on digital security risk and its management, mutual learning and convergence of views on core thematic issues related to digital security for economic and social prosperity. Its outputs feeds OECD policy discussions and can lead to the development of analytical work, principles and international policy recommendations.

More information about the Global Forum and its events is available at https://oe.cd/gfdsp.

Table of contents

Executive Summary

The Inaugural Event of the OECD Global Forum on Digital Security for Prosperity ("Global Forum") was held on 13-14 December 2018 at the OECD Headquarters in Paris, France. It gathered 240 experts and 50 speakers from governments, businesses, civil society, the technical community and academia. They examined the roles and responsibilities of actors for digital security with respect to the governance of digital security risk in organisations (Part I), and digital security of technologies throughout their lifecycle (Part II).

Discussions built upon the Responsibility Principle of the 2015 OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, which states that "all stakeholders should take responsibility for the management of digital security risk. They should act responsibly and be accountable, based on their roles, the context and their ability to act, for the management of digital security risk and for taking into account the potential impact of their decisions on others".

Part I – Digital Security Risk Governance in Organisations

Organisations need to change their culture to approach digital security as an investment rather than a cost centre

Experts discussed how to improve digital security governance to ensure that businesses fully realise the benefits from digital transformation.

Digital transformation, which turns data into a new energy and strategic asset, increases businesses' digital dependency and exposure to digital security risk. Organisations, including SMEs, need to change their culture to approach digital security as an investment rather than a cost centre. While there is no one-size-fits-all digital security governance, organisations need to integrate digital security risk management into all their important business decisions, in order to manage digital security risk together with digital opportunities.

Good practice for a collective digital security risk governance in organisations include:

- Educating and informing the board, which is often the weakest link, for example with a dedicated digital director, through crisis exercises, and with regular dashboards;
- Managing digital security risk holistically and from projects' inception, without distinguishing physical and digital aspects, and considering the entire supply chain;
- Establishing a collective and cross-disciplinary governance, with clear lines of communications between business and IT, to overcome the language gap between IT and C-levels, ensure that all business functions participate in risk assessment and mitigation, and inform leadership on the basis of credible risk scenarios and quantification;
- Ensuring that the Chief Information Security Officer (CISO) has sufficient technical knowledge and business expertise to be able to challenge the Chief Information Officer (CIO) and Chief Technology Officer (CTO), including in crisis situations.

The 2017 NotPetya incident[1] demonstrated that digital security is vital for companies relying on tangible assets. In case of major crises, businesses rely primarily on staff's energy and innovativeness to ensure resilience, business continuity and swift recovery. Such incidents show that businesses should test their preparedness plans and governance mechanisms.

Partnerships are essential to enhance trust between partners in the value chain

Incidents where companies have been hit through one of their value chain partners (e.g. Target Corporation) have increased awareness that digital security risk management should encompass the value chain. However, this is often difficult as value chains are complex ecosystems involving many actors. Panellists shared experience on how public policies can foster trust with respect to digital security between value chain partners.

Most initiatives to foster trust within value chains are based on partnerships and collaboration between stakeholders, including through Public Private Partnerships (PPP) and Information Sharing and Analysis Centres (ISACs). The difficulty to establish PPPs, their content and modes of organisation can significantly vary depending on the domestic culture. Information sharing, analysis and intelligence gathering in the financial sector are highly mature and a model for other sectors. However, many government agencies are still reluctant to engage actively, apart from a few countries.

Trust takes time, is based on people and requires mutual benefits

It takes time to build trust between partners. Establishing PPPs is easier when governments ensure that all parties can benefit from participating, and that representatives do not change often, can meet physically and have the appropriate expertise and authority to make changes.

Other challenges to collaboration and information sharing include *i)* lack of human resources, *ii)* lack of funding, *iii)* absence of legal basis for collaboration, *iv)* different expectations between industry and public sector, and *v)* difficulty to identify appropriate contact persons, often due to complexity of governments.

Policy initiatives to enhance trust in value chains include the following:

- Developing flexible standards with all stakeholders to provide a *lingua franca* to facilitate digital security risk management along the value chain. For example, the US NIST Framework provides common language that can be used across the value chain to improve security and help organisations and the government communicate their needs to value chain partners.
- Working with value chain actors to overcome information asymmetries between buyers and suppliers, for example by offering a platform based on a standardised questionnaire to simplify security self-assessments and third party certification. (INCD, Israel)
- Encouraging all partners within a sector to gather and achieve a shared understanding of risks and needs for security measures, and to develop trust, in particular as supply chains will become more flexible and non-linear with the integration of the digital and physical environments (METI, Japan).
- Fostering certification schemes to clarify to customers that assurance covers an entire value chain and to facilitate cross-border recognition. This can overcome the

complexity of value chains where nobody has a comprehensive understanding of the security of the entire ecosystem (DINL, Netherlands).

- Encouraging the use of certified services and products, educating investors, encouraging good practice for digital security governance, and incentivising SMEs to adopt basic security measures (METI, Japan).

Counter attacks should be banned

Experts also discussed how businesses could better defend themselves by using "active defence" or "hack back" measures to respond to a growing number of digital security attacks.

There was consensus that private actors should be banned from responding to digital security attacks by counter attacking. Such retaliations would create collateral damages to third parties, undermine human rights and feed geopolitical tensions. They would also raise significant legal concerns as they are likely to cross borders. International law is neutral with respect to private sector "hack back". However, a private actor cannot rely on a domestic right to self-defence in order to claim an international right to "hack back". Businesses carrying out "hack back" measures could violate both their domestic law and the law of the country where a damage is suffered. They could also expose the international responsibility of their State.

Several arguments, not shared by all panellists, were recalled in favour of businesses stepping out of their networks to protect themselves. Since they can sometimes be more efficient and better resourced than governments, businesses could increase the government's capacity to tackle malicious actors, in particular by gathering attribution information. However, businesses might not want to get involved in attribution, which is not only a technical matter but also a very political one.

Recognising that businesses should keep individuals, customers and users' trust as a key principle, potential contradictions were highlighted *i)* between the promotion of trust and the encouragement of a "hack back" industry that would develop and commercialise tools aiming at undermining digital security, and *ii)* between the overarching goal of protecting human rights and our collective security, and the possibility of collateral damages and crisis escalation.

Businesses' scope of action in response to attacks should be clarified

If businesses' priority in the course of an attack should be to take reasonable measures to mitigate damages, there are however examples of more "active" measures which can effectively increase users' security without affecting legitimate third parties, such as when Deutsche Telekom blocked the IP address of an infected server to which its customers' machines connected if they clicked in a phishing email.

Panellists agreed that international multi-stakeholder discussions, including at the OECD, could help clarify businesses' scope of action in the course of an attack, and examine the possible extension of private actors' role in digital security. For example, different types of security measures could be reviewed according to the possible risk they can carry, in order to determine which ones could be authorised, made illegal, or authorised only under certain circumstances, such as within a regulatory framework.

To enable open-minded and constructive debates, such discussions should avoid using terms that suggest counter attack, such as "hack back" and "active defence".

Part II – Making Digital Technologies More Secure Throughout Their Lifecycle

Digital security by design is a holistic approach that requires collaboration among all actors

Digital security by design is essential for consumer trust in IoT products, for consumer safety, and for ensuring the security and safety of critical activities.

Digital security by design is a holistic approach that involves the company's leadership and organisation, engineering mind-set, and supply chain. It is a business and technical challenge as companies have to manage trade-offs between products' security, performance and costs. It requires systematic implementation of rigorous standards with respect to product design, supply chain, and production environments.

Collaboration between all actors including partners and competitors is an important aspect of security by design. In the aviation sector, there is no competition on safety and security. ISACs, platforms such as the Charter of Trust and the Online Trust Alliance provide useful venues for dialogue and information exchange.

In the consumer IoT area, digital security by design should consider the entire product ecosystem (incl. smartphone app, cloud backend, etc.) rather than focusing only on the IoT devices.

A market failure prevents software security to improve

In some sectors, such as aeronautics, manufacturers have been ahead of regulation. They have transformed their processes and overall governance to take into account digital security as part of the broader safety commitment inherent to their sector.

However, in many other areas, a market failure prevents software security to improve. It results from *i)* an information asymmetry: customers don't have clear and neutral information about products' level of digital security and content; and *ii)* a negative externality: software producers are not accountable for consequences of incidents exploiting vulnerabilities in their products. In general, the software market does not reward quality, which remains low compared to other more traditional markets.

Businesses on the demand side are also sometimes creating conditions for security challenges. For example, they have had a tendency to use cheaper general purpose software for everything, and are reluctant to apply patches that could interrupt their production lines.

From a consumers' perspective, one may question whether functionalities enabled by connectivity are worth the security and safety risk they can create for customers and third parties. Security should be provided by design and by default because it is to the digital environment what safety is to the physical world. It should be non-negotiable and all products should comply with a safety-related baseline out of which consumers should not be able to contract, as it is the case with food and cars.

Products' design should provide for updatability, and patch availability should match the products' expected lifespan

Products' design should provide for updatability, in particular for physical products such as aircrafts and consumer IoT devices where safety is a priority. However, the complexity of value chains involving many actors with different roles, and limited availability of technical resources such as memory and cost can challenge "updatability by design".

A key challenge for customers is the misalignment between products' lifespan and patches' availability. Many vendors have an incentive to provide updates only for a short period of time in order to reduce cost and encourage consumers to buy new products. This accelerates obsolescence, can impact the environment and create social inequality by dividing consumers into those who can afford security by regularly buying new products and the others.

From a consumers' perspective:

- Patching should be easy. Security updates should be automatic, in particular when safety is involved. When it is not the case, all actors (e.g. manufacturers, integrators, sellers, software providers, and consumers) should be informed about their responsibility for the product to be updated,
- Patches should be available during the full products' expected lifespan. However, there should be a debate about how to define products expected lifespan.
- Consumers should be informed about possible limitations in the provision of updates.
- Technology companies have a responsibility to ensure that users understand what their products entail, including integrated generic components that might create systemic risks.

Apart from patching, IoT consumer devices raise additional security challenges such as data and password reset when the products' owner changes (e.g. smart home).

Voluntary approaches are no longer sufficient but regulation can have side-effects on innovation, access to ICTs and trade.

There is a debate regarding the extent to which voluntary approaches have improved products' digital security so far. In the physical world, voluntary approaches have proved less effective than regulation to ensure safety (e.g. fire extinguishers). Some governments are contemplating regulation to address the above mentioned market failure affecting software security, including by making participants in the value chain more accountable, and to reduce information asymmetries.

However, regulation can also have negative side-effects. Measures that increase products' prices can widen the digital divide, contradicting government's objectives to bring digital technologies to the largest number of people. Regulation can also inhibit innovation, for example in the case of IoT technologies which continue to rapidly evolve. It can also be interpreted as a technical barrier to international trade.

Labelling schemes can be useful, and certification needs to evolve to match the dynamics of digital security

Labelling and certification schemes can be useful, but the conditions for their success with respect to digital security are yet unknown:

- Labelling schemes can reduce information asymmetries and help vendors turn security into a competitive advantage and market differentiator. They can encourage the adoption of baseline security requirements and empower customers to decide how much risk they are willing to take when buying new products. However, it is unclear how many customers would be willing to pay for more security when less security would not significantly undermine their experience, such as when a device takes part in a botnet. Agile and flexible certification mechanisms, including continued verification and inspection, would however need to be established to support such labelling schemes.

- Mandatory certification can lead to "insecurity by compliance", as in Brazil where ISPs do not update some telecommunication equipment in order not to break mandatory certification requirements. Certification-related regulation needs to take economic aspects into account. It may not be economically feasible to certify everything on platforms that integrate many different parts. Risk-based approaches will be necessary to determine the components the certification of which can really bring value.

Test, Inspection and Certification (TIC) companies can enhance security knowledge and practice of vendors and integrators. However, TIC services need to evolve from periodic to continuous tests and inspections. They need to develop threat intelligence-based scenarios to best test products against the ever changing risk landscape.

Skills-related challenges are limiting the capacity of businesses to implement security by design. Students are not sufficiently trained to implement security by design and companies struggle to hire skilled digital security experts. Businesses have an incentive to help universities improve curricula in order to fill the digital security skills gap that they are currently facing.

More work is needed to inform policy efforts for digital security and to address issues at the intersection between digital security and product safety regulation

To improve digital security, policy makers should consider all policy tools, including regulation and self-regulation. They should in particular clarify what type of requirements are most cost-effective. For example: should producers have a security response team? A security contact point? A patching policy? Should products include secure code? Should their content be transparent?

To this end, policy makers could:

- Establish a multi-stakeholder dialogue, at domestic and international levels, to explore the types of requirements that would be most appropriate and cost-effective, including to address the market failure affecting digital security without generating negative side-effects.
- Avoid one-size-fits-all approaches in order to prevent any negative side effects of regulation. Different policy tools and incentives can be used in different risk scenarios (e.g. consumer market, critical infrastructure), depending on what customers are willing to pay, technologies, and other factors.
- Adopt a nuanced approach distinguishing levels of security depending on risks, markets, types of products, technologies, and use contexts. For example, digital security requirements are likely to vary between a nuclear power plant, a traffic system, a refrigerator and a doll.
- Take into account the complexity of the software ecosystem which includes many actors such as designers, integrators, distributors, sellers, etc. whose incentives with respect to patching – for example – may not necessarily be aligned.

Co-operation between digital security agencies and product safety regulators would help better understand the potential synergies, tensions and opportunities between digital security and product safety. The intersections between product safety regulation and digital security are yet to be explored by governments. This includes issues such as the extent to which a connected physical product can be certified according to safety regulation without preventing digital security updates at a later stage.

A market failure prevents responsible disclosure of vulnerabilities

Most software programmes have many vulnerabilities because the software market generally does not sufficiently reward quality. However, software is everywhere and supports all our economic and social activities, including critical ones. It is therefore essential to discover, disclose and fix software vulnerabilities for technical, economic, social and national security reasons. Panellists discussed how to encourage responsible and co-ordinated disclosure of vulnerabilities.

A market failure prevents the responsible disclosure of vulnerabilities. First, legal uncertainty discourages security researchers from disclosing vulnerabilities. Criminal law generally does not protect security researchers. Instead of rewarding those who disclose vulnerabilities, many software vendors sue them in order to protect their reputation. Second, the market for vulnerabilities rewards offense better than security. Some businesses and government agencies establish bug bounty programmes to reward researchers for reporting vulnerabilities. However, governments (i.e. national security and law enforcement agencies) and criminals can outbid vendors and distort prices.

Governments should adopt public policies to foster responsible and co-ordinated disclosure

Trusted intermediaries can encourage security researchers, by reducing legal uncertainty, streamlining disclosure processes, and facilitating reward. Computer Emergency Response Teams (CERTs) can act as co-ordinators between researchers and vendors. Some platforms can help researchers anonymously report bugs to CERTs while claiming credit for their work. Bug bounty platforms can act as trusted intermediaries between researchers and vendors, and facilitate their retribution.

Governments should adopt public policies to protect security researchers from legal proceedings, and encourage co-ordinated and responsible vulnerability disclosure. Software vulnerability disclosure remains a matter for experts and would deserve more attention from policy makers and other stakeholders. In Europe, only France and The Netherlands currently have adopted a policy framework, but ten other countries are developing one. Such policies can be based on several existing standards and guidelines. The EU Cybersecurity Act will give ENISA a mandate to assist EU members, on a voluntary basis, on how to develop a policy framework for vulnerability disclosure. It is also expected to legally bind manufacturers of newly certified products to provide contact information and information on accepted methods for receiving vulnerability information from end-users or researchers. Policies should pay particular attention to low cost embedded Internet of Things (IoT) devices that cannot be updated. In these cases, public disclosure of vulnerabilities could potentially increase safety risks for users, while keeping such vulnerabilities secret would reduce incentives for manufacturers to keep the devices secure.

Concluding session – Policy discussion

In the concluding session, representatives from governments, business, civil society and internet technical community discussed key findings from the event. They highlighted that:

- Digital security is an essential requirement for establishing trust in the digital economy and thus for driving innovation and prosperity. It should be approached with a view to achieving the broader beneficial objectives of digital transformation rather than as an end in itself.
- The digital environment is increasingly complex with different levels of interconnectedness across many layers of technologies, and many actors playing different roles at different stages of products' lifecycle. Since security is as good as the weakest link, it is essential to consider the entire products' lifecycle, value chain, and ecosystem to increase digital security in products and services.
- There is increased recognition that digital security risk is an inherently cross-border challenge with a global systemic dimension that requires an internationally co-ordinated response. However countries are not equally prepared to address digital security issues from the economic and social perspective. It is therefore necessary to coordinate and co-operate to level the playing field in terms of capacity. There is also a broader recognition that multistakeholder and multidisciplinary approaches are necessary at national and international levels to enhance digital security. However, breaking silos and establishing partnerships can be sometimes difficult.
- Self-regulatory approaches are no longer sufficient to make the digital ecosystem more secure, despite remaining useful in many cases. International co-operation to share good practice and identify a common way forward is all the more necessary as governments are increasingly considering regulatory mechanisms to address asymmetries, externalities and other market challenges.
- Digital security policy should promotes trust and respects fundamental values and human rights such as privacy protection, freedom of speech, free exchange of data across borders, and the promotion and protection of Internet freedom. While no countries should be left behind in the collective effort to enhance digital security, policies in this area should not be used as a pretext for practices that violate fundamental values.
- The OECD has played a key role over the last 25 years to foster co-operation (the "C" in OECD) and help governments and other stakeholders identify and share best practice for digital security policy. It should continue to lead and reach out to a wider audience to facilitate an international public-private dialogue towards a consensus on a set of principle-based minimal good practice with respect to key challenges, such as how to:
  - Strengthen the security of digital products and services throughout their lifecycle while involving all relevant actors in the value chain;
  - Encourage the responsible and co-ordinated disclosure of vulnerabilities and protect security researchers; and
  - Clarify the limits of what businesses can and cannot do to protect themselves in response to an attack.

Detailed Summary

Session 1 - Changing the Culture at the Top and Breaking Corporate Silos

Panellists: *Pascal Andrei*, Chief Security Officer, Airbus; *Sebastian Bregning*, Senior Risk Manager, A.P. Møller – Mærsk;*Andrea Bonime-Blanc*, CEO, GEC Risk Advisory; Dato' Dr. Haji Amirudin Bin Abdul Wahab, CEO, Cybersecurity Malaysia; *Hudi Zack*, Chief Executive Director (acting) Technology Unit, Israel National Cyber Directorate (INCD); *Philippe Cotelle*, Board Member, Federation of European Risk Management Associations (FERMA). **Moderator:** *Jeremy Millard*, Senior Consultant, Danish Technological Institute, Denmark

Panellists discussed how companies and other organisations can ensure that digital security risk is addressed as a business rather than only technical risk, how it can become a priority for CEOs, Boards and C-Suite, and how to integrate it within the broader enterprise risk management framework. Recognising that there is no one-size-fits-all governance model, they shared their experience and identified good practice.

Digital transformation requires a cultural change to integrate digital security risk management into business decision making and establish a collective risk governance

Businesses are approaching digital transformation at a different pace. For Airbus, digitalisation is a paradigm shift that requires a group-wide cultural change at all levels and functions of the organisation, and along the supply chain. This cultural change aims to transform data into a new energy and use it to feed competitiveness. It also affects how security is approached: security is now managed as an investment rather than a cost centre because the leadership understands that protecting the company is less expensive than not protecting it. Security is embedded in projects from inception and integrated into all important business decisions, especially when they affect the future of the company.

To facilitate this change across the company, a collective governance has been established. It includes a Digital Transformation Officer (DTO) who reports to the CEO, a Chief Security Officer reports to the DTO, and a general process whereby all business functions are represented in security discussions, and participate in risk assessment and risk mitigation meetings to set the priorities and define the way forward. A Data Governance Officer is also involved in providing a group-wide data management framework that includes security aspects as well.

In addition, recognising that everything is now interconnected and data-driven, all security matters have been integrated into a single holistic organisation and strategy. The company no longer distinguishes physical and digital aspects, and boundaries between different kinds of assets and divisions, including, for example, IT systems, operating technologies, industrial control systems, production, simulators, flight environments, crafts environments, etc. This approach includes stakeholders in the supply chain because their alignment with the strategy is critical.

Staff's creativity, energy and innovativeness are essential to ensure resilience in case of crises

Some companies are at an earlier stage in the process of understanding how to turn data into the new energy. The international container, shipping and logistics company A.P. Møller – Mærsk (Mærsk) operates in sectors where customer loyalty is limited and price is paramount. The company has huge fixed and tangible assets (vessels, containers, ports, employees, etc.), but today intangible assets like data are just as important to create new business opportunities. In 2017, the company was hit by the NotPetya malware which interrupted its global information system for ten days, leaving hundreds of vessels and tens of thousands of containers without information about their locations and destinations. The incident, which affected many other firms globally, underlined the vital importance of digital security for the functioning of a tangible assets company. The first lesson is the importance of staff's creativity, energy and innovativeness to ensure resilience, business continuity and swift recovery, for example by rapidly setting up new lines of communication when information systems are no longer operational. Despite the severity of the incident, no personal or property damage ensued, although losses of approximately USD 300 million were incurred.

Businesses should test their preparedness plans and governance mechanisms and invest more in digital security skills

The incident demonstrated the importance of testing preparedness plans at technical and organisational levels, including governance mechanisms. It underlined that while outsourcing IT is relatively easy, it is much more difficult to outsource digital security. In addition, the current digital security skills shortage appeared as a limitation to businesses' capacity to both manage crises and rapidly digitally transform.

The incident demonstrated the need to further integrate digital security risk management into business decision making. It also questioned whether to segregate the management of security risk to the company's core shipping activities from security risk to potential innovative data-driven services that it could develop to seize new business opportunities, as part of its digital transformation.

Boards are often the weakest link: they need to understand both digital opportunities and risk

Panellists put forward a number of additional good practice to improve digital security risk governance. Except in some very aware companies, boards are generally the weakest link: they do not pay attention to digital security until the business gets hurt. Boards often don't have directors who could ask the right questions both with respect to digital transformation and digital security risk. There is therefore increasing demand for boards to include a person qualified to be a director who has digital and digital security risk expertise. Boards can also be educated by external experts, or through customised crisis scenarios, and even through some board members talking to company experts in the field. With that knowledge, boards can ask management to provide quarterly or annually a dashboard of qualitative and quantitative information to understand business risks and take appropriate actions.

Businesses must overcome the language gap between C-levels and ICT professionals

Highest level (C-level) executives who prepare related strategy, planning and budget should have sufficient attention to digital security risk and receive appropriate information to make sound and educated decisions. However, there is generally a language gap between ICT professionals and C-level executives who often ignore the risk, do the absolute minimum, or try to act without a clear direction, hoping that it will work out. To bridge the language gap, businesses can gather an interdisciplinary team of people from different areas such as security, risk or crisis management, legal, IT, amongst other areas to work on crisis scenarios out of which a common language will emerge. A common language and tools to help leadership make informed decisions is also essential for SMEs.

Cross-disciplinary collaboration is key to inform leadership on the basis of credible risk scenarios and quantification

It is essential to establish a culture of openness and to encourage cross-disciplinary co-ordination, collaboration, communication, and sharing of information inside and outside the company.

An important lesson from the NotPetya incident faced by Maersk is that the Chief Information Security Officer (CISO) and Chief Information Officer (CIO) should be able to work together, share experience and be both involved at the very early stage of projects. The CISO needs to be separated from the CIO but should have the same amount of technical knowledge in addition to business expertise in order to be able to challenge him/her in crisis situation.

More generally, business, operations and support functions should be well coordinated and collaborate with each other. Simulation games such as Room#42 proposed by the Cybersecurity Competence Centre (C3) in Luxembourg can help increase awareness across different parts of the company. It is crucial to establish a clear line of communication between business managers and digital security experts, to develop risk scenarios that are credible both from a business and a technical perspective.

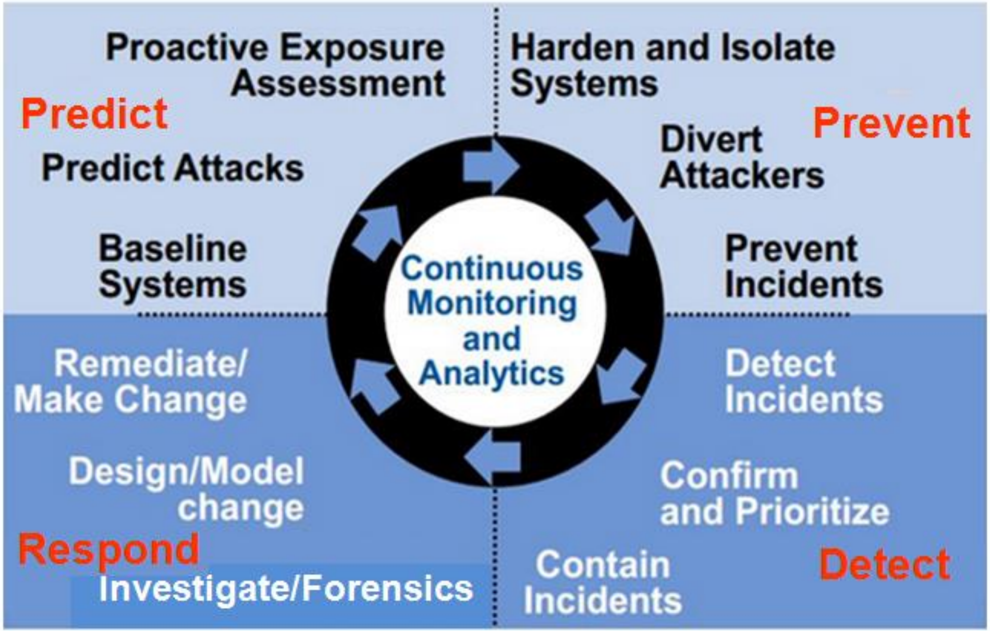
According to Philippe Cotelle, risk managers can help refine such scenarios and reach a consensus on the risk quantification as well as mitigation proposals, mixing security measures and process changes in order to reduce likelihood and/or possible impact. Risk managers can facilitate communications and express the risk to the company's leadership in business language in order to facilitate strategic decision making. This approach, proposed by the Federation of European Risk Management Associations (FERMA)[2], is effective for both large and small businesses. Overall, the more an organisation's digital security risk governance is mature, the more it is likely to convince insurers to provide an effective coverage.

Governments need to understand that opportunities and risks have to be managed together in order to develop effective public policies

Public policies can help break barriers of knowledge, technology, and budget to encourage businesses deal with digital security risk. However, governments are facing a complex challenge, with 50 billion devices expected to be interconnected by 2020, potentially unleashing immense economic opportunities, but also increasing digital security risk at a global scale.

In the highly digital driven Malaysian economy, security incidents already cost USD 12 billion per year. For the Malaysian cybersecurity agency (Cyber Security Malaysia), Governments need to understand that opportunities and risks have to be managed together, as digital security is not just a technical but rather an enterprise-wide business risk, which affects brand, finance, compliance and operational aspects. Malaysia adopted one of the first national cybersecurity strategies in 2006 that covered all critical sectors. The Malaysian government works with the private sector and the academia to promote a proactive, dynamic and integrated approach based on an adaptive security cycle that covers prediction, preventions, detection and response (Figure 1). It also promotes security by design through its Cybersecurity and IoT Guidelines 4.0. Digital security is also integrated in other policies, such as the recent National Policy on Industry 4.0.

- **Figure 1. Encouraging Adaptive Security for a more proactive, dynamic and integrated approach to business continuity**



Source: Dr. Amirudin, Cybersecurity Malaysia.

Governments can also offer tools to help businesses manage risk

Another way to help businesses manage digital security risk is to provide them with a tool to help them perform their risk assessment. According to the Israeli National Cyber Directorate (INCD), most organisations do not have the appropriate resources and skills to quantify in business terms the possible damages from incidents and benefits from reducing digital security risk. Few products are available to assist companies in every step of a risk assessment process: *i)* mapping all the critical assets; *ii)* defining with business managers, asset by asset, how much value would be at stake in case of a digital security incident; *iii)* building a realistic threat scenario; and *iv)* creating a risk map formulated in business terms that can then be used to analyse potential mitigation plans. INCD has built a solution to measure the readiness and risk management level of critical infrastructure operators, which it oversees, and offers a limited and easy-to-use version to all Israeli businesses. Businesses are invited to voluntarily subscribe to this cloud platform in order to get a risk analysis in near-real time.

Session 2 - How Can Value Chain Partners Trust Each Other's Digital Security Governance?

Panellists: *Henry Young*, Senior Technology Policy Advisor, Department of Commerce, United States; *Koji Ina*, Deputy Director, Ministry of Economy, Trade and Industry, Japan; *Evangelos Ouzounis*, Head of Unit, European Network and Information Security Agency, ENISA; *Yuval Segev*, Israel National Cyber Directorate (INCD); *Michiel Steltman*, Director, Digital Infrastructure Netherlands Foundation (DINL); *John Salomon*, Director, Financial Services Information Sharing and Analysis Center (FS-ISAC). **Moderator:** *Kathryn Jones*, Senior Policy Advisor, Department of Culture, Media, and Sports (DCMS), United Kingdom and Vice-Chair of the OECD Working Party on Security and Privacy in the Digital Economy (SPDE).

Digitalisation of value chains has brought many benefits but has also increased exposure to digital security risks. Panellists in this session discussed how to develop trust between partners along the value chain.

Digital security risk management should take the value chain into account

Too many organisations still believe that they don't need to care about what happens outside of their perimeter. Yet there are many examples that demonstrate the importance of the value chain for an organisation's digital security. For example, to hit Target Corporation in 2013, attackers first compromised a small HVAC company to break into Target's network and collect credit card data, causing a 250 million dollars loss and triggering the CEO's resignation. This incident shows that organisations' leaders and C-level executives should be able to understand, measure and communicate accurately about their supply chain digital security dependencies.

Partners need a lingua franca to facilitate digital security risk management along the value chain

Public policies can promote digital security and foster trust among partners along the value chain. However, governments need to recognise that there are limits to what they can achieve: compliance requirements can be quickly outdated and policies can disrupt effective mechanisms already in place. Therefore the United States Department of Commerce adopted a flexible policy approach based on the promotion of the NIST "Cybersecurity Framework" which is used by approximately 50 percent of critical infrastructure operators in the United States at the time of writing. (National Institute of Standards and Technology, 2018[1]) Developed through collaboration between government, industry and academia ("designed for industry by industry"), the Framework is a living document. It provides a common and standardised language that can be used throughout an organisation and across the value chain, to improve security and facilitate sharing of needs and requirements. It is adaptable to different technologies, sectors, risk appetite, and operational environments. It is also flexible and can be used by small businesses and government agencies in addition to critical infrastructure operators. It includes *i)* a Core, which provides guidelines, standards and practices on the five functions of digital security (identify, detect, protect, respond and recover) and enables IT staff to communicate with the company's leadership and other functions; *ii)* Profiles that help organisations and the government communicate their needs to value chain partners and describe how an organisation can adapt the Framework with controls tailored to statutory, regulatory and to its own requirements; and *iii)* Tiers which measure the degree to which an organisation's digital security risk management addresses the characteristics defined in the framework.

Governments can work with value chain partners to overcome information asymmetries between buyers and suppliers

According to the Israeli National Cyber Directorate (INCD), information asymmetries are causing a market failure with respect to digital security in the supply chain. Customers face Akerlof's so-called "lemons market" challenge: they do not have enough information to assess products and services' quality and therefore pay a moderate price for them. To help overcome such information asymmetries, the INCD first gathered all stakeholders to better understand the market failure, including suppliers, customers, vendors, certification bodies, auditors, etc. They identified that, in lack of a uniform language, most customers work alone to manage suppliers' assessment processes, don't have enough resources, and cannot easily verify suppliers' statements. To help buyers assess suppliers, the INCD developed *i)* a standard to provide market players with a common language, *ii)* a free vendor-risk management (VRM) platform that buyers can ask suppliers to use for self-assessment, and *iii)* a trust mechanism whereby the platform can also be used by certified auditors to assess suppliers. The implementation of this voluntary programme is ongoing in Israel at the time of writing and raises several challenges, such as the need for support mechanisms to assist suppliers who do not deal with security on a daily basis, or the need for sector-specific customisation to the general self-assessment questionnaire. If successful, the questionnaire and the platform currently dedicated to the Israeli market would need to be internationalised.

A multistakeholder effort can help address the increased complexity in the supply chain resulting from the integration of the digital and physical environments

The Japanese government vision for the future is a next generation smart social infrastructure called "Society 5.0", in which the interconnection of a wide variety of disparate industrial data increases the integration of the digital and physical environments to create social value. (Japanese Ministry of Economy, Trade and Industry, 2018[2]) According to this vision, the supply chain would become more flexible and non-linear and the deeper integration and linkages between the physical and digital environments are likely to increase the severity of potential digital security attacks.

To deal with this more complex supply chain, the Ministry of Economy, Trade and Industry's (METI) developed a "Cyber/Physical Security" (CPS) Framework divided into three layers. The first layer focuses on the trustworthiness of organisations (e.g. contracts, signature, certificates). The second layer addresses trust in the interface between the digital and physical space, such as the availability and integrity of the transformation of sensor measurements into data. The third layer focuses on trust in data, e.g. by examining the security of system architecture, protocols, and digital signatures. To implement the framework, METI engaged in a multi-stakeholder effort to develop sector-specific guidelines in order to assess risks and identify security measures. This process helped achieve a common understanding of the risks and provided a basis to develop trust between partners in specific sectors. For example, the guidelines for the building sector was co-developed with building owners, construction companies, design offices, building system operators (e.g. Building Management Systems, HVAC, Video monitoring, etc.), municipalities, amongst others.

Partnerships to build comprehensive certification schemes covering all actors in a value chain can foster trust and enable cross-border recognition

The internet infrastructure ecosystem involves a particularly complex value chain. In the Netherlands, the ecosystem that developed over 25 years around large internet exchanges and data centres represents 9% of the GPD and is one of the fastest growing sector in the country. This industry does not consists in siloes but is akin to the road and rail sectors, bringing together different layers of infrastructure, with various actors playing their part and using it: software, services, network infrastructure, data centre, payment gateways, etc. Each layer has its own specificities and security challenges within the digital value chain. It is however difficult for customers and partners to have an overarching understanding of the security of the ecosystem and its various components. To address that problem, the Digital Infrastructure Netherlands Foundation (DINL) developed the “Partnering Trust” initiative. This certification scheme enables customers to see that assurance covers the entire value chain at a particular risk level, for example to facilitate use for different types of data according to their sensitivity. “Partnering trust” is based on re-usable risk-based security and certification schemes addressing all components throughout the whole value chain. It enables international recognition without adding audit pressure to participants. DINL is currently at an advanced stage of the project covering the whole value chain. Many Information Sharing and Analysis Centres (ISACs) are connected to the project, and there is an agreement with seven EU member States while others have agreed to mutually recognise schemes that match these requirements.

Encouraging the adoption of good risk management practice can increase trust in value chains

Another way to promote trust among partners in the value chain is to encourage companies to adopt better digital security risk management governance. In Japan, METI *i)* introduced digital security in the “Practical Guidelines for Corporate Governance Systems” that businesses have to implement according to corporate governance regulation, *ii)* added digital security as a criteria for board activity evaluation by third parties (e.g. auditors), *iii)* educates investors about digital security risks, *iv)* cooperates closely with businesses to gather and share good management practices, *v)* created a digital security visualisation tool; *vi)* incentivises SMEs to adopt basic security measures, i.e. SMEs which pass a certification test receive “Blue Stars” which can be used to obtain subsidies for digital innovation.

METI also supports trust in the value chain by encouraging the use of certified services and products. As of October 2018, 79 services had been certified against the Standards for Information Security Services which covers information security auditing, vulnerability assessment, digital forensic monitoring and security monitoring services. METI is also implementing a “Practical Cybersecurity Evaluation and Verification Platform” to evaluate the effectiveness of digital security products, including through penetration tests by ethical hackers.

Partnerships are essential to foster trust within value chains, and governments can help establish PPP and ISACs

Partnerships are essential to help foster trust among partners in value chains and governments can play a key role to help establish them, in particular to enhance critical infrastructure protection. The EU Network and Information Security (NIS) Directive requires governments to adopt national strategies that address co-operation between private and public sectors. (EU, 2016[3]) ENISA’s experience shows that, depending on the national culture, such co-operation can be difficult. It can also vary from workshops and conferences to small and focused meetings of trusted individuals gathering to share information on a regular basis, including on detailed operational matters.

Public Private Partnerships (PPP) and ISACs are the two main vehicles for public-private collaboration. PPPs often aim to share knowledge, experience and good practice, increase trust between public-public, private-private and public-private sectors, achieve resilience in the digital ecosystem, get direct and credible contacts with other organisations. They help governments better understand the industry, create synergies between private sector initiatives and access private sector resources. They also help private sector access public funds, influence national legislation and mandatory standards, and access to public sector knowledge and confidential information.

ISACs are generally sector-based (e.g. energy, transports or aviation) and bring private actors together to share specific and focused information through regular meetings and working groups amongst other options. Members have a common understanding and they know and trust each other. ISACs in Europe tend to provide less analysis than in the United States. They facilitate cost saving, networking, access to knowledge and experience as well as the possibility to be part of a “peer pressure” group. For governments, they help assess the sector’s security level and can provide a single sector-wide point of co-ordination.

Another possibility to facilitate public-private cooperation is to build a dialogue around themes rather than sectors, such as, for instance, in Germany, where businesses have joined a platform to exchange information on CIIP matters.

Active information sharing on risks, good practices and mitigation strategies can help businesses to work more closely

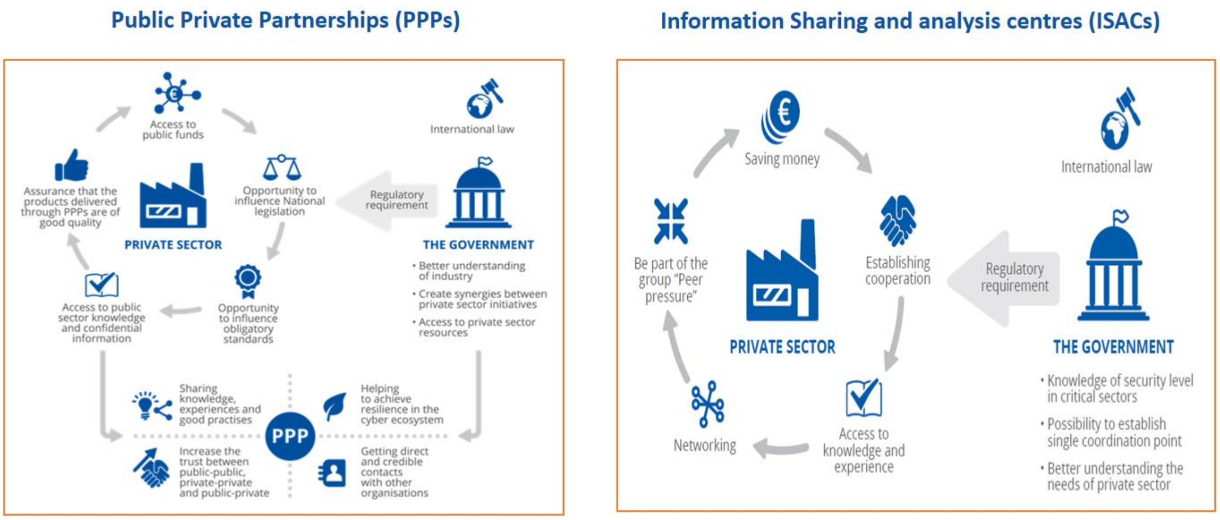
The financial sector is extremely interconnected and exposed to numerous value chain issues, including with respect to suppliers, vendors, retailers, points of sale terminals, payment networks, etc. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is one of largest ISAC and a good example to other industries and sectors. It facilitates active information sharing on risks, good practices and mitigation strategies between all actors within the sector. It is a large international non-profit with seven thousand member organisations. Although initially created in the US, the organisation is global and has a strong European footprint, paying special attention to European financial sector requirements and having a strong connection to European regulators, law enforcement agencies and other sharing initiatives. Discussions related to the value chain include the promotion of security by design (cf. session 4) within and beyond the sector, i.e. where payment solutions are used.

Governments’ strategies praise information sharing, but only a few governments encourage and actively participate in it in practice, such as the Israel, the Netherlands, Singapore, and United States, along with Europol, which take part in training and sector-wide exercises. While information sharing, analysis and intelligence gathering in the financial sector are highly mature, many government agencies, such as law enforcement bodies, are still reluctant to engage actively with FS-ISAC. Furthermore, public sector bodies are often complex entities to navigate through for stakeholders and one possible avenue to facilitate public-private co-operation would be to provide clear points of contacts within governments with whom private sector and ISACs can engage.

Key challenges to collaboration include trust, human resources, funding, legal frameworks and misalignment of expectations

The establishment of sustainable trust is a key challenge to collaboration. To foster trust, governments should let private sector lead or co-lead co-operation initiatives and ensure that all parties can benefit from participating. Governments and partners need to recognise that it takes time to establish trust. Trust is based on people and is therefore easier to maintain when organisations' representatives have the appropriate expertise and authority to make changes, don't change often and can meet physically. Trust also tends to decline according to the size of the groups where discussions are taking place, although large groups meetings can facilitate exchanges through side meetings. Other challenges to collaboration and information sharing include *i)* lack of human resources, *ii)* lack of funding, *iii)* absence of legal basis for collaboration, and *iv)* different expectations between industry and public sector.

Figure 2. Collaboration mechanisms


Public Private Partnerships (PPPs)
Access to public funds
International law
Assurance that the products delivered through PPPs are of good quality
Opportunity to influence National legislation
Regulatory requirement
PRIVATE SECTOR
THE GOVERNMENT
• Better understanding of industry
• Create synergies between private sector initiatives
• Access to private sector resources
Access to public sector knowledge and confidential information
Opportunity to influence obligatory standards
Sharing knowledge, experiences and good practises
Helping to achieve resilience in the cyber ecosystem
PPP
Increase the trust between public-public, private-private and public-private
Getting direct and credible contacts with other organisations
Information Sharing and analysis centres (ISACs)
Saving money
International law
Be part of the group "Peer pressure"
Establishing cooperation
Regulatory requirement
PRIVATE SECTOR
THE GOVERNMENT
• Knowledge of security level in critical sectors
• Possibility to establish single coordination point
• Better understanding the needs of private sector
Networking
Access to knowledge and experience

Source: Evangelos Ouzounis – ENISA. See slides at https://oe.cd/gfdsp

Session 3 – "Active defence'': how far can businesses go in proactive security?

Panellists: *Axel Petri*, Senior Vice President Group Security Governance, Deutsche Telekom; *Stewart Baker*, Partner, Steptoe & Johnson; *Yves Verhoeven*, Director for Strategy, National Cybersecurity Agency (ANSSI), France; *Théodore Christakis*, Professor of International Law, University Grenoble-Alpes, France; *Leandro Ucciferri*, Asociación por los Derechos Civiles, Argentina. **Moderator:** *András Hlács*, Vice-Chair of the OECD Committee on Digital Economy Policy.

As businesses face an increasing number of digital security attacks, there are debates on whether they would be able to better defend themselves by using "active defence" measures, also known as "hack back", in response to attacks. Panellists discussed the pros and cons of this idea from the perspectives of government, business, and civil society, as well as from a legal point of view. They focused only on private sector "hack back" or "active defence". They built upon a first round of debates at the 13th Internet Governance Forum (IGF) meeting in Paris on 12 November 2018.[3]

If they mean retaliation, "hack-back" and "active defence" should be banned

In the context of the 2018 *Paris Call for Trust and Security in Cyberspace* ("Paris Call"), "hack back" means responding or retaliating to a digital security attack by a digital security attack. (Ministère de l'Europe et des Affaires Etrangères, 2018[4]) "Hack back" is a practice that States should prevent private sector actors from adopting for their own purposes or those of other non-State actors. All panellists agreed that, regardless of legal considerations (discussed below), allowing private sector to carry out such retaliations would increase the overall level of risk. In particular in light of the specificities of the digital environment, where it is extremely delicate to accurately identify an attacker (attribution challenge) and to prevent collateral damages, even for governments.

Retaliating by breaching the availability, confidentiality or integrity of an information system would contradict the very objective of digital security and could affect third parties, including businesses, individuals and even governments, and potentially undermine human rights. Retaliations could also potentially feed geopolitical tensions: since attackers most generally operate through infected information systems located in third countries, those third countries' governments could interpret counter attacks launched against machines in their jurisdictions as plain attacks rather than defensive measures, and escalate, adding chaos to chaos.

Current terminologies are misleading

Panellists also agreed that "hack-back", "active defence" and similar terms were imprecise and misleading. They carry inappropriate connotations and fail to reflect the complexity of an issue that extends beyond the idea of retaliation to the possible extension of the role of private sector in digital security.

Further constructive international discussions would greatly benefit from avoiding these terminologies. In lack of a better term, "hack back" and "active defence" were used interchangeably during the discussions, as they are in this section.

There are several arguments in favour of businesses stepping out of their networks to protect themselves

A number of arguments in favour of allowing businesses to take security measures beyond their own networks can be identified. First, the current division of labour between businesses and governments is based on the assumption that the respective roles of police and businesses offline should be the same online. However, many of the advantages of the police in the offline world do not exist online, such as the police's capacity to patrol areas where crime can be committed. Instead, this patrolling function is already carried out by businesses monitoring their networks. Enabling businesses to have more security activities beyond their networks, including in a regulated or licensed manner, could increase the level of security for all.

Furthermore, governments lack resources, including skilled personnel, and it is unlikely that resources will increase sufficiently to effectively protect the private sector from digital security attacks. In contrast, private sector is already spending significantly more than the government on digital security, and therefore “active defence” could be viewed as a means to compensate government resources’ limitations.

In some cases, the private sector can be more efficient and react faster to tackle malicious attacks against its own networks compared to the government. If private sector could use its sophisticated digital security technologies and skills in favour of “active defence”, it could significantly increase the government’s capacity to tackle malicious actors. In particular, private sector could help gather attribution information.

However, the priority of businesses should be to strengthen digital trust

However, digital security is a key foundation for trust in digital transformation and therefore discussions on “hack back” should place individuals, customers and users’ trust at their core. From a civil society perspective, there are contradictions *i)* between the promotion of trust and the encouragement of a “hack back” industry that would develop and commercialise tools aiming at undermining digital security, and *ii)* between the overarching goal of protecting human rights and our collective security, and the possibility of collateral damages. The opportunity and potential consequences for private sector to get involved in the resolution of the attribution challenge was also questioned, considering that it is as much a political than technical matter.

It was questioned whether businesses’ digital security priorities were to “hack back” or rather focus on prevention and resilience measures such as patching or embedding digital security by design in their hardware, software, and digital services (cf. session 4 and 5). For example, the timely provision of software updates, and the promotion of digital security certification as included in the upcoming European Cybersecurity Act, or good practice reflected in the US Cybersecurity Framework were viewed as more important priorities than “active defence”.

Further international work is needed on which measures private sector could be allowed to take

Panellists agreed that businesses’ priority in the course of an attack should be to take reasonable measures to mitigate damages and that multi-stakeholder international discussions about the scope of such "reasonable measures” would be useful. Such discussions should be open-minded and not exclude any option *a priori*, including the idea that businesses could play a larger role within the broader continuum of digital security. They could aim at identifying measures *i)* could be authorised because they carry very limited risk (“white zone”), *ii)* should be illegal because they are associated to a level of risk that cannot be tolerated (“black zone”), *iii)* could be authorised under certain circumstances, within a regulatory framework, and perhaps only for some private sector actors (“grey zone”).

The example of how Deutsche Telekom managed the Emotet phishing campaign in 2018 illustrates which types of “active” measures private sector could be allowed to take to increase digital security without creating negative consequences. The company blocked the IP address of an infected server to which its customers’ machines connected if they clicked in a phishing email (Emotet phishing campaign). This initiative protected its customers, was proportionate, and did not create damages to third parties. In addition to such measures, It was noted that businesses can join forces with governments by sharing information and leveraging artificial intelligence to gain advantages over attackers. Deutsche Telekom is working with the Ben Gurion University in Israel to further innovate in this area, while respecting personal data protection regulations.

"Active defence" raises serious legal concerns

One should carefully understand the potential consequences of legalising active defence measures. For example, what would seem as an innocuous small legal step could open the door for larger rights in the longer term, that might lead to undesirable consequences (Pandora's box). More generally, From a legal perspective, international law is neutral with respect to "hack back" by private sector: it does not create any right to "hack back" or "active defence" but it does not prohibit it. Nevertheless, the Budapest Convention requires governments to criminalise any infringement of the integrity of computer systems.[4] The only soft law instrument addressing this issue, the Paris Call, encourages governments to prohibit "hack back". Furthermore, as of now, the theory of international law affirms that protective functions must be assured by States. Private actors cannot use theories designed to be used by States, such as theories of counter-measures, self-defence, or human rights to take "offensive" or "active defence" measures.

A private actor cannot rely on a domestic right to self-defence in order to claim an international right to "hack back": the right to do something under a domestic legal framework does not provide an international right to do it across borders. More generally, one could argue that "active defence" violates the domestic law in almost all countries. However, the reality could be more subtle. For example, as noted by Axel Petri, the German criminal law considers the right to self-defence, but under some very narrow conditions such as the attack being ongoing and self-defence being proportionate and not leading to a criminal act. Furthermore, businesses carrying out "hack back" measures could in fact violate both their domestic law and the law of the country where a damage is suffered. However, further work is needed in this area to understand domestic legal frameworks depending on how "hack back" is defined.

All States have a due diligence obligation to avoid that their territory is used by non-State actors to commit internationally wrongful acts against other States. Therefore, businesses carrying out "hack back" activities could engage the international responsibility of their State, regardless of whether "hack back" is authorised in their jurisdiction. Nevertheless, as noted by Stewart Baker, "hack back" measures aiming primarily at information gathering for attribution purposes may not create such legal consequences, although they might be considered as "cyber espionage", which is not covered by international law.

Session 4 – How to Achieve Security by Design?

Panellists: *Diane Rinaldo*, Deputy Administrator and Deputy Assistant Secretary for Communications and Information, Department of Commerce, NTIA, United States; *Pascal Andrei*, Chief Security Officer, Airbus; *Audrey Plonk*, Government and Policy Director, Intel; *Jeff Wilbur*, Technical Director, Online Trust Alliance (OTA); *Andreas Schweiger*, Managing Director Cyber Security Services, TÜV SÜD. **Moderator:** *Laurent Bernat*, Policy Analyst, OECD Secretariat.

Providers of digital technologies increasingly recognise the need to include digital security into the design of their services and products. However, digital technologies are developed in complex ecosystems in which many factors can cause difficulties. Panellists in this session discussed the challenges they face, shared best practices, and examined private and public sector approaches to encourage digital security by design.

Digital security by design requires a holistic approach, supported at the highest level, encompassing the product design, supply chain, and production environments

Both Airbus and Intel adopted digital security by design many years ago. In the case of Airbus, this approach is part of the company's holistic security governance (cf. session 1). Airbus realised in 2000 that digital security by design would become essential for its future, when it started to work on the A380, the first e-enabled aircraft. Digital security had to be taken into account before anything else was made, hence it even preceded the engine or the gears. The Chief Security Officer hired 21 "hackers" who demonstrated in practice that digital security had to be fully integrated into the aircraft's design because it was critical to safety. During the development of the A380's architecture, Airbus managed the avionics and other critical and sensitive components of the aircraft separately from the more open components, including the cabin. Sensitive components received the strongest protection, including for example with technologies to physically enforce one-way data flows. Hackers ran security tests throughout the product design stage. Extending digital security requirements to the supply chain was particularly challenging in the absence of digital security regulation. Airbus helped regulators develop certification requirements tailored to e-enabled aircrafts, i.e. integrating digital security into safety regulation. The company developed standards and baselines, provided them to suppliers and performed audits, including penetration tests in their facilities and of their equipment. The security of the industrial environment, including production, industrial control systems, assembly lines, testing and flight test beds, were aligned with that of the A380. The company also created a Public Key Infrastructure (PKI) to authenticate all software and data embedded in the aircraft.

Intel implements security by design by overlaying the so-called Security Development Lifecycle (SDL) over the product development lifecycle. At each product development's stage, security requirements must be embedded and they are tested and validated before the product reaches the next stage. This process merges security into normal engineering rather than addressing as a separate step. Intel also regularly improves its organisational processes to implement a more holistic approach to digital security. The most recent evolution is the establishment in 2018 of a central "Product Assurance Group" directly reporting to the CEO on security matters in order to scale up its existing security by design efforts. This new group centralises and enforces consistent security practices across the company's global operations and brings together existing resources.

Digital security by design of consumer IoT products should consider the products' ecosystem rather than only the IoT devices

Most producers of consumer IoT devices are much less mature than well-established global industrial players such as Intel and Airbus. Many start-ups offering IoT products are assembling various software and hardware components without any consideration of security and privacy risks. They have a time-to-market approach which is not sustainable for them in the long term and increases the risk to all stakeholders. The IoT Security & Privacy Trust Framework[5] was developed by the Online Trust Alliance through a multi-stakeholder effort to promote security and privacy in the design of consumer IoT devices. It provides a set of 40 principles covering four categories: i) security, ii) user access & credentials, iii) privacy, disclosures and transparency, and iv) notifications and related best practices. The framework can be used by various actors according to their role: manufacturers can adopt the principles, retailers can use them to decide which products to sell, and governments to inform the policy making process. Recognising that a system is as strong as its weakest link, the Framework takes a holistic approach, covering the IoT ecosystem (e.g. cloud backend, smartphone app, etc.) in context rather than IoT devices in isolation. For example, a data breach affecting the mobile application or back end cloud services supporting an IoT system can undermine consumer trust just as much as an attack on the IoT device itself. The Framework's principles also address aspects such as encryption of data in transit and at rest. It considers that security and privacy are both essential for consumer trust.

Updatability should be part of product design but can be challenging because of the complexity of integration ecosystems, technical limitations and cost

As products will become vulnerable once they are in customers' hands, products must be designed for survivability and resilience, despite many threats being unknown during the design phase, and designers not necessarily knowing how and for how long their products will be used. "Updatability" (or "patchability") is therefore essential. For chips and hardware devices, it varies according to architecture design. For example, Intel issued patches for many of its products affected by the recent SPECTRE and MELTDOWN[6] vulnerabilities. However, the sheer number of integrators through which patches have to flow to reach end users complicate updatability. Intel products for example go through many different distribution systems and Original Equipment Manufacturers (OEMs) which buy and assemble many digital components and often lack the incentives to pass patches on to end users. Public policies can help create such incentives, for example, through public procurement policy. For instance, in France OEMs responding to public tenders must make patches for firmware updates available within sixty days of public release of an issue. Airbus faces similar challenges with regards to patching software embedded in aircrafts. As aircrafts can have a lifespan as long as 30 years, the company hackers' team continuously tests them against new attack techniques to discover unknown vulnerabilities. Airbus uses a PKI infrastructure to ensure that all flying aircrafts operated by airlines run up-to-date certified software.

Manufacturers of consumer IoT devices should ensure that devices have sufficient memory and software headroom for patching. Unfortunately, they are generally balancing updatability with other factors such as cost, efficiency, etc. Furthermore, when products can be updated, patches need to be available during the full product's lifetime. What are consumers expected to do after two or three years when their refrigerator will no longer receive security updates? This misalignment between the product's lifespan and availability of patches may be particularly challenging where digital security can affect safety. IoT products' manufacturers have to consider additional challenges to take into account the full consumer product lifecycle. For example, responsibility for data management is often unclear: smart home products' design should provide clear processes and responsibility when home owners change, including how to change the electronic door keys and reset the IoT systems' data and passwords to ensure that previous owners can no longer access devices such as connected thermostats.

Technology companies have a responsibility to ensure that customers understand what their products entail, and what their role is with respect to security

In general, patching should be easy. Consumer IoT devices can for example be automatically patched, following the smartphone app model. But patching can be a complex challenge in industrial environments with thousands of servers and heterogeneous equipment. For example, Airbus had to update 16 000 servers over two days to contain the Wannacry attack. They had not been updated earlier for many reasons including because production lines could not be stopped.

More generally, consumers who buy a plant at a store know that they need to water it regularly to keep it alive, but the responsibility of those who buy a digital product is often unclear. Many consumers simply "don't know what is in the box" they purchased, where to easily find information about potential vulnerabilities and how to fix them. Technology companies have a responsibility to ensure that users understand what their products entail.

Certification can foster security by design but needs to evolve in order to meet the dynamics of digital security

Certification can foster digital security by design. So-called Test, Inspection and Certification (TIC) companies are neutral third parties which guarantee that their customers meet a certain quality standard, similar to a peer review process in science. In that process, certification services provide a baseline standard that enhances security knowledge and practice of vendors, sub-system and system manufacturers as well as integrators.

However, certification has to evolve to meet the dynamics of digital security. The current periodic certification approach based on annual tests and inspections no longer fits with the extremely dynamic digital security space. A certification service company cannot be liable for digital-dependent components based on tests carried out once a year knowing that a year in digital security can be seen as the equivalent of thousand years in classical engineering. According to TÜV SÜD, a more effective approach for companies in the TIC sector would be based on continuous rather than periodic tests and inspections. TIC companies are currently building up capabilities including in areas such as threat intelligence and analysis, in order to think like the attackers and develop scenarios to test the resistance of Original Equipment Manufacturer (OEM) devices' systems or sub-systems. TIC companies can then provide regulators with relevant information to help them adjust regulation, thereby feeding a virtuous cycle that can benefit all stakeholders. Still called "certification" for the moment, such services are quite different from classic certification and have the potential to significantly expand the TIC market.

The European Cybersecurity Act, expected to be adopted in 2019 encourages digital security certification and could have a trickle-down effect beyond Europe. However, it is still unclear how it will be implemented. A key challenge will be to define the scope of certification, recognising that it may be not be economically feasible to certify everything on platforms that integrate many different parts. It will therefore be necessary to determine the certification of which components can really bring value by making risk-based choices, on a case-by-case basis, while also taking the dynamics of the environment into account. It will also be important to manage trade-offs between testing/validation and exposure of sensitive information.

Students are not sufficiently trained to implement security by design and companies struggle to overcome the current digital security skills shortage

Two major skills-related challenges are limiting the capacity of businesses to implement security by design. First, only a few universities train programming and software engineering students to design software with security from the inception. Digital security is often approached during the last year of the programming or software engineering curricula as a separate and specialised area rather than as part of basic programming skills as of the first courses. Most students are trained to develop efficient but insecure software by design and to consider security as something that someone else will add later. Only the best universities have merged digital security into their general programming curricula and train students on the basis of real life start-up scenarios. This issue is particularly acute with respect to hardware-related technologies.

Second, there is a serious digital security skills shortage in most countries. Competition to hire talented digital security experts is intense and companies have to consider the global skills market. To overcome this situation, Intel is changing its corporate culture to become more flexible with respect to staff's location. TÜV SÜD is exploring solutions such as automation and online evaluations and is partnering with other firms to develop a service whereby OEMs upload their firmware and receive semi-automated assessment reports in 48 hours. More generally, businesses have an incentive to partner with universities to influence curricula in order to fill the digital security skills gap that they are currently facing.

Collaboration between all actors including partners and competitors is an important aspect of security by design

Collaboration and co-operation between all actors are key to promote and implement security by design. In the aviation sector, co-operation, including between airlines and manufacturers, to ensure end-to-end digital security is essential. For Airbus and the aviation industry more generally, there is no competition in safety and security. Airbus and Boeing cooperate very closely including to exchange safety and security information. For example, Airbus created the "Club of Four" including Boeing, Bombardier and Embraer to design new standards for safety and security. The company also participates in the Aviation-ISAC founded by Boeing.

Collaboration is also important between manufacturers, OEMs, integrators, and TIC companies to jointly address the dynamic challenges of digital security and find common solutions to enhance security by design. For example, an initiative such as the Charter of Trust provides a useful setting for different types of actors to share information and to address the challenges and find common solutions.[7] The IoT Trust Framework is an example of an effective multistakeholder collaboration to help inform actors in the consumer IoT ecosystem.

Public policies to encourage security by design should be based on a multistakeholder dialogue and consider all types of policy instruments

Public policy can promote digital security by design, but it needs to be balanced and well informed including to prevent regulation from stifling innovation. The experience of the United States National Telecommunications and Information Administration (NTIA) is that to avoid that scenario, governments should engage with all stakeholders to understand their needs and to assess the potential positive and negative consequences of policies on innovation, competitiveness and prosperity more generally.

Rather than focus on a single type of measure, governments should consider all policy tools and assess which ones would be the most effective according to the context and culture. For example, possible solutions to increase transparency about digital security and clarify all actors' responsibilities range from certification schemes to trustmarks and labelling and can be established through regulatory and/or self-regulatory measures.

Since digital security incidents can affect consumers' safety, product safety regulation might in theory provide an incentive to embed security by design in consumer IoT products. However, the intersection between product safety regulation and digital security are yet to be explored by governments. This includes issues such as, for example, the extent to which a connected physical product can be certified according to safety regulation without preventing the possibility to update it later. Co-operation between digital security agencies and product safety regulators could help better understand the potential synergies, tensions and opportunities between digital security and product safety.

Session 5 - Maintaining Security once Technologies are on the Market

Panellists: *Arne Schönbohm*, President, Federal Office for Information Security (BSI), Germany*; Angela McKay,* Senior Director of Cybersecurity Policy and Strategy, Microsoft*; Cristine Hoepers,* General manager, CERT.br*; Nelly Ghaoui*, Coordinating policy advisor cybersecurity, Ministry of Economic Affairs and Climate Policy, Netherlands*; Taro Hashimoto*, Deputy Director, Ministry of Internal Affairs and Communications, Japan*; Nimbe Ewald Aróstegui*, General Director of Technical Regulation, Instituto Federal de Telecomunicaciones, Mexico*; Monique Goyens*, Director General, BEUC. **Moderator:** *Jean-Baptiste Demaison*, Chair of the ENISA Management Board, Senior Digital Security Advisor to the Strategy Director, ANSSI, France.

Despite efforts to make technologies more secure from the outset, vulnerabilities are often found once products and services are used by customers. This session discussed challenges and possible solutions to maintain the security of digital products once they are in the hands of customers.[8]

A market failure prevents software from having a higher level of quality, in particular with respect to security

Software generally suffers from a lower level of quality than tangible products, as illustrated by a report from the German Federal Office for Information Security (BSI) which identified 700 vulnerabilities in the ten most widespread office products. Customers tolerate a low level of quality for ICT products that they would not accept for other products in part because there is generally no clear and neutral information about ICT products' level of security. This information asymmetry prevents security to be a criteria for customers' choice and a market differentiator for vendors. Furthermore, the cost of incidents exploiting software is born only by customers and other affected third parties. Software producers design vulnerable products without being accountable for consequences of incidents. This information asymmetry and negative externality create a market failure.

It is important however to have a nuanced approach when comparing software with tangible products' security and quality. The threats' dynamics are different in digital and physical environments. Trade-offs between costs and benefits are inevitable but more complex with software in part because vulnerabilities can be discovered long after products have been released. It is therefore necessary to explore what levels of security are needed depending on risks, markets, types of products and use contexts. For example, digital security requirements are likely to vary between a nuclear power plant, a traffic system, a refrigerator and a doll. Technologies should also be taken into account. For example, cloud services can more easily benefit from a more continuous update lifecycle and have less impact on customers infrastructure than regular patching cycles such as Windows "Patch Tuesdays".

Microsoft's experience shows that security can become a competitive advantage. Security became a market differentiator for Microsoft in the early 2000s, when some of its key customers indicated that they would turn to other products if security was not improved. Microsoft enhanced its software security over time, turning it into a competitive advantage. However, what worked for Microsoft may not necessarily work for other businesses, such as a financial company developing in-house applications, or a small niche software company.

The lack of transparency with respect to products' content increases the risk of large scale attacks

The software ecosystem is complex. It is often not limited to a vendor but rather includes a mix of actors such as designers, integrators, distributors, sellers, etc. whose incentives with respect to patching may not necessarily be aligned. For example, cheap components (e.g. chipsets) are often used across many different products. Malicious actors can exploit them simultaneously, for example to launch denial of service attacks, causing significant damages to a large range of third parties. The lack of transparency of "what's in the box", i.e. components inside products, prevents from swiftly identifying the cause of some incidents and requesting rapid action from the products or components' manufacturers. For example, the Mirai malware affected simultaneously devices such as cameras, TV recorders or home routers and Deutsche Telekom had to use its market power to oblige hardware and software providers to produce updates. Smaller ISPs however may not have such leverage over foreign firms or developers.

Businesses on the demand side are sometimes creating conditions for limited product security quality

The demand side sometimes plays a role in the lack of importance of security on the market so far. Businesses have had a tendency to use cheaper general purpose software for everything, including to support critical infrastructure, where products' lifecycle can extend beyond fifteen years making long-term patchability especially important. Similarly, to stay competitive, most businesses decision makers want everything to be interconnected in order to leverage real-time process monitoring and big data analysis, but they are reluctant to apply patches that could interrupt their production lines. They believe in the myth that some networks are isolated, until a disaster such as NotPetya or Wannacry brings them back to reality.

From a consumers' perspective, security should be provided by design and by default, and patchability should match products' lifespan

One may question whether functionalities enabled by connectivity are worth the security and safety risk they can raise to customers and third parties. For instance, a connected doll that could be easily exploited to spy on people's conversations and even take over its owner's home network was banned in Germany because its connectivity posed a significant danger to consumers.

More generally, for consumer advocates, security is to the digital environment what safety is to the physical world. It should be non-negotiable. All products should comply with a safety baseline out of which consumers should not be able to contract, as it is the case with food and cars. Security should be provided by design and by default, so that consumers can use a product safely without having to configure products or follow complex instructions. Users may have the freedom to lower the level of security if they wish, although there should be exceptions such as when it could affect others (e.g. a hackable car is dangerous for everybody). When safety is involved, security updates should be automatic, and in other cases, all actors (e.g. manufacturers, integrators, sellers, software providers, and consumers) should be informed about their responsibility for updating products and how to do it. The Japanese government, for example, carries out many awareness raising and educational activities focusing on patching and software maintenance.

When they sell connected products, businesses should ensure that their products are updatable but many vendors have an incentive to provide updates only for a short period of time in order to reduce cost and encourage consumers to buy new products. Shorter patch availability than the product's full lifespan accelerates obsolescence. This can impact the environment and create social inequality by dividing consumers into those who can afford security by regularly buying new products and the others. From a consumers' perspective, patches should be available during the full products' expected lifespan, and consumers should be informed about possible limitations in the provision of updates. It is therefore necessary for all stakeholders to discuss how to determine "reasonable expected lifespan" for different categories of products.

Regulation can address the market failure by making manufacturers liable and increasing market transparency

There is a debate regarding the extent to which voluntary approaches have improved products' digital security so far. In the physical world, security and safety measures such as seatbelts in cars or fire extinguishers in buildings generally resulted more from regulation than voluntary approaches. Some governments are contemplating regulation to address the market failure with respect to software security. For example, the German government is developing regulation in the router market to make producers liable if they provide low quality products. It is also preparing regulation to address information asymmetry and increase transparency about products' digital security, while working at the European Union level to establish minimum level digital security requirements for some products, in order to create a level playing field and drive higher security globally.

For consumer advocates, a regulatory solution based on voluntary measures is not the right approach. Security requirements should be an obligation for producers: if there is no compliance, there should be a consequence.

However, regulation can also have negative side-effects with respect to innovation, trade agreements, and access to technologies

Governments should however avoid one-size-fits-all approaches to avoid negative side effects of regulation. Different policy tools and incentives can be used in different risk scenarios (e.g. consumer market, critical infrastructure), depending on what customers are willing to pay, technologies, and other factors.

Regulation can also inhibit innovation, for example in the case of IoT technologies which continue to rapidly evolve. In some cases, technical requirements can be interpreted as technical barriers to trade. Measures that increase products' prices can widen the digital divide, contradicting government's objectives to bring digital technologies to the largest number of people.

Labelling and certification schemes can be useful, but the conditions for their success in this area are yet unknown

Labelling schemes can help vendors turn security into a competitive advantage and market differentiator. They can encourage the adoption of baseline security requirements and empower customers to decide how much risk they are willing to take when buying new products. However, it is unclear how many customers would be willing to pay for more security when less security would not significantly undermine their experience, such as when a device takes part in a botnet.

Agile and flexible certification mechanisms, including continued verification and inspection, would however need to be established to support such labelling schemes. In addition to issues discussed in session 4, certification can lead to "insecurity by compliance", as in Brazil where ISPs do not update some telecommunication equipment in order not to break mandatory certification requirements.

A multi-stakeholder dialogue, at domestic and international levels, is necessary to identify the most appropriate measures

To avoid potential counterproductive effects of regulation, stakeholders need to explore together, at the domestic and international levels, the types of requirements that would be most appropriate and cost-effective, including to make manufacturers accountable. For example: should producers have a security response team? A security contact point? A patching policy? Should products include secure code? Should products' content be transparent?

Such a discussion should take into account the complexity and wide variety of actors in the ICT value chain, from large players such as Microsoft and Deutsche Telekom to numerous smaller ones who nevertheless play an important role in providing key components or standing at key points in the value chain (e.g. there are 5000 ISPs in Brazil).

Session 6 – Encouraging Responsible Vulnerabilities Disclosure

Panellists: *Bruce Schneier*, Security Technologist and Author; *Marietje Schaake*, Member of European Parliament; *Rodolphe Harand*, Associate Director, Yes We Hack; *Lorenzo Pupillo*, Head of the Cybersecurity Initiative, Centre for European Policy Studies (CEPS); *Cedric Laurant*, Civil Society. **Moderator:** Prof. Beomsoo Kim, Vice-Chair of the OECD Working Party on Security and Privacy in the Digital Economy (SPDE).

Most software programs have many vulnerabilities because the software market does not reward quality, apart from a few exceptions. These programs are found everywhere in the economy and they support the functioning of the society including the government and critical infrastructure. It is therefore essential for technical, economic, social and national security reasons to discover, disclose and fix these vulnerabilities. Panellists in this session discussed how to encourage responsible and co-ordinated disclosure of vulnerabilities.

Legal uncertainty disincentivises security researchers from disclosing vulnerabilities to software vendors and the market rewards offense better than security

In an ideal world, security researchers would find vulnerabilities and disclose them to vendors.[9] Vendors would reward researchers, rapidly fix these vulnerabilities and distribute patches. Later, researchers would disclose the vulnerabilities they found to the public, to increase digital security knowledge and gain recognition from their peers, as appropriate. Responsible and co-ordinated behaviour by researchers and vendors throughout the disclosure process would prevent malicious actors from exploiting these vulnerabilities.

In reality, many vendors do not want researchers to disclose vulnerabilities, thinking this could damage their reputation and be potentially expensive. Instead of rewarding researchers, vendors in many cases sue them. This is possible because, as the Budapest Convention on Cybercrime does not take into account "ethical hacking", so researching vulnerabilities can be considered a crime in most countries. Vendors can also deny the existence of vulnerabilities found by researchers and even discredit them. For example, a security researcher who revealed a vulnerability in a database containing information of 93 million voters and was accused of using insider information rather than a vulnerability to access the data. The research ecosystem is extremely valuable to enhance all stakeholders' security and should be protected from legal and other threats.

Vulnerabilities have value for businesses and organisations who want to improve their products' security. Researchers can therefore also sell vulnerabilities. Unfortunately, vulnerabilities can have even more value for other actors who want to exploit them for offensive or criminal uses and who can often pay much higher prices than the businesses who could fix them. Such actors include weapons manufacturers, criminals, and governments, in particular the military, law enforcement and intelligence.

Some businesses and government agencies establish bug bounty programmes to reward researchers for reporting vulnerabilities. However, these other actors can outbid such bounties if these vulnerabilities can be exploited for offense, which is often the case. Price distortion by government actors is a major factor diverting the market towards offensive use. Overall, legal uncertainty disincentivises researchers from disclosing vulnerabilities to software vendors and feeds a market that rewards offense better than security.

Trusted intermediaries and technical platforms can encourage disclosure by streamlining disclosure processes, reducing legal uncertainty for researchers, and facilitating their retribution

Because of legal uncertainty, many researchers who contact vendors directly to report a vulnerability are taking a legal risk, in particular if they want to publish research information about what they discovered. The process can be cumbersome as some vendors may not even have a disclosure process or that can be unclear or complex.

To mitigate the legal risk and streamline the disclosure process, researchers can report vulnerabilities anonymously and/or through a trusted third party such as a Computer Emergency Response Teams (CERTs) which can act as a co-ordinator between researchers and vendors. If a domestic legal framework is in place, researchers can also disclose vulnerabilities to government agencies who in return can commit to protect them, as does, for example, the French cybersecurity agency ANSSI.[10] However, researchers are reluctant to rely on governments for disclosure and prefer to use non-profit trusted platforms, such as zerodisclo.com. The platform allows researchers to report a vulnerability anonymously to CERTs while receiving a signed and timestamped proof of deposit.

Bug bounty platforms bring together "ethical hackers" and software vendors to facilitate vulnerability disclosure. They simplify the organisation of bug bounty programmes by vendors and reduce legal risk for hackers. In fact, a bug bounty platform called YesWeHack was founded by three young ethical hackers who had friends who had been indicted in their youth for reporting vulnerabilities to vendors and who decided to help both hackers and vendors. Bug bounty platforms can also play a role in educating and helping researchers to develop skills. For example, YesWeHack launched a non-profit initiative where computer science students can submit code to the platform to improve their coding skills, and digital security students can train themselves in finding vulnerabilities in this code.

Public policy can promote responsible and coordinated vulnerability disclosure

Responsible disclosure of vulnerabilities is a public policy issue the origins of which can be traced back to Alfred Hobbs' work on locksmiths and lock picking in the 1850s' England. Hobbs argued that it is in the public interest to spread knowledge about locks' vulnerabilities rather than leave it in the hands of malicious actors who not only will have this information anyway, but will also exploit it in practice. Despite such a long history, software vulnerability disclosure remains a matter for experts and would deserve much more attention from policy makers and other stakeholders.

Governments should adopt public policies to encourage coordinated and responsible vulnerability disclosure, and better protect security researchers from legal proceedings. In Europe, only France and the Netherlands currently have adopted such a policy, but ten other countries are developing one.[11] Several standards and guidelines can be used as a basis to develop a European framework to encourage co-ordinated and responsible vulnerability disclosure in Europe. These include the ISO/IEC standards[12], Dutch Nationaal Cyber Security Centrum's Guideline[13] as well as other material from the United States Departments of Commerce and Justice[14]. Such a framework would encourage *i)* governments to recognise ethical hacking in their domestic legislation in order to reduce legal uncertainty for researchers, *ii)* vendors to publish their vulnerability disclosure policy on their web site, in line with ISO standards; *iii)* researchers to immediately disclose vulnerabilities to vendors to facilitate swift fixing; and *iv)* CERTs to act as trusted third parties and co-ordination centres.

To help reach a global consensus on this issue, the Global Commission on the Stability for Cyberspace adopted two norms in its so-called Norm Package Singapore (Global Commission on the Stability of Cyberspace, 2018[5])[15], addressing respectively States and private sector: the "Norm for States to Create a Vulnerability Equities Process" [16], and the "Norm to Reduce and Mitigate Significant Vulnerabilities"[17]. Since this area affects national security and intelligence, it is difficult for governments to coordinate at the European level. Nevertheless, the European Parliament has adopted amendments on vulnerability disclosure in the Cybersecurity Act.[18] The Act will give ENISA a mandate to assist EU members, on a voluntary basis, including on how to develop a policy framework for vulnerability disclosure. It is also expected to legally bind manufacturers of newly certified products to provide contact information and information on accepted methods for receiving vulnerability information from end-users or researchers.

Data protection laws can also create an incentive for businesses to fix vulnerabilities as they can be exposed and their reputation can be damaged if data protection agencies take action after being informed of a security breach. However, this is not always effective. For example, civil society reported in 2013 a large data breach in a Mexican bank to the data protection authority, which did not follow up.

Vulnerabilities in Internet of Things (IoT) devices raise difficult challenges for responsible disclosure

Co-ordinated and responsible vulnerability disclosure places pressure on vendors to fix the vulnerability because once the researcher has disclosed a vulnerability to a vendor, he/she can make it public whether the vendor fixed the vulnerability or not. However, there is sometimes no ecosystem for updating low cost embedded systems, such as routers or some IoT devices. In addition, in some cases, such as with aircrafts, incidents exploiting such vulnerabilities can lead to severe physical consequences. In these cases, the decision on whether and how to make a vulnerability public can be difficult for researchers. Artificial Intelligence (AI) also raises a difficult challenge. In the future, AI could help systematically find vulnerabilities to ensure secure software development. However, AI may also help identify myriads of vulnerabilities in programmes already deployed. Many of these vulnerabilities will not be possible to fix and could be exploited for offensive use.

Conclusion - Public Policy Discussion

Panellists: *Henri Verdier*, Ambassador for Digital Affairs, France; *Amb. Thomas Fitschen*, Special Representative for Cyber Foreign Policy and Cybersecurity, Germany; *Matthew Travis*, Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA),Department of Homeland Security (DHS), United States; *Carlos da Fonseca*, Head of the Information Society Division, Ministry of Foreign Affairs, Brazil; *Makoto Yokozawa*, Business at OECD (BIAC); *Suso Baleato*, Civil Society Information Society Advisory Council (CSISAC); *Nigel Hickson*, Internet Technical Advisory Committee (ITAC). **Moderator**: *Katarina de Brisis*, Chair of the OECD working Party on Security and Privacy in the Digital Economy (SPDE)

Henri Verdier, French Ambassador for Digital Affairs, underlined that many issues addressed during the event have gained significant maturity over the last few months after having been underestimated for a long time. There is in particular increased awareness of the global systemic dimension of digital security risk, and the need for public-private co-operation and sharing of good practice. France's current priority is to foster an international consensus on a set of minimal good practice with respect to key challenges such as strengthening the security of digital products and services throughout their lifecycle while involving all relevant actors in the value chain from inception ("security by design") to integration ("security by default") and end of life; ensuring transparency with respect to the length during which products' security updates are provided ("maintien en conditions de sécurité"), and promoting responsible disclosure of vulnerabilities. Henri Verdier emphasised the key role OECD has played over the last 25 years. He stressed that the OECD should continue to lead in this area, including to facilitate an international public-private dialogue. France will also support the development of an international consensus on these topics through various fora, including in the European Union, and at the G7 and G20.

Ambassador Thomas Fitschen, Special Representative for Cyber Foreign Policy and Cybersecurity, Germany, emphasised that it is essential to place privacy, freedom of speech and the right to seek information at the core of public policies when considering digital security from the perspective of prosperity. Human rights have to be protected online as they are protected offline. Our economies cannot realise the full potential of the Internet and digital transformation if individuals do not trust that the tools they use for carrying out digital interactions are sufficiently secure. As the current chair of Freedom Online Coalition 2018, Amb. Fitschen underlined the agreement by the Coalition's 30 governments that all cybersecurity policies should respect human rights by design.[19] He also underlined linkages between the roles of governments, private sector and individuals and mentioned the United Nations' work on "The Right to Privacy in the Digital Age" which places a strong emphasis on the role of States while also considering the role of the private sector. Finally, Amb.

Fitschen highlighted the cross-border nature of the Internet which raises complex enforcement challenges and encouraged OECD members and private sector to work on practical ways of cooperating across borders rather than trying to harmonise all legislations globally, which seems unrealistic. He pointed out the Internet Jurisdiction Project which will meet in June 2019 in Berlin as a useful venue to continue the discussion in this area.

Matthew Travis, Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS), United States, underlined the important role of the OECD with respect to digital security over the last 25 years. He provided information about the Cybersecurity and Infrastructure Security Agency (CISA), the lead civilian cybersecurity agency in the United States which is responsible to secure federal networks, conduct cybersecurity response operations for federal agencies, States, local territories and private sector partners, and to manage sixteen critical infrastructure sectors. Mr. Travis commented on some discussions held during the Global Forum Inaugural Event. Noting that a single user's weak password can take down an entire company, he echoed the need for business leaders to change their companies' culture and engage with CISOs in order for digital security risk management to be treated as a business priority rather than as a backoffice function. With respect to security by design, he drew a parallel between trade-offs that need to be made today with digital technologies and those made in the United States when the death toll on the roads increased in 1950s and 1960s. The government could have decided to build more hospitals or train more doctors but decided to make cars safer. While the analogy has limits, it shows the potential benefits of adopting a stronger regulatory regime. The Department of Homeland Security (DHS) has been increasingly active in this area, in particular with respect to the security of government's systems. Recalling that co-operation is core to OECD's mission (the "C" in OECD), Mr. Travis underlined the need to start co-operating internationally to identify common principles for a more secure digital ecosystem based on a better understanding of what shapes or does not shape the market, and taking into account common values such as human rights, the free exchange of data across borders, and the promotion and protection of internet freedom. He also stressed, as part of these values, that responsible nation States should not target other nations' critical infrastructure through cyberspace, or steal businesses' intellectual property. The OECD is a key international forum to share and support such values.

Carlos da Fonseca, Head of the Information Society Division, Ministry of Foreign Affairs, Brazil, highlighted several high-level take-aways from the meeting. First, the huge increase in criminal activities against businesses, governments and individuals undermines trust in digital technologies. Second, there is a need for an internationally co-ordinated response to an inherently cross-border challenge but countries are not equally prepared to face digital security issues. There are also significant asymmetries between companies, governments, individuals, etc. It is therefore necessary to coordinate and co-operate to level the playing field in terms of capacity building, preparedness, digital literacy, etc. Third, there is a high degree of digital complexity, with different levels of interconnectedness across many layers of technologies, and many actors playing different roles. The Internet of Things is likely to increase this complexity, as the number of connected and less secure devices will grow. It is therefore essential to address the security of the value chain as a whole in order to approach these layers simultaneously or at least in a coordinated manner because security is as good as the weakest link. A multistakeholder and multidisciplinary approach is necessary at national and international levels. Mr. Fonseca highlighted that in theory it should be easy to co-operate and articulate a co-ordinated response to all these challenges because everyone wants better security. In reality, silos are difficult to overcome despite everybody recognising the need to do so. This is a typical case of a "collective action problem". It is also important to approach digital security as an enabler to empower citizenship rather than an end in itself. It should also not be used as a pretext for practices that violate privacy, freedom of speech and other fundamental values.

Building on the Brazilian experience, Mr. Fonseca underlined the need for robust personal data protection and freedom of expression frameworks and stressed the importance of approaching digital security within the broader context of the digital transformation rather than as a standalone objective. He noted that the development of a comprehensive digital transformation strategy addressing digital security as part of a broader framework can facilitate co-operation and collaboration at the national level. Nevertheless, he recognised that collaboration can be more complicated at the international level as there are many international fora and tools addressing different facets of cybersecurity. Mr. Fonseca concluded by praising the OECD Global Forum on Digital Security for Prosperity and pointing it out as an important vehicle for future work in this area.

Makoto Yokozawa, from the Business and Industry Advisory Committee to the OECD (BIAC), underlined the importance of OECD Recommendations on digital security and their emphasis on multistakeholder co-operation. He however highlighted the need to further engage individuals and in particular elderly, junior and disabled populations with respect to awareness raising on digital security. Mr. Yokozawa also underlined that self-regulation can be very effective to enhance digital security in particular in combination with standards such as ISO/IEC 27000. Mr. Yokozawa suggested that OECD reaches out to a wider audience including APEC, the United Nations, and organisations such as ISACs and Computer Security Incident Response Teams (CSIRTs).

Suso Baleato, from the Civil Society Information Society Advisory Council (CSISAC) thanked the OECD for actively engaging with the civil society and inviting it to participate in the Global Forum. He stressed that the objective of digital security is to establish trust as an essential requirement for the digital economy to drive innovation and prosperity in general. The emergence of the Internet of Things will be a key challenge for trust in the next few years and a human-centric approach will be key to promote trust and address information asymmetries. Mr. Baleato also underlined that trust requires both security and privacy. He suggested to promote the notion of "cryptography by default" and, where artificial intelligence is involved, to encourage algorithmic transparency as a means to enable risk assessment. With respect to "hack back", Mr. Baleato suggested to avoid framing digital security in binary and military terms and rather adopt an economic and social narrative with users, consumers, providers, and governments. In conclusion, Mr. Baleato supported the development of follow-up work at the OECD promoting a human-centric perspective, information sharing and, more specifically vulnerability disclosure.

Nigel Hickson, from the Internet Technical Advisory Committee (ITAC) underlined that pragmatism, honesty, openness and transparency are essential values to create a digital environment where people have trust and confidence and can innovate, and that practices such as "hack back" are not conducive to establish trust. Discussions during this event showed that self-regulatory approaches are no longer sufficient. It has become necessary to have minimal baseline security. Global approaches that bring stakeholders together are needed to make progress in this area. It is important that no countries are left behind in this international dialogue. Multistakeholder policy development is also key at the domestic level, including through national digital transformation strategies. Mr. Hickson criticised the top-down approach in some other intergovernmental organisations where issues such as cybersecurity, cyberterrorism, cryptography, etc. are discussed only by governments without the relevant stakeholders in the room. He praised the OECD for having been innovative over the last 25 years in ensuring that stakeholders have a role in fashioning digital economy policy. He concluded by calling for the OECD to continue this work and engaging more countries in this dialogue.

Annex A. Agenda

GLOBAL FORUM ON
DIGITAL SECURITY
FOR PROSPERITY

OECD

Roles and Responsibilities of Actors

GOVERNANCE OF DIGITAL SECURITY IN ORGANISATIONS AND SECURITY OF DIGITAL TECHNOLOGIES

13-14 December 2018 – OECD Conference Centre, Paris, France

Global Forum Web Site: oe.cd/gfdsp

> “**All stakeholders should take responsibility for the management of digital security risk.**”
>
> OECD 2015 Recommendation on Digital Security Risk Management for Economic and Social Prosperity

The OECD Global Forum on Digital Security for Prosperity

- Aims to consolidate a global network of experts and policy makers by fostering regular sharing of experiences and good practice on digital security risk and its management, mutual learning and convergence of views on core thematic issues related to digital security for economic and social prosperity.
- Is an international multilateral, multi-stakeholder and multidisciplinary setting for all communities of experts to meet, dialogue, network and influence public policy making on matters related to digital security for prosperity.
- Feeds OECD policy discussions. Its output can lead to the development of analytical work, principles and international policy recommendations.

Purpose of the event

This inaugural event of the Global Forum will examine the roles and responsibilities of actors for digital security, with a focus on good practice for the governance of digital security risk in organisations, and improving digital security of technologies throughout their lifecycle.

It will bring together businesses and organisations using digital technologies, suppliers of these technologies, suppliers of security solutions, experts from civil society and academia as well as government policy makers interested in encouraging the adoption of best practice to reduce digital security risk.

Who should participate?

Public policy makers from governments in OECD member and non-member countries; Chief Information Security Officers (CISOs), risk managers and other experts in charge of digital security in businesses and public sector organisations; digital security experts from firms offering digital products and services (hardware and software products, network and cloud services, etc.) or digital security services; experts from civil society, academia and the technical community.

Format and language

Organised around 6 plenary sessions, the event will interactively engage speakers and participants. The final session will lay out main findings and possible future work to enhance international co-operation. Interpretation in English and French will be provided.

Contact

For more information, please contact: OECD Secretariat - digitalsecurity@oecd.org

GLOBAL FORUM ON
DIGITAL SECURITY
FOR PROSPERITY

OECD

AGENDA

Chair: Jørgen Abild Andersen, former Chair of the OECD Committee on Digital Economy Policy (CDEP)

DAY 1: Thursday 13 December 2018

8:30 Registration

9:00 **Welcome remarks**

Keynote: Guillaume Poupard, Director General, National Cybersecurity Agency (ANSSI), France

PART I: DIGITAL SECURITY RISK GOVERNANCE IN ORGANISATIONS

This part will explore roles of actors within organisations (session 1), and their responsibilities with respect to others (session 2) and regarding how far they can go in protecting themselves (session 3).

9:30 Session 1 - Changing the Culture at the Top and Breaking Corporate Silos

A clear chain of responsibility starting at the highest level of leadership is essential to manage digital security risk. A governance framework is also necessary to clarify who is responsible for what, and how collaboration can take place, including across silos. This session will discuss how to make digital security a priority for CEO, Board and C-Suite. It will also discuss good practice for digital security risk governance, including co-ordination, chains of reporting, incentives, evaluation, etc.

Moderator: Jeremy Millard, Senior Consultant, Danish Technological Institute, Denmark

Panellists:

- Pascal Andrei, Chief Security Officer, Airbus
- Sebastian Bregning, Senior Risk Manager, A.P. Møller – Mærsk
- Andrea Bonime-Blanc, CEO, GEC Risk Advisory
- Dato' Dr. Haji Amirudin Bin Abdul Wahab, CEO, Cybersecurity Malaysia
- Hudi Zack, Chief Executive Director (acting) Technology Unit, Israel National Cyber Directorate (INCD)
- Philippe Cotelle, Board Member, Federation of European Risk Management Associations (FERMA)

11:00 **Break**

11:30 **Session 2 - How Can Value Chain Partners Trust Each Other's Digital Security Governance?**

In hyper-connected economies, digital security threats can come from anywhere, including from partners along the value chain. How can partners trust each other in a business ecosystem and value chain? Are there particular mechanisms or measures that can achieve trust between partners (e.g. standards, certification, information sharing). This session will discuss good practice and incentives schemes to foster trust between partners.

Moderator: Kathryn Jones, Senior Policy Advisor, Department of Culture, Media, and Sports (DCMS), United Kingdom and Vice-Chair of the OECD Working Party on Security and Privacy in the Digital Economy (SPDE)

Panellists:

- Henry Young, Senior Technology Policy Advisor, Department of Commerce, United States
- Koji Ina, Deputy Director, Ministry of Economy, Trade and Industry, Japan
- Evangelos Ouzounis, Head of Unit, European Network and Information Security Agency, ENISA
- Yuval Segev, Israel National Cyber Directorate (INCD)
- Michiel Steltman, Director, Digital Infrastructure Netherlands Foundation (DINL)
- John Salomon, Director, Financial Services Information Sharing and Analysis Center (FS-ISAC)

13:00 **Lunch Break**

14:00 **Session 3 - "Active Defence": How Far Can Businesses Go in Proactive Security?**

The private sector has been exposed to an increasing number and variety of attacks and businesses are dependent on their governments if they wish counter-offensive action to be taken against attackers. Today practices known as "hacking-back" are within governments' prerogative only. Should public policy evolve in order to clarify whether and how private sector could take proactive defensive measures (also called "active cyber defence")?

Moderator: András Hlács, Vice-Chair of the OECD Committee on Digital Economy Policy

Panellists:

- Axel Petri, Senior Vice President Group Security Governance, Deutsche Telekom
- Stewart Baker, Partner, Steptoe & Johnson
- Yves Verhoeven, Director for Strategy, National Cybersecurity Agency (ANSSI), France
- Théodore Christakis, Professor of International Law, University Grenoble-Alpes, France
- Leandro Ucciferri, Asociación por los Derechos Civiles, Argentina

15:30 **Break**

PART II: MAKING DIGITAL TECHNOLOGIES MORE SECURE THROUGHOUT THEIR LIFECYLE

This part will explore roles and responsibilities of actors to make technologies more secure at technology design and integration stages (session 4) and once the technology is in customers' hands (session 5). It will also discuss how increase the responsible discovery and disclosure of vulnerabilities (session 6).

16:00	**Session 4 – How to Achieve Security by Design?**

Providers of digital technologies are increasingly aware of the need to take digital security into account in the design of their products and services. But digital technologies are no longer purely digital: they are embedded in physical devices and products such as cars and planes, robots in factories, and heating systems in our homes. Digital technologies are developed in complex ecosystems involving large numbers of partners such as designers, integrators, distributors, etc. They are also deployed by customers in very different environments, also involving many actors and partners. Trade-offs need to be made between security, functionality, cost, time-to-market, and other factors affecting competitiveness. This session will discuss the roles and responsibilities of actors for making technologies more secure from the outset, the incentives and disincentives they face, the need for baseline and other security standards, their implementation throughout the value chain, and the possible need for third party evaluation.

Moderator: Laurent Bernat, Policy Analyst, OECD Secretariat

Panellists:

- Diane Rinaldo, Deputy Administrator and Deputy Assistant Secretary for Communications and Information, Department of Commerce, NTIA, United States
- Pascal Andrei, Chief Security Officer, Airbus
- Audrey Plonk, Government and Policy Director, Intel
- Jeff Wilbur, Technical Director, Online Trust Alliance (OTA)
- Andreas Schweiger, Managing Director Cyber Security Services, TÜV SÜD

17:30	**End of Day 1 - Cocktail**

DAY 2: Friday 14 December 2018

9:00 Session 5 – Maintaining Security once Technologies Are on the Market

Despite efforts to make technologies more secure from the outset, vulnerabilities are often found once products and services are used by customers. This session will discuss challenges related to the management of vulnerabilities, including the roles and responsibilities of different actors in the development, integration and application of security updates, and with respect to products' end of commercial support, i.e. when they are no longer supported (vulnerabilities' discovery and disclosure will be discussed in session 6).

Moderator: Jean-Baptiste Demaison, Chair of the ENISA Management Board, Senior Digital Security Advisor to the Strategy Director, ANSSI, France.

Panellists:

- Arne Schönbohm, President, Federal Office for Information Security (BSI), Germany
- Angela McKay, Senior Director of Cybersecurity Policy and Strategy, Microsoft
- Cristine Hoepers, General manager, CERT.br
- Nelly Ghaoui, Coordinating policy advisor cybersecurity, Ministry of Economic Affairs and Climate Policy, Netherlands
- Taro Hashimoto, Deputy Director, Ministry of Internal Affairs and Communications, Japan
- Nimbe Ewald Aróstegui, General Director of Technical Regulation, Instituto Federal de Telecomunicaciones, Mexico
- Monique Goyens, Director General, BEUC

10:30 **Break**

11:00 Session 6 - Encouraging Responsible Vulnerabilities Disclosure

To make technologies more secure, so-called "zero day" vulnerabilities must first be discovered and disclosed for mitigation measures to be developed and implemented. However, many vulnerabilities are discovered by researchers and "hackers" and have a lot of value for technology suppliers and security firms who want to improve products' security, and for criminals and other actors who want to exploit or sell them. Coordinated disclosure of vulnerability processes are easier to implement in a finder-vendor relationship but become more complex where they involve a variety of companies and complicated supply chains. This session will discuss how to reduce zero-day vulnerabilities' lifetime, encourage responsible disclosure of vulnerabilities and ethical hacking ("white hat"), and how coordinated disclosure of vulnerability can be implemented in increasingly complex environments and supply chains.

Moderator: Prof. Beomsoo Kim, Vice-Chair of the OECD Working Party on Security and Privacy in the Digital Economy (SPDE)

Panellists:

- Marietje Schaake, Member of European Parliament
- Bruce Schneier, Security Technologist and Author
- Rodolphe Harand, Associate Director, Yes We Hack
- Lorenzo Pupillo, Head of the Cybersecurity Initiative, Centre for European Policy Studies (CEPS)
- Cedric Laurant, Civil Society

Conclusion

12:00 **Public Policy Discussion**

This session will bring together policy experts from OECD and non-OECD governments, private sector, civil society and technical community for a high-level policy discussion on the main findings from the event, possible avenues for future work and international co-operation.

Moderator: Katarina de Brisis, Chair of the OECD working Party on Security and Privacy in the Digital Economy (SPDE)

Panellists:

- Henri Verdier, Ambassador for Digital Affairs, France
- Ambassador Thomas Fitschen, Special Representative for Cyber Foreign Policy and Cybersecurity, Germany
- Matthew Travis, Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS), United States
- Carlos da Fonseca, Head of the Information Society Division, Ministry of Foreign Affairs, Brazil
- Makoto Yokozawa, Business at OECD (BIAC).
- Suso Baleato, Civil Society Information Society Advisory Council (CSISAC)
- Nigel Hickson, Internet Technical Advisory Committee (ITAC)

13:00 **Concluding Remarks**

- Angel Gurría, Secretary-General, OECD

13:20 **End of the event**

Global Forum Web Site: oe.cd/gfdsp

Global Forum Partners

Endnotes

[1] In 2017, a malware called NotPetya hit many businesses in Ukraine and spread internationally, affecting the several major US and European organisations. According to some estimates, losses by large firms reached USD 1.2 billion. Cf. www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue.

[2] Federation of European Risk Management Association (FERMA), European Confederation of Institutes of Internal Auditing (ECIIA) (2017), "At the Junction of Corporate Governance and Cybersecurity". www.ferma.eu/ferma-eciia-cyber-risk-governance-report

[3] Open Forum 33 on "Privacy Sector Hack Back: Where is the Limit?". www.intgovforum.org/multilingual/content/igf-2018-day-1-salle-ix-of33-private-sector-hack-back-where-is-the-limit

[4] Council of Europe (2001), *Convention on Cybercrime,* https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[5] Online Trust Alliance: *IoT Security & Privacy Trust Framework v 2.5,* https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

[6] For more details, cf. https://meltdownattack.com.

[7] Charter of Trust for a secure digital world, https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/corporate-core/topic-areas/digitalization/cybersecurity/shi-13378-cot-dok-narrative-online-2018-02-13-sbi-en.pdf

[8] Discovery and disclosure of vulnerabilities are addressed in session 6.

[9] In this section, the term "vendor" means the person or organisation that created or manages the product that is vulnerable.

[10] https://www.ssi.gouv.fr/en-cas-dincident/vous-souhaitez-declarer-une-faille-de-securite-ou-une-vulnerabilite/

[11] CEPS (2018), Software Vulnerability Disclosure in Europe. www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf.

[12] ISO/IEC 29147:2018 Standard on Vulnerability Disclosure, ISO/IEC 30111:2013 on Vulnerability Handling Processes

[13] Nationaal Cyber Security Centrum (2018), Coordinated Vulnerability Disclosure: The Guideline. www.enisa.europa.eu/news/member-states/WEB_115207_BrochureNCSC_EN_A4.pdf.

[14] Department of Commerce, National Telecommunications and Information Administration (NTIA) (2016), Coordinated Vulnerability Disclosure Template; US Department of Justice, Cybersecurity Unit, Computer Crime and Intellectual Property Section Criminal Division (2017), Vulnerability Disclosure Program for Online Systems, www.justice.gov/criminal-ccips/page/file/983996/download.

[15] Global Commission on the Stability of Cyberspace (2018), Norm Package Singapore. https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf.

[16] "States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favour of disclosure."

[17] "Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take reasonable steps to ensure that their products or services are free from significant vulnerabilities, take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity."

[18] Cf. https://marietjeschaake.eu/media/uploads/posts/1525687697-Marietje%20Schaake%20AM%20EU%20Cybersecurity%20ACT%20ITRE%20COM(2017)0477_26042018.1050.pdf

[19] See also Freedom Online Coalition (2016), *Freedom Online Coalition Statement on a Human Rights Based Approach to Cybersecurity Policy Making*, www.freedomonlinecoalition.com/wp-content/uploads/2017/01/17-10-16-FOCWG1_FOC_SupportLetter.pdf