How to improve cyber resilience of SMEs by successfully implementing policy initiatives

February 9th, 2021, 9:30 – 12.30 Virtual event

Organised on behalf of:
European Commission DG GROW
Executive Agency for Small and Medium sized Enterprises (EASME)
By Capgemini

There is no digital transformation without cybersecurity. Digitisation of SMEs is an important and big challenge: from various evidence it is clear that SMEs are hesitant when it comes to adopting new technologies. Despite market volume or business growth opportunities, most SMEs keep lagging behind. And that is NOT going to help them on the long term. Cyber-risks are threatening business continuity, in two ways. First, continuity of the SME itself since 60% of SMEs that are victims of cyber-attacks did not recover and had to shut down within six months. Second, cyber criminals are increasingly looking towards SMEs as a gateway to the supply chain they are part of – and hence also a liability to the larger corporations on that chain.

The crucial question is: how can SMEs be supported to become cyber-resilient? What are the key factors of implementing policies successfully and which stakeholders are essential in that process?

This seminar tackled these questions by asking both EU policy makers, as well as other stakeholders, presenting good practices, and via an interactive debate. It was organised by the Advanced Technologies for Industry (ATI) project (https://ati.ec.europa.eu/) commissioned by EASME and DG GROW.

Welcome and introduction to the ATI project

Evangelos Meles, European Commission, DG GROW F.1 – Industrial Strategy and Value Chains

Evangelos Meles welcomed the audience and briefly introduced the ATI project and its current implementation supporting the EU's industrial policy, with a systematic monitoring of technological trends and reliable, up-to-date data on advanced technologies. More in detail, the ATI project is providing:

- Statistical data on the production and use of advanced technologies including enabling conditions such as skills, investment or entrepreneurship;
- Analytical reports such as on technological trends, sectoral insights and products;
- Analyses of policy measures and policy tools related to the uptake of advanced technologies;

- Analysis of technological trends in competing economies such as in the US, China or Japan;
- Access to technology centres and innovation hubs across EU countries.

Objective of today

Introduction – Niels van der Linden, Senior Director and EU Lead Capgemini Invent

Niels van der Linden, host of this seminar, kicked-off the session by illustrating the importance of improving cyber resilience of SMEs. Recent figures reveal the importance of SMEs for the European economy. At the same time SMEs are increasingly under threat since there is a rise of cyber-attacks on SMEs especially during the COVID-19 pandemic with 60% of SMEs even having to shut down within 6 months after the cyber-attack.

Skills shortages are a key part of the puzzle: lacking awareness on leadership level, shortages of cyber specialists and missing basic digital skills by other employees. Also, training of employees in SMEs is far from common practice.

Although there are many barriers, the ultimate objective is to increase the capacity of industry, social partners, education and training organisations and policy makers at all levels to promote and support the acquisition of skills related to Cybersecurity by SMEs in Europe.

In this seminar cybersecurity policies are presented by the European Commission, the findings of the ATI project regarding the policy brief on cybersecurity are presented, and good practices related to the policy initiatives supporting cybersecurity SMEs are outlined.

EU Cybersecurity Strategy and Capacity-building for SMEs

Martin Ubelhor, DG CONNECT, Head of Sector Cybersecurity Technology and Capacity Building

Martin Ubelhor presented the challenges in cybersecurity and related to this the EU's Cybersecurity Strategy for the upcoming 'Digital Decade'. Key aspects of this strategy are resilience, sovereignty and leadership. Operational capacity is needed to prevent, deter and respond to cyber-attacks, including the establishment of a Joint Cyber Unit, the cyber-diplomacy toolbox and the review of the Cyber Defence Policy Framework to increase the cyber defence cooperation and coordination. To support a global and open cyberspace, the EU takes leadership on international norms and standards and reinforces the cooperation with partners. The development and set-up of an EU External Cyber Capacity Building agenda will strengthen the capacities to tackle cyber threats.

A European Cybersecurity Technology & Innovation Ecosystem of EU funding, capacity building and community building supports the EU's resilience against cyber threats. A wealth of cybersecurity knowledge is available in the EU: more than 660 cybersecurity expertise centres are registered and ECSO has about 250 members. Other examples of the ecosystem are the European Competence Centre, the Network of National Coordination Centres and a large, open competence community of cybersecurity stakeholders. Next to this there are EU pilots helping to prepare the European Cybersecurity Network. The European Competence Centre manages the funds foreseen for cybersecurity under Digital Europe and Horizon Europe 2021-2027. The presentation outlined the initial funding priorities of both programs.

Capacity building for SMEs

Demosthenes Ikonomou, ENISA, Head of Capacity Building

Demosthenes Ikonomou presented the findings of the ENISA study on Cybersecurity for SMEs (2020 – 2021). In this study 249 SMEs participated from 25 EU Member States in 12 different industries. One of the key findings was that 36% of the SMEs reported they had experienced incidents and that 8% experienced a large increase during the COVID-19 period, but that only a small percentage of the SMEs increased security during this period. Less than 30% of the SMEs have an Information Security Officer on premises and Business Continuity and Disaster Recovery Plans. In general, SMEs do not appear to be inclined in implementing more measures than currently employed without it being explicitly mandated by a law or a regulation.

An overview of national efforts to support SMEs was provided including the Centre for Cyber Security Belgium, the CyberMalveillance portal in France, and the online source for cybersecurity in Luxembourg SECURITYMADEIN.LU. Also ENISA's support for SMEs was presented:

- Development of technical, organisational, and policy guidelines
- Development of online tools and campaigns to raise cybersecurity awareness – Cyber Hygiene
- Recommendations for EU MS to support SMEs
- Building knowledge of SMEs needs through information exchange and stakeholder engagement
- Technical training

Improving resilience through awareness raising about cyber-theft of trade secrets

Davide Follador, DG GROW, Unit F3 – Intellectual Property

Davide Follador presented the vulnerability of trade secrets in a digitally connected world. The distribution of incidents and the consequences for companies were presented. An overview was presented of the EU response in terms of related policies:

- COM Communication "Strengthening Europe's Cyber Resilience System" (2016)
- COM and EEAS Joint Communication on Cybersecurity for the EU (2017)
- Trade Secrets Directive (2016/transposition due by 2018)
- IP Action Plan - EU Cybersecurity Strategy (2020)

This was complemented with the strategic tools to address the challenges and what can be done to support SMEs: raise awareness about cyber theft of trade secrets, increase knowledge sharing, promote international cooperation, incentivise investments in cybersecurity, R&D on cybersecurity and cyber-diplomacy. The presentation was concluded with the way forward, from consultations (2020-2021), to the development of an awareness toolkit (2021), creation of synergies (Q4 2021) with specialists and the dissemination (as from 2022).

Insights from the ATI project on cybersecurity for SMEs

Morten Rasmussen – Technopolis Group

Morten Rasmussen presented the ATI project results on cybersecurity so far with a focus on the Policy Brief on Cybersecurity: more investments and better skills . The policy brief shows there is a strong focus on research and development in the EU27 and a relatively high number of digital security patent applications. Especially France and Germany contribute to the EU strengths in cybersecurity patenting. Canada, US and China are the most specialized countries globally. The research shows a relatively low investment and start-ups in the EU cybersecurity industry. The number of professionals with cybersecurity skills is lagging behind in the EU27. The US have relatively higher shares of cybersecurity professionals compared to the EU27 in all industries investigated (including ICT, finance, electronics, medical devices, automotive, chemicals). Within the EU, the countries with the highest share of professionals with specific technological skills in cybersecurity include Luxembourg, Cyprus, Spain, France, Ireland & Estonia. Of all professionals with cybersecurity skills 86% are men which points at a large gender gap in the field (though in some countries such as Ireland the gap is closing). With regard to the adoption of security technologies, 55% of SMEs have already used cybersecurity and 19% plan to adopt it over the course of the next twelve months.

Good practice 1: Developing a competitive European cybersecurity ecosystem

Luigi Rebuffi, Secretary General, European Cyber Security Organisation (ECSO)

Luigi Rebuffi presented his vision on the development of a European cybersecurity ecosystem providing trusted cybersecurity solutions and advancing Europe's cybersecurity posture and its technological independence. ECSO has a leading market platform for promoting European cybersecurity companies, forming a regional and European ecosystem where demand meets supply, funding, resources and know-how.

The ECSO SME Hub Suite is a European Cybersecurity SMEs marketplace. The three main components of the SME hub were presented: radar & registry, label and quadrant.

Also, the role of SMEs and of the regions in strengthening the European Union's cybersecurity in the coming future was presented. Analysis of regional ecosystems and European cybersecurity value chain validated the methodology (including market taxonomy) to collect market data and enhance the visibility of the SMEs. ECSO supports coordination in the future Network of European Digital Innovation Hubs.

One of the most urgent challenges for SMEs in the EU is to facilitate a sustainable path and ecosystem for companies to scale up and exit or proceed to an IPO with the support of European investments instead of looking to access funds from the US market. ECSO supports access to finance for European startups and scaleups. The objective is to enhance the visibility of the European cybersecurity SMEs and to strengthen the community of cybersecurity investors. Examples of this are the ECSO Cyber Investor Days, European Cybersecurity STARtup Award, and the creation of a cybersecurity investment platform. An overview of the ECSO activities for SMEs and the support to the European strategic autonomy was presented:

- European SME marketplace: creation of a European cybersecurity SME Hub where SMEs would be able to better display in a marketplace their competences and services / products as a strategic tool for the promotion of EU solutions (autonomy) in innovative sectors.

- ECSO label “Cybersecurity made in Europe” promoting the use of solutions coming from European suppliers
- ECSO Cyber Investment Days: keep companies and competences in Europe, developing specific Capital Venture investments
- Cooperation activities between Regions, Clusters and local bodies (e.g. smart cities) for accelerating the commercialisation and scaling up of the interregional innovation projects

Good practice 2: Ireland’s Cyber Security Initiative (CSI)

Carmel Somers, Board Member at Cyber Ireland & Human Capital Strategist at Technology Ireland ICT Skillnet

Carmel Somers presented the details of the Cyber Security Skills (CSI) initiative. The SME cybersecurity trends (employees are a risk due to lack of cyber security knowledge) were presented and the key strategies to address these were discussed: the cyber security skills pathway, continuous professional development and new entrants (attract and retain young people). The SME ecosystems trends (lack of cyber resources, cost being an issue) should be addressed by organic growth: broaden the skills base by fostering internal mobility within organisations.

A variety of activities are part of the CSI initiative, including:

- 5 Capture the Flag Events
- 12 Cyber Education Webinars
- 2 MSc Cyber Security Programmes
- 1 Cyber Analyst course (Future in Tech)
- 2 Cyber Essentials & 2 Intro to Cyber
- 2 Certified Cyber Risk Officer Courses
- 1 Certified Cyber Risk Specialist Course

Mrs Somers explained these initiatives in her presentation.

Good practice 3: Increasing cyber resilience in regional and sectoral ecosystems

Kim van der Veen, Account Manager at Digital Trust Center, Ministry of Economic Affairs (NL) & Fokko Dijksterhuis, Project manager CYSSEC at Schiphol Group

Kim van der Veen and Fokko Dijksterhuis presented the approach of the Digital Trust Center which enables Dutch corporations to become more digitally resilient. This initiative targets 1.7 million companies ranging from self-employed worker to SMEs and large companies. It supports these organisations by providing specific information through the access to the Digital Trust Community, and by making subsidies available to start collaboration.

The specific case of the Cyber security collaboration in the Schiphol community (CYSSEC) was presented as a successful example of regional and sectoral initiative to support SMEs. It is a local collaboration initiative which includes private companies, academic institutions and public institutions. It provides a centre of expertise with a focus on gathering, sharing and development of information and knowledge and organising cross-organisational activities and campaigns. The ambition of CYSSEC is divided into 7 work packages that build a foundation for sustainable digital resilience in the Schiphol community:

- Sharing information and knowledge: disseminate information through a website with a secured platform, newsletters and social media
- Ambassadors network: cross-organisational campaigns
- Addressing cyber at local educational institutions: incorporate cyber security in the study tracks of aviation academies
- Organising sessions with external experts on a wide range of topics such as cloud security, privacy and cyber crisis
- Hands on tools to enable SMEs to get started with increasing their cyber maturity right away
- Involving students from cyber security studies in the CYSSEC activities
- Link students to jobs and positions in cyber security in our local community

Interactive discussion

What are the specific needs and barriers that need to be addressed to help SMEs?

Key challenges concern awareness, adoption by SMEs using technology, skills shortages, access to funding and in general costs of investing in cyber resilience, mismatch in training offers, lack of understanding how to build capacity in a SME or with several SMEs together. The root-cause analysis shown in the introductory presentation gives an even broader picture.

Other remarks that were made:

- Lack of interest: 90% of the management boards are only starting to get interested in cybersecurity when they had an issue – not before.
- There is a huge lack of knowledge. We urgently need to get the importance of cybersecurity into the minds of the management boards and the owners of micro SMEs.
- Most of the CEOs think their IT administration takes care about this issue. But people need to understand that you have to separate cybersecurity from the IT administration. Because nobody can audit her/his own work correctly. So – from our point of view - we should think about some sort of EU-wide „general inspection“ for large, small and micro SMEs. (according to a German cyber-security SME)
- People need to understand that cybersecurity is a process, not a one-time purchase of a firewall, antivirus or a new backup tape. Owners and companies need guidelines how to develop those processes for their business (e.g. how are the backups monitored and are there recovery tests on a regular basis).
- When 99% of the companies are SMEs and 93% micro SMEs – we should definitively address this last group. And they definitively do not need new frameworks or ISOs: They simply need the awareness and easy access to the knowledge.

What are potential solutions or lessons learned in this regard?

The various presentations give relevant examples of solutions and lessons learned in the process.

Further to that:

- Ireland has developed some relevant methods to detect potential new cybersecurity resources (Cyber Aptitude test) which also helped to increase the number of female cyber specialists in Ireland. This was also further supported by education programmes (such as a Master programme) and fits the concept of Continuous Professional Development (CPD) very well. There is also a dedicated Women in Cyber initiative.

- ENISA is working towards a cybersecurity skills framework that could be of help to stakeholders in developing fitting education and training programmes and related skills-assessments.

- ENISA has also been organising an EU Cyber Challenge, with 25 countries and still growing towards a more global scene. Next year it will take place in Prague.

- DTC shared six lessons and challenges: cyber initiatives need to have close relationships with business, don’t underestimate the impact of knowledge sharing sessions, collaborate with existing initiatives with a target audience, think about sustainability and becoming future proof, how to measure (and demonstrate) success and tool development (co-create!)

How can different stakeholders (government, associations, education, other intermediaries) contribute?

- The Triple-Helix is essential to design and implement initiatives that should support SMEs in this challenge. Reaching SMEs is essential – not just for awareness purposes, but also to trigger them to set next steps to become more resilient.

- Besides the importance of helping cyber security SMEs, it is also key to help protect ‘user-SMEs’. Attracting and engaging them is even more challenging also because in some sectors awareness of the risks is low, and because non-digital SMEs have less knowledge in-house to advance on cyber security.

- It was mentioned by Luigi Rebuffi that it is important to work on local and regional connections.

What can be done to further improve collaboration on EU scale?

- At EU level it is pivotal to bring all different initiatives, tools, examples together in one place to increase findability and allow easy access for SMEs – as well as (and maybe even more so) for the intermediaries that are in regular contact with SMEs and can trigger them to take action. Intermediaries could be associations, chambers of commerce – but in this context also think about accountants and insurance companies.

- A suggestion was done by Carm Cachia during the discussion to include reference to the work being developed under the Digital Skills & Jobs coalition, and the Skills & Jobs Platform that is in development (by DG CONNECT; news item here).