On the evening of 5 May during its 2021 Spring General Meeting, CyberSec4Europe hosted an online panel discussion entitled *Developing SME Cybersecurity Resilience in Europe*.

Following an introduction from **Mark Weinmeister**, Secretary of State for European Affairs of the State of Hessen and **Kai Rannenberg**, Goethe University Frankfurt and co-ordinator of CyberSec4Europe, moderator **David Goodman** from Trust in Digital Life introduced the panellists:

- **Martin Übelhör** Head of Cybersecurity Industry and Innovation, DG CONNECT, European Commission
- **Annika Linck** Senior EU Policy Manager, European DIGITAL SME Alliance
- **Nicholas Ferguson** Trust-IT Services, Partner, CYBERWISER.EU; Project Coordinator, cyberwatching.eu
- **José Francisco Ruiz** Atos Spain, Technical Coordinator, Cyber-GEIGER

The goal of the evening's discussion was to explore issues relating to developing SME's awareness of cybersecurity in order to improve resilience and responses to cyber attacks which will be an important aspect of the work of the new European Cybersecurity Competence Centre in Bucharest.

SMEs account for the majority of businesses worldwide and are therefore vital contributors to job creation, innovation, and global economic development. SMEs represent about 90% of businesses and more than 50% of employment worldwide, and similarly, in the European Union, 99% of enterprises are SMEs who provide two-thirds of private sector employment. In 2018, there were over 25 million SMEs in the European Union, employing 100 million people, of which 93% were micro-SMEs, defined as having 10 or less employees.

Given the size and limited resources of most SMEs, it's not surprising that SMEs are as susceptible but more vulnerable than larger enterprises to cyber attacks. However, without effective training and support, many SMEs are not sufficiently protected or able to recover from the impact of such attacks with, in many cases, dire consequences. All SMEs are busy building their businesses - what time or resource do they have to worry about cybersecurity?

Martin Übelhör introduced the topic with insights as to what the Commission plans are to help SMEs with cybersecurity. He opened by quoting from an ENISA study from the end of 2020 on 250 SMEs in 25 Member States, which reported that 36% of respondents had experienced a cybersecurity incident in the previous five months. A large majority had very basic cybersecurity measures in place – for example anti-virus, back-ups and a firewall – but only less than 30% had more advanced measures, such has having appointed an information security officer and having a business continuity or disaster recovery plan. Some of the challenges facing SMEs were found to be awareness, budgetary and resource constraints, poor management as well as IT-related human resources, skills and expertise support, a lack of tools and so-called 'shadow IT', due to the trend for employees to use their own devices for work with their own associated third-party IT and networking services.

In terms of policy, what more can be done for SMEs? A lot of good initiatives exist within Member States: for example, in Belgium, the CCB supports SMEs with guidelines and tools, in France, ANSSI runs a portal for SMEs to report incidents, and in Luxemburg, SECURITYMADEIN.LU carry out consultancy targeting SMEs. ENISA are *inter alia* working on guidelines for SMEs as well as developing online tools for awareness and making recommendations for Member States.

How does this fit into a broader context? The Commission published its cybersecurity strategy in 2020 and there is a whole array of infrastructure measures, including a big pillar on investment which leads back to the Centre and the funding programmes, a pillar on skills as well as the Digital Innovation Hubs which the Commission is setting up in conjunction with Member States.

The regulation on the Cybersecurity Competence Network is due to be adopted and published before the end of May; ECSO, which started as public private partnership has an important role to play as do the four pilot projects, among which is CyberSec4Europe. In parallel, the Commission is both setting up the Centre in Bucharest and in the meantime handling its responsibilities, as well as setting up the National Cybersecurity Coordination Centres in each Member State – these could be powerful levers to reach SMEs which are difficult to reach.

In addition to Horizon Europe, the new Digital Europe funding programme will support the rollout of different cybersecurity projects and tools, update of best cybersecurity practices, certification targeting SMEs and skills development.

Finally, Martin remarked that there is a potentially powerful mix between the different approaches to policies and funding between DG CONNECT and the other groups within the Commission working with SMEs.

Annika Linck is from the European DIGITAL SME Alliance is a network of over 20,000 SMEs, a variety of companies most of which, roughly 90%, are in the ICT sector. In the network, as direct members, are national and regional associations which have companies associated with them at a local level. They organise working groups focussing on different areas, one of which is cybersecurity, in which SMEs and association workers develop policy positions and responses to proposals coming from the Commission.

In 2019 they carried out a study looking at the hurdles inside organisations to the adoption of cybersecurity solutions. It was apparent that cybersecurity is perceived as a cost rather than something that brings immediate benefits. There is no immediate return on investment unlike with emerging technologies such as artificial intelligence or the use of big data where there are clearly discernible benefits. It would appear that companies would only be happy that they've improved their cybersecurity level after the damage is done.

With micro-SMEs in particular, a lot of the prioritisation tasks fall on the CEO's desk, unless there is an IT person who can take care of them, but either way capacity is quite limited. One of DIGITAL SME Alliance's recommendations was to increase capacities at the organisational and individual level and raise cybersecurity awareness of the CEO's management team. Investment in training and skills is vital. The level of cybersecurity awareness training received by individual employees in large companies – 91% – compares markedly with the 58% in smaller companies.

It was suggested that awareness and training could be spread in the SME eco-systems of B2B relationships and supply chains that most SMEs operate in and, as well as working through local chambers of commerce, to use as their go-to point their insurance providers and accountants who they would visit at least once or twice a year. There are several ways of reaching SMEs, and one of them is through intermediaries.

It's important not to consider SMEs as one single type of entity with differences not only in size but also in their digital maturity, in terms of both their awareness of security issues but also the extent to which IT is part of their daily business activities. Consequently, measures have to be adapted depending on these levels of digital maturity.

Nick Ferguson works for a 50 person SME, Trust-IT Services, and is on the panel representing two projects, cyberwatching.eu and Cyberwiser.eu, both of which have developed strategies for SMEs. Trust-IT Services specialise in strategic communications particularly for funded activities and projects and dissemination services for the Horizon Results Booster, and so understand the pressures that SMEs are under and the value that the research community can bring to SMEs. These types of high-quality resources from research and innovation projects are really interesting and help multiple organisations reach their target. Trust-IT Services sees a role for itself to take project results beyond project lifetimes and so become a digital societal asset.

cyberwatching.eu, an H2020 coordination and support action (CSA), is coming to the end of its lifetime. Firstly, one of its main targets is the project community, and it has developed a "Radar", a visual representation of all projects which maps all cybersecurity projects based on a high-level (JRC) cybersecurity taxonomy as well as a self-assessment based on market and technology readiness-levels and their lifetime position. cyberwatching also provides an online marketplace where project information and results can be published, making that information as well as the individual project websites more accessible than they would be otherwise – all of which can be very useful for SMEs. The project has a number of events and online resources targeting the SME community, including the DIGITAL SME Alliance. A lightweight cybersecurity 'seal' is coming out in June, directly targeting SMEs. There is a GDPR temperature tool, an information notices tool and a risk management tool - all of which are promoted to SMEs.

Cyberwiser.eu which has just finished provided capacity building services to SMEs for the use of cyber ranges. It is understandably very difficult in getting SMEs interested in cybersecurity – sending an employee to get training on a topic which is seen as an extra is challenging. Attending training costs money and means employees are not doing what they are employed to do to further the business. It's an investment and not usually cheap.

> Questions from the audience: *"There are a lot of programmes, a lot of opportunities to get training for SMEs, that cyberwatching.eu does a good job in highlighting. Two questions: is there too much and is the lack of coordination confusing? And do we have any idea about the effectiveness of the programmes and training exercises?"*

There are a lot of resources for SMEs, and a simple Google search will reveal a lot of private companies and consultancies offering services – it's unlikely that EC-funded projects can afford Google Ads. What both projects tried to do was to collect results and showcase them in the Cyberwatching Project Radar and marketplace. Pooling these resources in one place, such as ENISA or ECSO, could be one solution. Another consideration is that these resources need to be continually updated: for example, the GDPR temperature tool needed to be updated after a year and a half because recommendations changed and need to be improved. Monitoring is also important, which is done through putting on events for their customers. The difficulty for projects is that they have a limited lifetime but a resource may stay online and go out of date which is a concern.

> Question from the audience: "*Could you explain the seal*?"

It's another awareness raising service. It's like a checklist for SMEs to get into a frame of mind around attaining certification for best practices, which typically is too expensive for an SME. Done in collaboration with SGS, it will be launched in June 2021 and beyond that the seal will be sustained by AEI on their cybersecurity innovation hub.

Question from the audience: "*Are there plans for the EU institutions to obligate SMEs to obtain lightweight cybersecurity certificates from all of their vendors and supply chain? Is this something the institutions could pick up one day?"*

Martin agreed that it is an important question, in general the Commission is careful with regulatory obligations especially on SMEs. The approach in the NIS Directive is, the more critical the entity, the more stringent the security requirement should be. It is possible for SMEs to fall under the NIS Directive and its revised form which is being negotiated. Part of the proposal is to enhance requirements on the company management to make them more attentive to the issues of security and to incentivise investment in order to avoid the situation as mentioned already that we always invest in insurance or security locks the day after the house has been burgled. Realistically, for requirements concerning all the SMEs in Europe, the Commission has to take a careful approach.

José Francisco Ruiz is from Atos and participating as technical coordinator of the GEIGER project which evolved from an earlier three-year project, SMESEC, for which José was project coordinator. Both projects aimed at working with SMEs on cybersecurity. Whereas SMESEC was oriented to technical aspects, GEIGER is focussed on both technical and awareness raising pillars – one without the other cannot be understood. It's impossible to make an SME understand cybersecurity unless they understand why it is important. Speaking about his 20 years' experience of working with SMEs in the field of cybersecurity and what he's seen in Europe, José chose to focus on two specific aspects about developing SME cybersecurity resilience in Europe. Firstly, it should be 'building' rather than 'developing', there are so many cybersecurity solutions emerging from European projects, which if you start compiling, some would be very difficult to find. So, the question is why are we still not tackling cybersecurity in SMEs? Two things that José has learnt from working with SMEs, both formally as well as informally. First of all, they don't understand the solutions: for an SME, the main critical aspect is money. Why? Because they need it to survive. That's how they see it. And when it comes to cybersecurity, they don't see it as José, a cybersecurity expert, sees it. They see something that consumes time, effort, people, resources, and it doesn't bring immediate benefits today. One very important aspect is to make SMEs understand how cybersecurity is beneficial for them. They will know how beneficial it is after they've been the victim of an attack. When did any of us change our passwords? It's easy with hindsight to say I should have paid this extra money for this solution, or that solution. But it's easy for Jose to say, he works in cybersecurity and wouldn't dream of talking about it with, for example, his parents.

If you go to an SME and tell them you've got this amazing solution that can protect your servers, your passwords, your employees, and then ask them how much are they willing to pay – 100 euros every, say, three months? To which you would have to say to them that they had no idea what you were talking about or have any idea how cybersecurity works. So, without good cybersecurity awareness, it doesn't matter how many solutions an SME is directed towards or given, if they don't understand the basics of the problem, they are not going to be attracted to properly addressing it. The difficult thing is to make cybersecurity attractive to SMEs for them to buy well and get engaged.

The other aspect is that when they see solutions, what they understand is an anti-virus or anti-malware, which is what they'll want to install in their systems. If asked whether these solutions really fulfil all their needs, they wouldn't know. But at least they would consider that they were trying and it was the best they can do. Going to the market is difficult because they don't know what best suits them or fits their needs. Are cybersecurity solutions too generic to fit their specific needs – probably. Solutions tend

to be built with large companies in mind. For SMEs, it's like killing flies with cannonballs. Not knowing or understanding why you need cybersecurity is at the core of the problem.

Finally, we, the cybersecurity community, have to make cybersecurity more day-to-day for everyone in Europe so they can understand how important it is. People only learn when something fails or goes wrong. Unfortunately for SMEs, if they are the target of a ransomware attack or similar, they would usually go out of business, and that is very scary. It also means they are not going towards digital transformation: it's safer to keep sensitive data close rather than in the cloud where it could be stolen.

The two most important aspects then are making cybersecurity attractive and understandable for SMEs and having solutions that fit their needs, not only technically but also from the point of view of performance and budget.

One of the partners in GEIGER is a hairdresser and it has been amazing talking to her about cybersecurity. It's a very different world but the goal has been how to make cybersecurity understandable for her. This translation requires a lot of effort. We are so used to the complexities of cybersecurity that when somebody says can you explain to me in a simple way for me to understand – it's tough. There is an amazing gap between the world of the experts and that of the SMEs. It doesn't matter how many solutions you throw at them you have to build these bridges.

> Question from the audience: *"Besides all the well-known names in the GEIGER project, there is also Loredana, the ladies' hairdressing salon. How difficult is it to find a non-IT organisation like Loredana and how much effort did it take for you to bring them up to speed? And, out of curiosity, how did the salon get involved in the project – did you approach them?"*

It turns out that Loredana were the hairdresser of one of the partners in the project – the best ideas are always the simplest! It was very challenging, in a good way, to get them involved. When the salon was being invited to participate in the proposal, they were asking why – they are two or three people, they have only one laptop, an Excel file, and their phones. This type of company is one of the most common in the EU. When Atos first talked to them about the need for cybersecurity in the proposal, they talked about encryption, passwords and all sorts of crazy things. Then Atos told them that they would provide them with a solution that they would only have to have minimum interaction with in the most user-friendly way. This meant that the salon could really benefit by being provided with status information and recommendations on best steps to take without having to take training courses etc. Seeing the benefit and the ease of use made it much more attractive to them. They knew bad things can happen from watching the news and were glad to have a solution to protect themselves which was going to be transparent and with minimum impact on the way they work. This was a very specific case – to reach the rest of Europe, we need a much more general approach.

> Question from the audience: *"The owner of the hairdressing salon apparently doesn't speak English that well which raises the question of language and how important it is to have materials available in local languages*."

Annika remarked that in places like Brussels where people are used to speaking in multiple languages it may not be an issue but in remoter parts of Europe this is not the case. This has come up in conversations with other associations about dealing with emerging technologies and the question came up would it be available in local languages – because if not, there would be no point, nobody would be interested.

Nick lives in Italy and admits that even in his company many of those working in IT only mastered English after a massive investment in language lessons. It's imperative that

not everything is in English, ensuring that materials are made available in local languages.

> Question from the audience: *"What do we think about cybersecurity maturity between countries or regions, and, if so, is there a particular reason for that?"*

José recounted participating in a collaborative project in Japan and found that SMEs had exactly the same problems as in Europe – difficulties accessing the market, difficult to find solutions that fit and understanding cybersecurity. Despite perceptions that Japan would have more technology experts, they were exactly the same as Europe.

Nick said that if you look regionally there are different behaviours or levels of wealth. He recalled an example of putting an alarm on your house: you don't worry if your cutlery is stolen, as long as the important things are kept safe. General cybersecurity issues don't need to be addressed, it's knowing what is important – like the hairdresser's notebook with her clients' names and addresses.

> *Question from the audience: "Over the last 15 months in the context of the pandemic, the public health campaigns have been very impressive in getting across the right messages to the public at large. In times of emergency, like during wartime or the AIDS crisis in the 80s, governments step up to the plate and reach out across the board: do we need to do something similar as radical as that for cybersecurity? Do we think that cybersecurity is a sufficient priority, given its impact on society and supply chains, for anything like that to come about? Would it work?"*

Martin came back to the need to work through intermediaries. We have to recognise the limitations of what can be done by the public sector here in Europe to reach SMEs. The Commission is relatively good at building ten supercomputers scattered across Europe but reaching out to hundreds of thousands of SMEs in their local language, one would have to set the right framework and provide resources but then to work through actors who are closer to the ground. These could take place at either Member State, regional or local levels or through certain economic functions like insurers that were mentioned. This is the philosophy behind the network of national coordination centres and the digital innovation hubs which will address digitisation more broadly and they will have more or less a regional footprint. Some will specialise in cybersecurity and others will advise SMEs in technology transfer and digitisation more broadly – and we'd want to make sure they include cybersecurity when they preach digitalisation. The importance has been recognised and the field is growing and becoming more complex and different stakeholders are getting into this policy field – which is a good thing.

> Question from the audience: *"Annika, as EU Policy Manager, are there any outstanding policies or issues that you would recommend to Martin or any of his colleagues in the Commission?"*

Annika asserted that they have been making cybersecurity recommendations on proposals on the NIS Directive and earlier than that on the Cybersecurity Act. What is important also, as has been mentioned, is to take into account different levels of digital maturity and that there are many actors at a local level. For example, local municipalities are giving training to older people not to pick up the phone when they see a strange number and not to give away their contact details or bank account number. These kinds of things are happening in the offline world through different actors - we need to look at cybersecurity more like that. This is something we all have to learn in a holistic way as we are all using digital tools in our daily lives.

One additional point is the DIGITAL SME Alliance working group has been busy translating some of the more complex standards, the ISO 27000 series for example, into

more accessible, practical guides for SMEs which we consider to be useful, not least because many of these standards are tailored for larger companies.

In conclusion, here are some closing thoughts from each of the panellists:

José noted that the Commission, cybersecurity vendors and users are at the same point in recognising the importance and that there remain outstanding issues, holes, to cover to work together and that we should keep going. It's not something that will get fulfilled in one year and should be rooted more in the core of our society because if want to achieve the goal of being digital Europe, digital companies, digital people, we need cybersecurity integrated naturally in our day to day lives.

Nick observed that within the 27 Member States, the regions are a very important gateway to different communities, likewise the network of national coordination centres. But the regions have the local knowledge of networks which are very active in their communities and probably have a high degree of trust in their regions. They understand their geographies and dynamics and can facilitate trickle-down effect of regulations and help educate their various communities.

Annika wanted to highlight three things:

- to tailor cybersecurity awareness to different maturity levels and regional differences and not look at SMEs as a single homogenous group
- to include the intermediaries in any cybersecurity considerations
- to make sure that standards are tailored or at least accessible for SMEs

Martin said that the issues have been identified, more broadly on all levels and the resources are being put in place and the structures are developing to address these issues. What needs to be achieved is awareness and then the right tools need to be made available and be diffused. Different actors at different levels of governance all have their role to play. Diffusion should take place more regionally or locally but the providing of resourcing and tools can take place at the European or national level. It's an important and evolving field and Martin would love to be back on this panel in two years' time and see how things have evolved!

David replied that, although it's not clear whether the project will still be here in two years' time, it would certainly be good to revisit and review what progress we've made in the many issues we've talked about. What is clear is that we are all in agreement about the nature of the problem, the vastness of it, how fragmented it is by language, by digital maturity, by wealth and the difficulty of reaching out particularly to micro-SMEs – why should they be interested. Working through intermediaries which was touched upon several times would seem to make a lot of sense as does the perspective of supranational, national and regional participation also makes sense. The news both good and bad is that there is a lot of work to be done. The bad news for SMEs is that there are a lot of people not being reached but for the cybersecurity community there is gainful employment for years to come driving the momentum to get the right messages out to SMEs and also the general public which is equally important. Appropriate outreach happens in the offline world but as we get more immersed in the digital world it is citizens who need to be made aware of the dangers and the malevolent actors that exist online.

See also https://cybersec4europe.eu/event/establishing-the-competence-centre-in-bucharest-and-building-the-network/ for a recording of the event.

David Goodman, Trust in Digital Life