friends of europe

EVENT REPORT

EU SMEs 2030: boosting cyber-resilience during the EU's Digital Decade Event report

01
03

Cover image credits: Unsplash © Marvin Meyer

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

Co-organised with

Google

Co-funded by the European Union

EU SMEs are vulnerable to the booming trade in cybercrime

Small and medium-sized enterprises (SMEs) are often referred to as the backbone of the European economy. They represent 99% of all EU businesses and account for around two-thirds of all jobs, but remain especially vulnerable to attacks by cyber criminals. Unless SMEs become more resilient, Europe faces a severe challenges.

In a morning debate hosted on Wednesday 1 March by Friends of Europe, policymakers, academics and industry representatives discussed what's at stake and how to ensure that Europe's economic powerhouse isn't crippled by criminals seeking to mine data or bitcoin from unsuspecting, unprepared businesses.

> *"Cybercrime is growing. By 2030, it is forecast to become a €5.5tn market*
>
> **Ivan Štefanec**, Member of the European Parliament and President of SME Europe

Recommendations

- Stem the brain drain for cyber-security engineers using either tax incentives or vouchers.
- Tap into the Recovery & Resilience Facility (RFF) to help SMEs hire the cyber-security engineers they need.
- Help SME employees avoid becoming the entry point for malicious code or the victims of phishing attacks.
- Encourage more women to become cyber-security engineers.
- Support a bottom-up drive for improved cyber-security skills generation.

"Cybercrime is growing. By 2030, it is forecast to become a €5.5tn market," said **Ivan Štefanec**, Member of the European Parliament and President of SME Europe, who listed the three main challenges that SMEs face: bureaucracy, access to capital and a lack of relevant skills.

As Europe gears up for the 30th anniversary of the creation of the single market, Štefanec pointed out its shortcomings in the area of services. There has been a raft of recent legislation in the digital domain, such as the Digital Services Act (DSA) and Digital Markets Act (DMA).

"The good news is that these laws do create a digital single market," Štefanec said,

> *While 92% of SMEs recognise the threat posed by cybercrime, only 16% of businesses feel very well prepared for a potential attack*
>
> **Karen Massin**, Head of EU Government Affairs and Public Policy at Google unveiled a new study

but he added that it is too early to evaluate them. "Everything including AI [artificial intelligence] has to fit together from a cyber-resilience perspective."

Karen Massin, Head of EU Government Affairs and Public Policy at Google, unveiled a new study. Entitled 'Europe's SMEs in the Digital Decade 2030: building cyber-resilience, overcoming uncertainty', which finds that while 92% of SMEs recognise the threat posed by cybercrime, only 16% of businesses feel very well prepared for a potential attack. The study points to the same challenges raised by Štefanec.

Roughly 43% of firms were attacked in the past year. "We've seen a 300% increase in attacks in the past year alone," Massin said. "SMEs are often the target. It's the staff who are targeted with phishing attempts. You have to protect the individuals."

The study, commissioned by Google and executed by researcher Kantar, reveals that the COVID-19 pandemic partly prompted the digitalisation of SMEs, which is helping them protect themselves. However, it also shows that only 15% to 20% of SMEs are using big data and AI. Even though digital literacy is probably the best defence, "there's a risk that SMEs may be put off digital as a result of being attacked," Massin said. "There's a lack of basic skills, and many SMEs can't hire specialists because there aren't enough of them."

"It's not enough to rely on policy tools. We can't solve this at EU level. There needs to be a bottom-up drive from universities," Štefanec added. This view sparked some kickback from the audience of roughly 60 attendees at the debate. "Our universities are good. The fact is that well-trained engineers are being lured to work for the tech giants in the US. There needs to be a tax incentive or suchlike to keep the cyber-security talent in Europe," said one attendee.

> *There's a risk that SMEs may be put off digital as a result of being attacked*
>
> **Karen Massin**

Another suggestion from the floor sparked a lot of interest: vouchers, instead of a tax incentive, issued by local and regional governments could help SMEs hire the cyber-security talent that they need. Closing the pay gap between tech giants in Silicon Valley and European SMEs would help stem brain drain, one attendee suggested.

Digitalisation is one of the priorities of the €723.8bn RRF and member states must spend 20% of their RRF share on digitalisation. "Couldn't a voucher scheme be funded from this?" asked moderator and Chief Operating Officer at Friends of Europe, **Dharmendra Kanani**.

"Vouchers would be far quicker than a tax incentive, which could take years to be felt by an SME," said **Iva Tasheva**, Co-Founder of CyEn, a cyber-security consultancy. She welcomed efforts at the EU policy level to address cyber-security challenges

> *"There needs to be a tax incentive or suchlike to keep the cyber-security talent in Europe*
>
> **Ivan Štefanec**

but said the laws simply provide a baseline. "Member states have to place SMEs in their cyber-strategies."

This view was backed up by **Christiane Kirketerp de Viron**, Head of Unit for Cybersecurity and Digital Privacy at the European Commission Directorate-General for Communications Networks, Content and Technology (DG CNECT). While EU legislation, such as the NIS2 Directive on network infrastructure security that came into effect this year, deals with larger players, "member states have to look after the small guys," she said.

Michelle Ancher, Lecturer and Researcher at The Hague University of Applied Sciences (THUAS), also focussed on the 'S' in SMEs, asking: "What about the butchers? The hair dressers?" Like bigger businesses, they too need to strike service-level agreements with their digital suppliers.

Governments should also explore the relatively untapped potential of women, who are woefully underrepresented in the field of computer science. "There are women out there doing tech jobs. If this was more visible, it would attract more female talent," concluded Tasheva.

> *"Member states have to look after the small guys*
>
> **Christiane Kirketerp de Viron,** Head of Unit for Cybersecurity and Digital Privacy at the European Commission Directorate-General for Communications Networks

Friends of Europe
Connect. Debate. Change.

+32 2 893 98 23
info@friendsofeurope.org
friendsofeurope.org

Friends of Europe is a leading think-tank that connects people, stimulates debate and triggers change to create a more inclusive, sustainable and forward-looking Europe.