Interview with Erlend Gjære

We have had the honor of interviewing Erlend Gjære, a renowned cybersecurity specialist and ambassador for the European Digital SME Alliance.

With a solid professional background, Erlend has dedicated his career to addressing the challenges of digital security and promoting technological transformation in Europe.

Drawing from his experience in Norway, one of the leading countries in innovation and digitalization, Erlend has worked on developing advanced cybersecurity solutions, helping companies, institutions, and citizens protect themselves against the growing threats in the digital environment.

We are confident that his expertise and knowledge will provide us with a unique and valuable perspective on the challenges and opportunities of cybersecurity and digitalization in Europe. Welcome, Erlend!

Erlend, your professional profile in cybersecurity is impressive. What led you to specialize in this field, and what were the biggest challenges you faced at the start of your career?

I've always had a passion for people and cyber security, and the combination of those two in particular. Having started my career as a research scientist within the field, I was drawn towards helping my 2000 colleagues with security awareness and training, internally at the research institute I worked at. Learning first hand how different people are, in backgrounds, interests and across 70 nationalities – I got to really understand why there is not one single solution to help them all, and why more security innovation is needed. So in 2017, I founded Secure Practice, learning also how to build and scale a technology company, which again introduced a whole new set of challenges.

Secure Practice
QEHVB
Lotte skrur på PC-en og logger inn
Men hun rekker knapt å åpne mail og nettleser før PCen går i stå, og slutter å respondere.
Dere skal akkurat til å tvinge av strømmen, når følgende bilde komme opp på skjermen:
"Ooops! Your files have been encrypted"

As an ambassador for the European Digital SME Alliance, how do you see the role of cybersecurity in the process of Europe's digitalization? What challenges do you identify in this context?

Europe needs resilience on many levels, and with the digitalization leaps we're making, cyber resilience is essential to our overall resilience as a society. We need to protect our innovations, our companies and our citizens to be competitive in a global context, while the threats we're facing are also digitalized and not bound to physical borders. There are still large gaps to be filled in both basic and advanced digital skills for us to succeed in the fight against cybercrime, which is a matter to everyone these days. So I'm happy to voice this need and agenda among and on behalf of fellow European SMEs also as an ambassador.

How does your role as a digital ambassador contribute to advancing cybersecurity and digital transformation in Europe?

The ambassador role is a way to represent not only ourselves, but European SMEs in a broader sense. Being one such SME ourselves, building digital solutions for cybersecurity, yet also as part of the ecosystem and supply chain facing the same challenges that so many other companies face, allows us to understand and connect better with others, for better innovation, collaboration and impact in society.

What is the European Cybersecurity Centre (ECCC), and what are its main objectives?

The ECCC mission is to help increase the global competitiveness and high standards of the EU's cybersecurity industry, turning cybersecurity into a competitive advantage for EU industry. As a beneficiary of ECCC ourselves, through the DIGITAL Europe programme, Secure Practice receives financial support to scale our award-winning concept of national cyber exercise tours, which has so far trained 5000 cyber preparedness professionals across Norway and Denmark in 2024. We are now looking for national partners in other countries, too – so please reach out if interested!

Can you clarify the concept of cyber resilience and explain why companies need it?

Cyber resilience goes beyond prevention to include both incident response and recovery, and maintaining business continuity during a cyber attack. And the last part here makes resilience truly a management responsibility, seeing how operations depend on digitalized systems which may be adversely affected. The recent Network and Information Security Directive (NIS2) brings extra attention to resilience, also in supply chains, so also in terms of regulatory compliance, there are so many companies now which have a legal obligation to simply be resilient.

Artificial intelligence is transforming both defense and attacks in the field of cybersecurity. What role do you think AI plays in the fight against cyber threats?

Just like you point out, AI is available do to both good and bad. There are so many cybersecurity tasks which can benefit from automation, and AI – freeing up human effort for higher value tasks, which I suppose also the cybercriminals are doing. There is no doubt we need AI to keep up with our defenses, just like there is no doubt we still need people to plan, prioritize and relate cybersecurity to the people in the organization. It is really a matter of automating what can be automated, so we can focus better on the rest.

If you could share a key message with European companies and citizens about the importance of cybersecurity and digitalization, what would it be?

Cybersecurity today is essential to every company, and to every citizen, because we are all citizens in a digitalized society. We know that most people learn primarily about cybersecurity at their workplace, so companies investing in cybersecurity skills will both protect their company and protect their own employees from harm. And by giving cybercriminals a bad time in business, we can together make better business in Europe, too.