Last call for securing Europe's digital defences

By EDIMA

Non-harmonized approach to cybersecurity threatens to undermine the Digital Single Market.

Exactly eight years ago, computer networks in one of Europe's most "wired" countries were making headlines for all the wrong reasons. In spring 2007, a wave of cyber-attacks crippled Estonia's banks, media outlets, government ministries, and the national parliament. As the sites subject to attack grew into the hundreds, the Estonian government was forced to block all international web traffic, effectively cutting off the country. It was deemed one of the first attacks of its kind on a nation state.

The sheer scale of the incident was enough to make Europe sit up and take notice. It highlighted how even the most digitally advanced of nations are not immune to cyber-attacks and reinforced the fundamental need to protect the digital connections which have become integral to our daily lives.

Estonian policy-makers responded quickly to the events of 2007. By the next year, a national cybersecurity strategy was in place and NATO's Cooperative Cyber Defence Centre of Excellence had installed itself in the Estonian capital of Tallinn. The country is now considered to be a paragon of consistent, coordinated and comprehensive cybersecurity.

But Estonia is the exception, not the rule. Most other countries have been slower to act, as highlighted in the BSA's recently published EU Cybersecurity Dashboard, and even in those countries which have taken steps to shore up their digital defences, approaches vary significantly. Some member states have opted for sector-specific measures or formalized public-private partnerships, while others have focused instead on developing their emergency cyber response capabilities.

While it's encouraging to see countries working towards the development of cyber resilience, the different ways of going about this could backfire. 28 member states each developing and implementing their own cybersecurity policies in isolation means 28 different rationales, informed by 28 sets of social, economic and political motivations. This silo mentality risks Europe becoming a cybersecurity patchwork and, in the worst case scenario, it could undermine Europe's overall cyber resilience.

In our borderless digital economy, Europe's cyber defences are only as strong as their weakest link. And without a common foundation, these defences could crumble under attack.

To prevent this from happening, we need to establish a common baseline for cybersecurity in Europe, rooted in a common agreement on what matters most. This should be the fundamental principle underpinning the European Commission's proposal for a Network and Information Security (NIS) Directive, which is about to enter final negotiations between the Commission, Parliament and Council. Unfortunately there are several outstanding elements within the draft Directive which mean that it is unlikely to have the desired effect.

For instance, the draft Directive calls for a long-list of open-ended services, including internet enablers or "digital platforms", to fall under its scope. But this is based on the incorrect premise that all services are equal and should be subject to the same kind of cybersecurity protection.

Take the risk to Europe's critical infrastructures – which include our energy, transport and power systems. Most of these essential services are quickly becoming digitized. This delivers innumerable benefits, not least the ability to control large-scale systems, run real-time data analysis and create seamless connections between multiple different systems, all at the flick of a switch. But this same level of convenience creates risks. One flaw in the cyber defences of a national power grid or a city's public transport system can expose vulnerabilities ripe for exploitation.

This is not a theoretical abstraction. A well-organized, coordinated cyber-attack on any of Europe's critical infrastructures could have a highly damaging impact on individuals, communities and whole societies, as highlighted recently by the European Network and Information Security Agency (ENISA). With the lights out, the power off and the transport systems at a halt, Europe would be paralyzed.

While every individual should be protected from malicious cyber activity when online, defending a whole continent against cyber-attacks demands a clear prioritization of what services are most at risk. The critical sectors that Europe relies on to keep running should be at the top of the list. This is even more crucial when you consider that most of Europe's cybersecurity authorities are still in their infancy. By trying to cover too much ground with limited and emerging resources, we run the risk of Europe becoming a "jack of all trades, but master of none".

This is not helped by the fact that, under the current proposal for the NIS Directive, the final decision over what constitutes "essential services" will be made at national level, according to the principle of "minimum harmonization". For classic critical infrastructures this is not so problematic, as most energy providers or water companies tend to operate in only one Member State. But so-called "internet enablers" typically provide services across the European Union. Should these services be included within the scope of the Directive, the principle of minimum harmonization means they would face a whole host of varying regulatory approaches applying different security baselines and standards which could potentially conflict with one another. Not only will this add to the bureaucratic complexities of operating a digital service across the EU and increase regulatory costs, it might actually also undermine cybersecurity.

This non-harmonized approach threatens to undermine the European Commission's ambitious plans for a Digital Single Market. As highlighted byEuropean Commission Vice-President Andrus Ansip, the key to unlocking Europe's digital potential, to drive growth, jobs and global competitiveness, is breaking down barriers between EU member states, so the digital world is not limited by analogue borders. But different applications of what constitutes an "essential service", or potentially conflicting national requirements for standards governing operators, are unlikely to encourage cross-border digital growth and economic development.

The broad scope of the draft Directive will not only increase costs for national cybersecurity authorities and tie up their limited resources, but it is also unnecessary. Governments and digital platforms already collaborate on protecting European cyberspace, through the sharing of best practices, the voluntary exchange of information, and a mixture of formal and informal cooperation agreements. Many classic critical infrastructures, in the process of digitizing legacy industrial control systems, are only beginning to identify cybersecurity risks to their businesses. The NIS Directive should therefore focus first and foremost on operators whose services would pose a risk to European citizens' security if compromised by a large-scale cyber-attack.

When it comes to cybersecurity, governments, businesses and individuals are often reluctant to embrace new technologies, for fear of the potential safety repercussions. What is often overlooked is how such technologies can actually reinforce Europe's cyber resilience.

Cloud computing for instance, has been identified by the OECD as having the potential to reduce cyber vulnerabilities, through enhanced, cheaper and easier

access to data control. Estonia has again shown itself to be ahead of the curve on this front. The 2007 cyber-attack could well have brought the country's digital transformation grinding to a halt. But it had the opposite effect. Estonia is now not only a cybersecurity leader, but it is turning challenges into opportunities, having last year become one of the first EU member states to test the resiliency benefits of moving government services to public cloud.

Such solutions are a key part of making the most of cyberspace and mitigating potential risks. But this innovative approach to technology must be underpinned by a strong policy foundation, in the form of a harmonized, coherent and effective framework for European cybersecurity. If done right, the NIS Directive is such an opportunity.

The information and communications technology sector recognizes the importance of playing our part and we remain committed to building a safe, trusted online environment for all European citizens. But only a risk-based approach, focused on what is truly critical, and further alignment of different national positions will allow us to take significant steps towards achieving the vision of a secure and trusted Digital Single Market for every European individual, business and government.

By EDiMA
www.edima-eu.org