FMBusinessDaily

Can DORA stand up to a $10T cyber damage threat?

3 years ago

Insight from Monica Oravcova, Co-Founder and Chief Operating Officer of Naoris Protocol

Effective regulation of the digital arena can be compared to our ever-expanding universe, just when we think we have figured it all out, we discover another black hole or a 9th planet. Navigating the protection of consumers, businesses and infrastructures in this space is a moving target.

Given the growing number of cyber-attacks, potentially causing a massive $10 Trillion cyber damage headache by 2025, governments have had to appoint a myriad of task forces to ensure that financial entities such as banks, insurance companies, exchanges and investment firms, are not only resilient to severe operational disruption from a cyber-attack, but they employ measures that ensure partners and clients are also protected.

To this end the European Council has put into place regulation that seeks to manage and mitigate the ever-increasing threat from hackers and bad actors. The Digital Operational Resilience Act (DORA) has prescribed a set of requirements for the security of networks and information systems of entities operating in the financial sector, as well as 3rd parties that provide ICT services to them. In addition to addressing traditional financial institutions, it also covers digital assets that will be further regulated by the Markets in Crypto-Assets Regulation (MiCA) next year. Organisations need to be able to withstand, respond and recover from the impact of ICT incidents, and continue to deliver critical functions with minimal disruption for customers and for the financial system as a whole.

Cybersecurity regulation is not a simple task as there are many moving parts and players in the field, each requiring their own set of rules while ensuring that there are no contradictory elements in the various pieces of legislation. To effectively navigate global cybersecurity, stakeholders are going to have to collaborate on a massive scale.

Does it go far enough? Obviously DORA has to address a number of challenges, especially when it comes to integration with regulators and businesses. According to numerous research sources, humans are responsible for between 85% and 95% of data breaches, the majority of which are through emails. So it makes sense that the DORA legislation focuses on phishing and email scams. DORA will require that ICT suppliers used by Financial Services companies have the policies and processes in place to meet regulations. It sets a benchmark for organisations globally to look to improve their digital operational resilience and business continuity planning.

However there is a lack of clarity in the regulation, for example, it does not mandate how much companies should aim to spend on cybersecurity. There is also not a lot of clarity on what methods should be employed in order to achieve a higher capability of threat mitigation.

It talks a lot about traditional cyber security solutions, but they have not been successful at mitigating risk. While approaches like the cybersecurity mesh, have been recognised and championed as the latest trend by Gartner, the narrative is still around centralised solutions that by default inherit multiple points of failure. In contrast, a decentralised cybersecurity mesh removes single points of failure as it protects all devices no matter where it lives in the connected universe of IoT and networks. It protects devices in real time from cyber threats and associated risks, while enforcing CyberSecurity standards across the entire digital infrastructure. This leading edge solution is not yet being discussed by the authorities and thought leaders in the cybersecurity space. Naoris Protocol is developing this decentralised hyperstructure as a real solution to the current failings in the current cybersecurity ecosystem.

Naoris Protocol creates real time Zero Knowledge proofs/reports of the cyber-status of all devices, networks and environments, using Swarm AI and blockchain technology. The proof of the state of security at a specific point in time will be demanded by auditors and businesses, as well as possibly used as forensics data in court. It is designed to run in tandem and compliment existing cybersecurity systems.

Although we welcome DORA as a big step in the right direction, there is always the fear that regulation will stifle innovation. It may create a checklist culture amongst companies, who feel they are compliant but fail to address the biggest issue – the lack of integration of a cybersecurity mindset amongst all its employees, rather than just leaving the IT team to defend the borders. Until we move away from creating reaction-based regulation to proactive solutions that mitigate risk, we will continue to be one, or many steps behind the cybercriminals.