Impact of the conformity of the NIS2 Directive on the competitiveness of an undertaking 1/19/25

Director, IT Consulting, PwC Latvia
Dr.dat. Baiba Apine

NIS2 (Network and Information Security Directive) is a European Union (EU) directive aimed at strengthening cybersecurity across the EU, particularly concerning critical infrastructure and essential services. In Latvia, this directive has been transposed into national legislation by the adoption of the National Cybersecurity Law (NCL). Right now, companies should have clarity about their status (whether NCL subject or not) and should have registered by 1 April 2025, at the National Cybersecurity Centre (NCC). Organisations are due to appoint a cybersecurity manager and submit their first self-assessment report by 1 October 2025 and begin reporting cybersecurity incidents from 1 July this year.

The Digital Trust – 2025 survey, conducted by PwC, included over 4,000 business and IT executives from 77 countries and focused on cybersecurity. Only 2% of executives believed their companies had taken sufficient measures to ensure cyber resilience. Fewer than half of the respondents said their cybersecurity leaders were involved in strategic planning or in preparing reports for company management. This highlights a clear gap between words and actions when it comes to cybersecurity.

The NIS2 Directive aims to legally require approximately 100,000 companies across the EU to strengthen their cyber resilience, enhance the role of the cybersecurity officer within the company, and reduce threats. In Latvia, the NCL would apply to around 1,500 companies; currently, about 600 companies have begun registration with the National Cybersecurity Centre (NCC).

The introduction of NIS2 and NCL is certainly not a step towards cutting red tape. The introduction of requirements will increase the administrative burden on businesses due to the need for cyber risk policies, procedures for identifying and reporting incidents, and a plan to ensure continued operation. However, the law requires a change in the attitude of business executives toward cybersecurity. Enforcing NIS2 requirements will improve cyber resilience, yet will not guarantee full protection from incidents. For example, incident response and business continuity plans help businesses recover quickly from cyber threats. Companies will be better positioned for partnerships and access to the EU market, improving the protection of their systems, reducing the risk of expensive data leaks and downtime, and boosting customer loyalty.

Compliance with the requirements of the NIS2 Directive is an important step in strengthening corporate cybersecurity, and its implementation requires the active participation of all stakeholders. While administrative burdens may cause difficulties, companies that have successfully implemented the requirements of the NIS2 Directive will be better prepared for future cyber threats and able to remain competitive in the EU market.