FONDAZIONE BRUNO KESSLER
MAGAZINE

From compliance to resilience: how digital security is evolving in businesses

March 25, 2026

With support from InnovAction, the case of Tecnoenergia Srl addresses the challenges of the NIS2 Directive from both a strategic and operational perspective

For companies operating in critical sectors such as energy, strengthening digital security is now a strategic priority as well as a regulatory requirement. As part of the InnovAction project, in the final months of 2025, an important collaboration took place between the Cybersecurity Center of Fondazione Bruno Kessler (FBK) and Tecnoenergia Srl—an Italian company based in Trento specializing in services and solutions for the energy and infrastructure sector. The company operates in the **management, maintenance, and remote monitoring of energy systems,** with a particular focus on hydroelectric plants and renewable energy production systems.

InnovAction is an initiative co-funded by the Italian Ministry of Enterprises and Made in Italy (MIMIT), aimed at building a European Digital Innovation Hub to support companies in their digital and green transformation. Specifically, Fondazione Bruno Kessler, through its Center for Cybersecurity and Center for Digital Industry, has offered “Test Before Invest” services across various operational areas, as outlined in the catalog available here. In the case of Tecnoenergia, the engagement went beyond a simple pilot test, evolving into a structured process for defining and validating security governance processes. The primary objective was to prepare the documentation and procedures needed to plan the company’s future compliance with the **NIS2 Directive**—not only from a regulatory standpoint but also operationally—while taking the opportunity to strengthen its overall security posture.

The NIS2 Directive was approved by the European Union in 2023 and represents an evolution of the previous NIS Directive issued in 2016. Its main goal is **to raise the level of cybersecurity across Europe by harmonizing rules to reduce risks related to cyberattacks, data breaches, and disruptions to essential services.** The updated NIS2 significantly broadens its scope, covering not only critical sectors such as energy and transport, but also industries such as manufacturing, food production, waste management, and public administration. For a company managing essential services like the 24/7 remote monitoring of energy production systems,

compliance with NIS2 is **not just a regulatory obligation—it is a key step toward ensuring operational continuity and resilience.**

From risk Analysis to strategy

The starting point of the process was mapping **strategic assets** and conducting a corresponding risk assessment. In the context of cybersecurity and operations, assets are defined as all resources, technologies, information, and infrastructures that contribute to an organization's functioning and value. These may include hardware, software, data, business processes, human resources, and any elements that support operations and business continuity. Before defining any countermeasures, the working group conducted an in-depth analysis to identify vulnerabilities within both IT and OT infrastructures. This phase brought to light latent critical issues that, if overlooked, could have compromised the entire value chain. The analysis differentiated between "acceptable" and "unacceptable" asset risks. Acceptable assets were those with residual risk within the company's tolerance thresholds, while unacceptable ones presented vulnerabilities requiring priority mitigation. This provided Tecnoenergia's leadership with a clear picture of intervention priorities. Only with this understanding of the attack surface was it possible to develop the documentation required for NIS2 compliance, such as the Incident Response Plan and the gap analysis against the ISO 27001 standard.

Integrating operations and compliance

The main challenge was aligning the needs of a dynamic company with the rigidity of regulatory requirements. The issue effectively became an exercise in management engineering: integrating the speed of business operations with formal security protocols. The project addressed this need not only by identifying technical risks, but also by defining roles and responsibilities at critical decision points. The adoption of the RACI matrix—a widely used project management tool—helped eliminate role ambiguity by assigning clear responsibilities for each security process. At the same time, to mitigate external risks, the Kraljic model was applied to supply chain security, enabling the classification of suppliers not only by cost but also by their strategic impact on business resilience.

A common ianguage

The greatest challenge that emerged from the field experience was aligning different languages and perspectives. The company's pragmatic approach—focused on solving immediate operational issues—often had to be aligned with the level of formalization required for NIS2 compliance. Conversely, abstract concepts such as "residual risk" or "management maturity" needed to be translated into concrete actions to produce a tangible impact on the company's security posture. The key to success was the ability to adapt mutually—bringing regulatory requirements into alignment with day-to-day business realities. The result is a governance framework that does not slow down operations, but instead **supports and strengthens them while reducing exposure to legal and operational risks.**

Value for the local area

For the Center for Cybersecurity, the project provided an opportunity to apply advanced risk management methodologies in a real critical infrastructure context, validating theoretical models in practical IT/OT integration scenarios. For the company, the added value goes beyond having a

solid foundation for compliance documentation. Tecnoenergia now has a defined strategy and roadmap to achieve a “managed maturity” level within the NIS2 timeline.

PERMALINK

https://magazine.fbk.eu/en/news/from-compliance-to-resilience-how-digital-security-is-evolving-in-businesses/

TAGS

- #cyberattacchi
- #cybersecurity
- #digital innovation
- #digital transformation
- #digitalindustry
- #energia
- #energy
- #green
- #idroelettrico
- #innovaction
- #mimit
- #renewable energy
- #risk management

AUTHORS

- Martina Cicaloni