ERMIS

Newsletter

July 2026 - Issue No 7

In this Issue

SMEs Under the Spotlight

Rising Exposure in a Digital Economy

Small and Medium-sized Enterprises (SMEs) form the backbone of modern economies, yet they are increasingly exposed to a rapidly evolving cyber threat landscape. As digitalisation deepens, SMEs face growing vulnerabilities, often without the resources or expertise available to larger organisations. Evidence suggests that cyber incidents are now a leading cause of operational disruption and data loss, with potentially severe consequences, including financial damage or even business failure.

The Challenge of Prioritisation

Despite these risks, cybersecurity is frequently not prioritised within SMEs. Limited budgets, competing operational demands, and a lack of in-house expertise mean that many businesses adopt a reactive rather than proactive approach. Cybersecurity is often viewed as an abstract or secondary concern, overshadowed by immediate business needs such as payroll, tax obligations, or business growth.

The Role of Cyber Insurance

Cyber insurance has emerged as a complementary tool to support cyber risk management by covering financial losses associated with incidents such as data breaches and business interruption.

However, adoption among SMEs remains low. This is not because SMEs dismiss its value entirely, but due to a complex mix of factors, including limited awareness, perceived high costs, and uncertainty regarding benefits.

Perception Gaps and Misconceptions

A key challenge lies in how SMEs perceive cyber risk and make decisions related to insurance. Many underestimate their exposure, often believing they are "too small to be targeted," despite evidence that SMEs are frequently exploited due to weaker defences. This perception is further reinforced by reliance on third-party service providers, leading to misunderstandings about responsibility and risk ownership.

Barriers in Decision-Making

Decision-making is also influenced by structural and behavioural barriers. Complex insurance policies, technical jargon, and unclear coverage terms create confusion and reduce trust in insurers. SMEs often rely heavily on brokers or external advisors, while at the same time questioning their impartiality. Additionally, financial trade-offs play a critical role, with investment decisions frequently favouring immediate operational needs over longer-term risk mitigation.

Insurance as a Catalyst for Security

Importantly, the process of obtaining cyber insurance can itself drive improvements in cybersecurity practices. Requirements imposed by insurers — such as risk assessments, implementation of controls, and compliance with standards — often act as catalysts for strengthening organisational resilience.

However, this impact varies depending on the maturity of the SME and the structure of the insurance product.

Enablers for Better Adoption

To improve SME engagement, several enablers are highlighted: targeted awareness initiatives, simplified and transparent insurance products, financial incentives, and the development of user-friendly tools to assess cyber risk. Collaboration between insurers, policymakers, industry bodies, and service providers is also critical for bridging knowledge gaps and building trust.

The Role of DEP-ERMIS

Initiatives such as the DEP-ERMIS project directly address these findings and become particularly relevant. By fostering structured awareness, providing practical tools, and supporting SMEs in aligning cybersecurity with risk management strategies, such efforts address the exact gaps identified in SME perceptions and decision-making. In doing so, they not only enhance resilience at the organisational level but also contribute to strengthening the overall cybersecurity posture of the wider ecosystem.

By George Kittes, NCSA

Reference:

Adriko, R., & Nurse, J. R. C. (2026). *Cybersecurity and cyber insurance for Small to Medium-sized Enterprises (SMEs): Perceptions, challenges and decision-making dynamics*. Computers & Security, 163, 104818.
https://doi.org/10.1016/j.cose.2025.104818

5th Plenary Meeting

The DEP-ERMIS Consortium held its 5th Plenary Meeting on July 1st and 2nd, 2026, hosted by ZELUS in Athens, Greece.

Over two productive days, all partners came together to review the project's progress, discuss ongoing technical and implementation activities, and align on the key priorities and next steps. As DEP-ERMIS enters its final months, the meeting provided an important opportunity to address pending actions, strengthen coordination across the Consortium, and ensure that all activities remain on track towards the successful completion of the project.

With the final phase of DEP-ERMIS now underway, partners continue their close collaboration, focusing on the successful delivery of the project's results and the achievement of its objectives.

Technical Event

As part of the second day of the 5th Plenary Meeting, DEP-ERMIS organised a two-hour stakeholder event focusing on the cybersecurity and cyber insurance landscape and the ERMIS Marketplace.

The event started with a focused discussion, with the participation of three with the participation of three end users representing potential cyber insurance clients, cyber insurance providers, and cybersecurity solution providers, on the current needs and challenges of the market, perceptions of cyber risk and cyber insurance, and the factors that influence the adoption of cybersecurity and insurance solutions. The participants shared their experiences and views on the current cyber insurance market, as well as their thoughts on the potential value and challenges of combining cybersecurity assurance and insurance services.

Following the discussion, the DEP-ERMIS project was presented, including its main objectives and progress so far. The core concept and key features of the ERMIS Marketplace were also introduced, with a particular focus on the combination of cybersecurity assurance tools and cyber insurance services within an integrated offering.

The event provided valuable feedback and insights, which will contribute to the further development of ERMIS and help ensure that the project's solutions address real market and business needs.

ERMIS Article in the Cyber Defence Magazine

Defence Magazine Article

<u>Summary</u>

The DEP-ERMIS project was featured in the May issue of Cyber Defense Magazine with the article "Why Cyber Insurance & Cyber Assurance Matter More When Considered Together." The article discusses why cyber assurance and cyber insurance should be considered together, showing how this combination can improve cyber risk assessment, support better decision-making, and help organisations build a stronger security posture.

<u>Importance and Impact</u>

The publication helped increase the visibility of the DEP-ERMIS project and its objectives among the cybersecurity community. It also supported the project's dissemination activities by promoting the importance of combining cyber assurance and cyber insurance as part of a more effective approach to cyber risk management.

By Elli Alimperti, Zelus

Contact	Project Coordinator	Zelus	Inquiries	info@dep-ermis.eu

Disclaimer

This project has received funding from the European Union’s Horizon 2020 Research and Innovation program under grant agreement No 101128013.

The project is supported by the Ministry of Digital Governance of Hellenic Republic and the National Cyber Security Authority and is aligned with the Hellenic Cyber Security Strategy.

Consortium Partners