ERMIS

Newsletter

November 2025 - Issue No 5

In this Issue

How Cybercrime Redefines Corporate Risk

In recent years, the global business landscape has been shaken by an unprecedented surge in cyberattacks and data breaches. From retail and luxury fashion to technology and sportswear, these incidents have exposed critical vulnerabilities in corporate infrastructure, compromised sensitive customer data, and inflicted significant financial and reputational damage.

One of the most consequential breaches occurred in April 2025, when British retailer Marks & Spencer was targeted by the cybercriminal group known as Scattered Spider. The attackers infiltrated M&S's systems by exploiting stolen Active Directory password hashes and deployed ransomware across VMware ESXi hosts, severely disrupting the company's online operations. The financial impact was substantial, with M&S reporting a £300 million reduction in operating profit and a 40 percent decline in online fashion and home sales. The company's market value fell by £1 billion, and customer data—including names, email addresses, and birthdates—was compromised. In response, M&S accelerated its digital transformation initiatives and filed a £100 million insurance claim to mitigate the damage.

In the luxury sector, the French conglomerate Kering, which owns brands such as Gucci, Balenciaga, and Yves Saint Laurent, confirmed in September 2025 that it had suffered a significant data breach earlier in the year. The attack, attributed to the hacker group Shiny Hunters, reportedly compromised data linked to 7.4 million customers. The stolen information included names, email addresses, phone numbers, postal addresses, and purchase histories. Although no financial data—such as credit card or bank account details—was exposed, the breach underscored the vulnerability of high-end brands to cyber threats.

Adidas, the global sportswear manufacturer, faced a different type of threat in 2024. The company experienced a series of credential stuffing attacks, where cybercriminals used previously leaked passwords to gain unauthorized access to customer accounts. While the breach did not result in large-scale data theft or operational disruption, it highlighted the persistent risks associated with password reuse and the importance of implementing multi-factor authentication and user education.

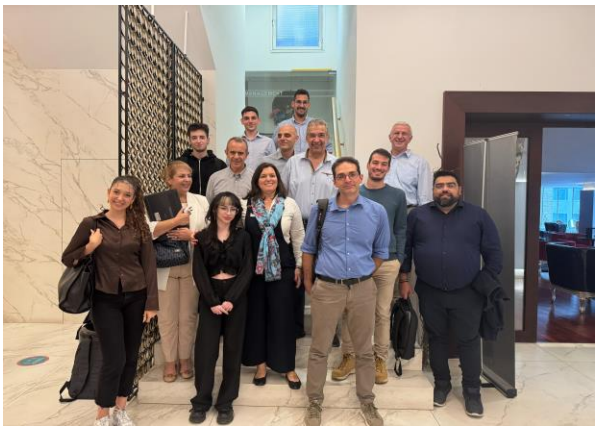
Technology giant Google was at the center of one of the largest password-related incidents in history. In June 2025, cybersecurity researchers uncovered a colossal leak involving 16 billion login credentials scattered across 30 exposed databases. These records included usernames and passwords for major platforms such as Google, Apple, and Facebook. The data originated from infostealer malware and credential-stuffing compilations, making it a blueprint for mass exploitation. Although Google clarified that its systems were not directly breached, the leaked credentials put millions of Gmail accounts at risk of takeover, phishing, and identity theft. Google urged users to change passwords immediately and adopt stronger security measures such as two-factor authentication and passkeys, emphasizing that passwords remain inherently vulnerable to theft and misuse.

The financial and reputational costs of these cyberattacks are staggering. Beyond immediate losses, affected companies face regulatory scrutiny, potential litigation, and erosion of consumer trust. These incidents have underscored the necessity for organizations to treat cybersecurity as a strategic imperative rather than a technical afterthought. Investments in zero-trust architectures, real-time threat detection, and comprehensive incident response plans are no longer optional—they are essential. Moreover, the human element remains a critical vulnerability. Many breaches are facilitated not by technological flaws but by social engineering and user error. As such, employee education and awareness must be integral components of any cybersecurity strategy.

These cases illustrate the escalating financial and reputational impact of cyberattacks on global enterprises, reinforcing the urgency for adaptive risk management and insurance solutions. Such incidents demonstrate that static questionnaires and traditional underwriting cannot keep pace with dynamic threat landscapes. ERMIS directly addresses these challenges by operationalizing real-time risk assessment, certification readiness, and evidence-based insurance models. Through its Dynamic Risk Model, Asset and Threat Mapping, and Risk Profile Valuation, ERMIS enables insurers to move beyond reactive coverage toward proactive, data-driven policy adaptation. By integrating periodical monitoring and claims analytics, ERMIS ensures that insurance contracts remain aligned with actual exposure, mitigating the severe financial shocks and trust erosion described in the article. In essence, ERMIS transforms cybersecurity from a technical safeguard into a measurable business resilience strategy, bridging the gap between assurance and insurance in an era of pervasive cybercrime.

By Vasilis Kakariaris,

Karavias Underwriting Agency

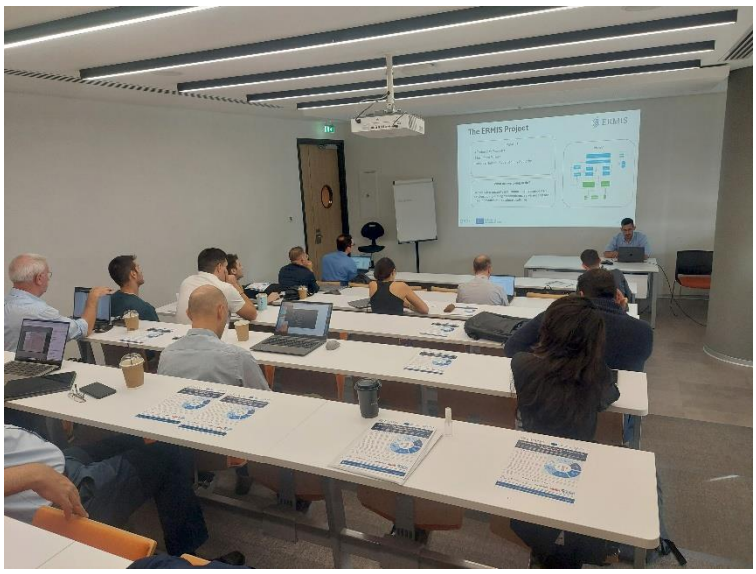


3rd Plenary Meeting

The Consortium held its 3rd plenary meeting in Nicosia, Cyprus on October 21st and 22nd, 2025. All partners came together to review progress, align strategic objectives, and ensure strong coordination across all Work Packages. The meeting served as an important opportunity to assess ongoing developments and prepare for the next phase of project implementation.

Looking ahead, the 4th plenary meeting will be hosted in February in Heraklion, Crete, Greece by Sphynx Hellas, where partners will continue to advance efforts and strengthen collaboration.

Cybersecurity Awareness & Assurance Workshop



On October 21st, 2025, the ERMIS Project, in collaboration with SecAwarenessTruss, held the workshop *"Bridging Cyber-Risk Awareness & Assurance"* at the European University of Cyprus.

The event brought together participants for an engaging showcase of the two pertinent initiatives.

Attendees were introduced to advances in cyber-range training for critical infrastructures, followed by an overview of the ERMIS marketplace and its role in supporting assurance and insurance services for organizations. The session featured demonstrations, pilot insights, and an open discussion that highlighted how these two EU-funded projects complement each other in strengthening cyber-resilience across sectors.

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