2026 IEEE CSR Workshop on Cyber Range, Insurance, and Risk Management: Enhancing Cyber Resilience(CRIRM)

Call for Papers

Important dates

Paper submission deadline:
April 13, 2026
Authors' notification:
May 4, 2026
Camera-ready submission:
May 25, 2026
Registration deadline (authors):
May 25, 2026
Workshop dates:
August 3–5, 2026

Workshop chairs

Dr.Michalis Smyrlis (GR)
Dr. Georgios Spathoulas (NO)

Organizing committee

Dr. Nikos Nikoloudakis (GR)
Dr. Panagiotis Bountakas (CH)
Dr. Eliana Stavrou (CY)
Dr. Emmanouil Vergis (GR)

Technical program committee

Dr. Konstantinos Votis (GR)
Dr. Karld Waedt (GER)
Romarick Yatagha (GER)
Ndeye Gagnessiry Ndiaye (GER)
Dr. Muhammad Mudassar Yamin (NO)
Notis Mengenidis (GR)
Evangelos Floros (GR)
Dr. Dimitris Deyannis (CH)
Dr. Andriani Piki (CY)
Dr. George Alexandris (GR)
Michail Koniotakis (CY)
Dr. Vasilis Tountopoulos (GR)

Publicity chairs

E.Alimperti (GR)

Contact us

smyrlis@sphynx.ch
georgios.spathoulas@ntnu.no

Over the years, cyber threats have increased in both volume and sophistication, with adversaries employing a diverse arsenal of tools and tactics to target victims for motives ranging from intelligence collection to financial gain or destruction. The integration of advanced technologies, such as **cyber ranges for simulated and emulated training**, the evolving **cyber insurance landscape**, and robust **risk assessment and management strategies**, has become critical in navigating this increasingly complex threat environment. Effective cyber resilience today requires a multidisciplinary approach, integrating **simulated training through cyber ranges**, **strategic cyber insurance adoption**, and **innovative risk management techniques** that collectively improve preparedness and response capabilities.

CRIRM aims to spotlight cutting-edge advancements and research in the integration of **cyber range training, cyber insurance, and risk management** to enhance organizational resilience. It emphasizes practical applications of these strategies in critical areas such as **supply chain and logistics security**, **smart cities and critical infrastructure**, and **transportation and fleet management**. By bringing together experts from academia, industry, and policymaking, the workshop seeks to foster a holistic approach to cybersecurity, preparing stakeholders to tackle modern threats and ensure a secure and sustainable digital ecosystem.

The workshop will be held in conjunction with the IEEE CSR 2026 conference as a **physical event**, during August 3–5, 2026. Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include but are not limited to the following:

- Cyber-range platforms
- Cyber insurance
- Cyber-risk assessment methods
- Cyber-security training
- Gamification in cyber-security
- Preparation and adaptation strategies
- Critical infrastructure security
- eHealth security
- Software security
- Cyber-threat intelligence
- Federation of cyber-range platforms
- Cyber-risk forecasting and mitigation
- Cyber-threat adaptive capacity in IoT
- Operational recovery and continuity

The CRIRM workshop will accept high-quality research papers presenting strong theoretical contributions, applied research and innovation results obtained from funded cyber-security and resilience projects, and industrial papers that promote contributions on technology development and contemporary implementations.

Submitted manuscripts should not exceed 6 pages (plus 2 extra pages, being subject to overlength page charges) and should be of sufficient detail to be evaluated by expert reviewers in the field. Accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements. Detailed information about paper submission and guidelines for authors can be found at the workshop's website **https://www.ieee-csr.org/crirm**.

Supported by

https://secawarenesstruss.eu/

https://cyberunity.eu/

https://dep-ermis.eu/

https://www.synapse-project.eu/