International Conference on Computer Security in the Nuclear World: Securing the Future

Monday 11 May 2026 - Friday 15 May 2026

Vienna International Centre

Scientific Programme

Conference Themes

Listed below are the six conference themes, along with potential technical sessions to be organized within each theme. These technical sessions are subject to change.

Computer Security’s Place in the Nuclear Sector and Beyond

- Breaking down silos: fostering collaboration and knowledge sharing.
- Opportunities to adapt experience from non-nuclear sectors.
- Building computer security into material detection, transport, use of radioactive sources and other activities.
- Computer security explained to non-cyber nuclear professionals.
- Effective incident response, and ensuring resource readiness.
- How are we going to work together on advanced reactors, small modular reactors (SMRs) and microreactors?

Regulatory Frameworks

- Practical use of international standards and guidance to enhance computer security
- Regulatory frameworks – lessons learned including from outside the nuclear sector.
- Inspections – how to reduce risk and gain assurance.
- How regulatory frameworks can help reduce supply chain risk.
- How regulatory frameworks are written to anticipate emerging threats and new technologies and evolve as necessary.

Capacity & Competency Management for Computer Security and Sustainability

- Attracting and retaining skilled computer security staff – the skill shortage.
- Continuing professional development and education in computer security.
- Working together to solve the shortage: academia, industry, and government.
- Embedding a culture of security – and that includes everyone!
- Enhancing computer security through exercises and drills.

Threats and Risks

- Practical risk management strategies, the role of the DBT.
- Detect, respond and recover: lessons learned from when “protect” fails.
- Threat intelligence in action: informing risk management decisions.
- Managing risks and mitigating vulnerabilities in the supply chain.
- Insider threats and cyber-enabled sabotage: balancing human and computer security.

Computer Security by Design

- Secure-by-design in practice – integrating computer security.
- Building a fortress: effective controls, security architecture, and defensive strategies.
- Using complex technology, e.g. software-based systems, Field-Programmable Gate Arrays.
- Mitigating risks of human error and social engineering.
- Safety/Security interface – practical steps for safety/security to work together.

Computer Security Impact of New Digital Technologies

• Balancing innovation and security: trade-offs in digital transformation.
• Secure use of smart sensors, cloud, remote operations and maintenance, and autonomous operations.
• Applying non-nuclear industry innovations to nuclear computer security.
• Harnessing the benefits of AI while mitigating cyber risks.