Be Part of the Movement: Shape the Future of Cyber-Physical Risk in the Built Environment

As information technology (IT) and operational technology (OT) converge into a cyber-physical systems in all machines, facilities and infrastructure, both professional engineers and the insurance underwriters that protect their liability must now account for a category of public safety risk that sits outside traditional engineering disciplines. This risk is foreseeable, repeatable, and life-safety relevant. Yet it remains largely unassigned within professional engineering responsibility and liability structures. The education and practice of cyber safety engineering must be recognized as a distinct designer of record with a formal Standard of Care, professional licensing, and clear professional liability assignment incentivized by insurers.

An inaugural **Cyber Safety Summit 2026**, taking place on ***June 10, 2026 at the National Academy of Sciences in Washington, D.C***., is a national convening of infrastructure owners, insurers, engineers, academics, and policymakers. Together, we will establish the first-ever Cyber Safety Standard of Care for the built environment. In a world increasingly dependent on connected life-essential infrastructure—utilities, healthcare, transportation, water systems, buildings, homes —cyber risk in engineering can no longer be assumed by traditional disciplines. Human safety depends on a new approach. The Summit is focused on action by aligning technical standards, professional practice, and liability policy to protect life, health, and property.

The relationship between insurance and professional engineering standards of care has evolved over the past century, usually when major engineering failures (fires, bridge collapse, boiler explosions) resulted in significant claims. Professional engineering societies developed codes of ethics and practice standards in part to address public safety failures and insurance market concerns. As projects grew larger and more complex, engineering firms sought professional liability insurance. Insurers, in turn, required predictable professional behavior, defensible norms of practice, and evidence that engineers adhered to accepted standards of care. State-based professional licensing became widespread with insurance coverage beyond gross negligence to include "errors and omissions". Insurers increasingly required documentation and risk management protocols. Engineering societies responded by formalizing standards and guidance to serve as benchmarks for professional judgment.

Cyber-physical systems now present the same conditions that historically drove the creation of engineering standards of care: foreseeable hazards, repeatable failure modes, and catastrophic consequences. Yet no comparable standard exists for cyber safety in the built environment. Compliance with recognized standards can reduce premiums while deviation may increase liability. exposure or void coverage altogether.

We invite representatives from your professional society to actively participate in the cross-sector collaboration to develop guidance and standards. Participants will have the opportunity for:

- Visibility with top federal and private sector stakeholders to address cyber risk mitigation
- Engagement with a generational national standard-setting effort to reduce liability.
- Leadership in shaping the future of cyber-physical safety for the engineering community

We also ask that you share this event with your Membership

Join us in writing the future of engineering and infrastructure security to make the world a safer place.

For more information about the event:

Lucian Niemeyer, CEO- BuildingCyberSecurity.org
Lucian@buildingcybersecurity.org (571) 277-3115

Rachel Roberts-Jones, CEO RJTech
Website: www.RJTechConsulting.com
CEO@RJTechConsulting.com (301) 643-9434

CyberSafetySummit