MIT MANAGEMENT SLOAN SCHOOL

CYBERSECURITY

THANK YOU CAMS MEMBERS

"We extend our sincere thanks to all our members for contributing to the success of the AI & Cybersecurity Conference this past May. We were proud to have so many leading cyber experts join us to share best practices and explore what's ahead."

Stuart Madnick

"Thank you for lending your insights to our community of members, researchers and special interest groups on critical topics such as Cyber Culture, OT/ICS, and Risk Management."

Michael Siegel

IDEAS MADE TO MATTER

HIGHLIGHTS FROM THE CAMS AI & CYBERSECURITY CONFERENCE

Our recent AI & Cybersecurity Conference wasn't just a gathering of experts, it was a vibrant meeting of minds, driven by a shared purpose: to understand how artificial intelligence is reshaping our digital lives and what we as a community can do to keep each other safe. Held at the Samberg Conference Center, overlooking the Cambridge skyline, our event brought together researchers, industry leaders, policymakers, and practitioners in an atmosphere of openness, urgency, and collaboration. From keynote talks on AI-enabled DeepFakes to late afternoon "hot topics" sessions on insurance and regulation, the discussions were rich, honest, and forward looking. What united us all was the recognition that AI is transforming the threat landscape faster than many organizations can respond and that only through shared knowledge, thoughtful governance, and sustained dialogue can we keep pace. Cybersecurity is no longer just a technical challenge, but a collective one. Let's keep learning, connecting, and building together. Read the meeting summary.

Pictured from Right to Left; Sander Zeijlemaker, MIT CAMS Research affiliate, Michael Siegel, Director & Co-founder of MIT CAMS, Vidit Baxi Co-founder & CISO of Safe Security.

RETHINKING THE CYBERSECURITY ARMS RACE

In a recent working paper authored by Michael Siegel, Sander Zeijlemaker, Vidit Baxi and Sharavanan Raajah, researchers were

About Cybersecurity at MIT Sloan (CAMS)

MIT is a natural place to study cybersecurity, given its rich history of technology innovation, and the MIT Sloan School of management is the home of the Cybersecurity at MIT Sloan (CAMS) research consortium. The Consortium is focused on the managerial, organizational, and strategic aspects of cybersecurity. More information can be found at https:// cams.mit.edu or by contacting us:

Stuart Madnick
Founding Director
smadnick@mit.edu

Michael Siegel
Director
msiegel@mit.edu

able to determine that 80% of ransomware attacks are now powered by AI. We're facing a new kind of arms race, one where speed, scale, and adaptation are being redefined. This CAMS working paper calls on organizations to fundamentally rethink their approach. It's no longer about reacting, it's about anticipating. CAMS researchers and affiliates argue for an AI-integrated defense posture that blends automation with human judgment, and real-time threat intelligence with long-term strategic oversight. This paper doesn't just sound the alarm, it offers a roadmap for action, urging CISOs, policymakers, and technologists to pivot from defense as containment to defense as intelligence. Read the paper here.

GLOBAL CYBER REGULATIONS: A CALL FOR HARMONIZATION

At SECRYPT 2025, the poster "Understanding the Differing Definitions of Cyber Incidents and Reporting Requirements in Regulations" authored by Dr. Angelica Marotta and Dr. Stuart Madnick—sparked dynamic conversations around regulatory fragmentation in cybersecurity. The study analyzes how fragmented definitions of "cyber incidents" across U.S. and European regulations complicate compliance and incident response for organizations. Drawing on a database of nearly 200 regulations and interviews with industry leaders, the research calls for more harmonized and proactive regulatory approaches. The poster session sparked rich discussions with fellow researchers and practitioners, many of whom echoed the challenges of navigating conflicting definitions in their day-to-day work and highlighted the practical value of the authors' regulatory database. Several attendees also emphasized the need for a global dialogue on standardizing cyber incident terminology—an encouraging sign that this work is resonating with both the academic and practitioner communities.

Dr. Stuart Madnick and Dr. Angelica Marotta at SECRYPT 2025, in Bilbao, Spain. June 2025.

CYBERSECURITY AT MIT SLOAN 2025 PRIORITIES

RISK AND RESILIENCE

- Measure and manage cyber risk and resilience
- Explore mechanisms like insurance and CAT bonds to transfer and model risk
- Strengthen supply chain security and third-party resilience
- Understand the role of trust in managing cyber risk

GOVERNANCE

- Clarify the Board's role in cybersecurity oversight
- Track evolving regulations and define what's needed next

AI AND CYBERSECURITY

- Use AI to strengthen cybersecurity practices
- Secure AI applications themselves
- Identify new risks and vulnerabilities introduced by AI

CYBERSECURITY ECOSYSTEMS

- Support SMEs in improving their security
- Measure and manage supply chain risk
- Build a strong culture of cybersecurity inside and outside organizations

CYBER-PHYSICAL SYSTEMS

- Secure IoT devices and complex operational environments
- Integrate safety and IT security knowledge to protect OT systems

CYBER RISK THROUGH THE EXECUTIVE LENS

(AMCIS 2025 Papers)
Advancing Cyber Risk by Reducing Strategic Control Gaps
Balancing Risk and Reward in Cybersecurity Investment Decisions
By Sander Zeijlemaker, Ranjan Pal, Jeff Proudfoot, Goeun Kim, and Michael Siegel

Executives often hold the keys to cyber resilience, but too often they're flying blind. These two papers use simulation gaming to expose five common executive decision-making failures that increase cyber vulnerability. The findings are a wake-up call; whether it's underinvesting in the wrong areas or overlooking key interdependencies, leadership blind spots can become open doors for attackers. The research also offers pragmatic guidance on closing strategic control gaps, helping boards and C-suites lead more effectively in a volatile risk environment.

SECURING SUPPLY CHAINS AT SCALE

(Published by the World Economic Forum)
Three key ways to make supply chains more resilient to cyber risks
By Michael Siegel, Sander Zeijlemaker, Raphael Yahalom, Ranjan Pal, Mirco Ross

Supply chains are increasingly digital and increasingly fragile. This piece published by the World Economic Forum, outlines three critical directions for improving cyber resilience in global supply networks: embedding cyber into vendor selection, enabling adaptive risk responses, and rebalancing incentives across stakeholders. It's a call to arms for supply chain leaders, CISOs, and regulators alike. Resilience won't come from checklists; it will come from new frameworks that promote visibility, accountability, and shared risk ownership.

ADDRESSING DUAL-USE GENAI THREATS: CAMS RESEARCH SPOTLIGHTED AT JOHNS HOPKINS APL

Ranjan Pal received a prestigious invitation from Johns Hopkins University Applied Physics Laboratory (APL) to share research on the critical topic of "GenAI vs GenAI in Industrial Control Systems Cyber Risk Management." This presentation, delivered by CAMS research student Cynthia Zhang, explored how generative AI models can be both powerful tools and formidable threats in securing industrial control environments. This invitation underscores the growing influence and real-world impact of Cynthia's earlier work, first introduced at the Winter Simulation Conference 2023. That research has steadily gained attention across government agencies and academic institutions for its rigorous analysis and practical frameworks. Cynthia's contributions are an inspiring example of how student-led research

DISCUSS WITH US

MIT CAMS Friday Research Community Discussion: The CAMS research community meets almost every Friday from:

11:30 -12:30 EST

The topics vary each week. If you are interested in participating, contact us now!

For more information on CAMS Research and getting involved, please reach out to our team at: mitcyber@mit.edu

CAMS IN THE PRESS

at CAMS can shape the national dialogue around emerging cybersecurity challenges.

COLLABORATIVE CYBERSECURITY STRATEGIES FOR LARGE FIRMS AND SME SUPPLIERS

Jillian Kwong recently led a discussion titled "Securing the Fleet: Collaborative Cybersecurity Strategies for Large Firms and their Small and Medium Suppliers." The session addressed a pressing challenge: while many large organizations expect SME suppliers to defend themselves against sophisticated cyber threats, these businesses often lack the resources, expertise, and dedicated security staff to meet growing demands. As a result, supply chains remain exposed to significant risk. Jillian and participants explored how leading companies are moving beyond compliance mandates to actively support their suppliers. The conversation highlighted examples of effective training, collaborative frameworks, and practical initiatives that have helped reduce risk across industries.

Jillian is currently preparing to present a paper with Dr. Keri Pearlson, at the 2025 Pacific Asia Conference on Information Systems in Kuala Lumpur, Malaysia this July. Titled "Building a Resilient Supply Chain: Collaborative Approaches to Small and Medium-sized Enterprise (SME) Cybersecurity," the paper documents and explores ways companies support their SME suppliers and offers practical guidance to organizations looking to strengthen third-party security.

JOIN CAMS TODAY TO ACCESS MORE EXCLUSIVE CONTENT

CAMS members gain access to cutting-edge cybersecurity research, exclusive webinars, and executive education opportunities. Join CAMS today to stay ahead of emerging cybersecurity trends and connect with global industry leaders.

READ ALL ABOUT IT! CAMS IN THE NEWS & PUBLICATIONS

July 9, 2025: Stuart Madnick was featured in a Bloomberg article titled "US Pushes Software Developers to Embrace Memory Safe Languages." Professor Madnick emphasized that while performance remains critical in domains like defense and AI, concerns about switching languages have waned as computing power grows more affordable.

July 2, 2025: Ranjan Pal had an article published by Forbes India. "Why does cybersecurity management in enterprises fail?" The article discusses governance gaps, misaligned incentives, and profit-first mindsets leave even well-funded organizations vulnerable in the age of AI and digital supply chains

LEARN MORE NOW

For more information about attendance contact our Senior Director of Communications: Kelty Fitzgibbons (kcfitz@mit.edu)

June 11, 2025: Ranjan Pal had an article published by Forbes India. “How to manage cyber risk in AI LLM-driven pharmaceutical supply chains.” The article features four action items to mitigate the effect of LLM security vulnerabilities on the pharmaceutical industry and its supply chain ecosystem

June 10, 2025: Sander Zeijlemaker had an article published “Strategic Board Perspectives on the Threat Landscape and the Role of Management Dash-boarding” The article explores how boards can better understand and oversee evolving cyber risks.

May 21, 2025: Dr. Keri Pearlson coauthored an article for Harvard Business Review “Boards Need a More Active Approach to Cybersecurity.”

May 9, 2025: Ranjan Pal and Cynthia Zhang had an article published by Forbes India. “How to manage GenAI cyber risk in industrial control systems.”

May 3, 2025: Dr. Keri Pearlson participated in the video panel “Cyber Resilience in the Age of AI: Threats, Responses & Human Stories” hosted by IIA MIT. In the discussion, she highlighted the evolving nature of cyber threats driven by AI advancements and emphasized the critical role of human-centered strategies in building resilient organizations.

April 29-30, 2025: Angelica Marotta and Stuart Madnick presented at the ASC Conference in Las Vegas. Their session, “Harmonizing Cyber Incident Reporting: Challenges in Definitional Consistency,” explored the critical need for standardized definitions across cyber incident reporting frameworks to improve regulatory compliance and organizational resilience.