# Welcome to the Cybersecurity at MIT Sloan (CAMS) AI & Cybersecurity Conference 2025

# Wednesday May 21, 2025

8:00am-5:00pm

# Location: Samberg Conference Center WIFI: MIT GUEST

**CHATHAM HOUSE RULE:** To encourage interactivity, we will use the Chatham House Rule ("Under the Chatham House Rule, participants are free to use information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant may be revealed")

# Agenda

- 8:00 Doors open for Registration & Breakfast
- 9:00 Opening Remarks and Welcome Conference Overview & Goals
- 9:15 MIT Keynote : John Williams, Generative AI and Security: DeepFakes and Super-Human Performance
- 10:00 Panel: Al for Cybersecurity Discussion
- 10:45 Break
- 11:15 Industry Keynote : Peter Bailey, Harnessing Generative AI for Cybersecurity
- 12:00 Panel: Cybersecurity for AI Discussion
- 12:45 Working Lunch
- 1:45 Nobel laureate Keynote: Simon Johnson, Technology and Inequality in the Age of AI

Begin Afternoon Session & Cyber Security Workshop 2:30PM – 4:45PM

- 2:30 Hot Topics Discussions: Al and Cybersecurity
- 3:30 Break
- 4:00 Planning Now for the Future: Industry Partners Discussion
- 4:45 Next Steps for CAMS and Members
- 5:00 Closing Remarks & Goodbye!

# Cybersecurity at MIT Sloan (CAMS) AI & Cybersecurity Conference 2025

# Wednesday May 21, 2025

8:00am-5:00pm Location: Samberg Conference Center

**Materials Packet** 

# Cybersecurity at MIT Sloan AI & Cybersecurity Conference

Wednesday May 21, 2025

# TABLE OF CONTENTS

- 1. Conference Agenda
- 2. Chatham House Rules

3. VIP Dinner & Welcome Reception Keynote Speaker Una-May O'Reilly : Developing Artificial Adversarial Intelligence

4. MIT Keynote: Professor John Williams: Generative AI and Security: DeepFakes and Super-Human

### Performance

- 5. Panel 1: AI for Cybersecurity Discussion
- 6. Industry Keynote : Peter Bailey : Harnessing Generative AI for Cybersecurity
- 7. Panel 2: Cybersecurity for AI Discussion
- 8. Nobel laureate Keynote : Simon Johnson : Technology and Inequality in the Age of AI

9. Afternoon Session & Cyber Security Workshop : Introduction to Poster Session, Lightening Talks, and Word Cloud.

- 10. Afternoon Session & Cyber Security Workshop : Hot Topics Discussions Regulation and Compliance
- 11. Afternoon Session & Cyber Security Workshop : Hot Topics Discussions Cyber Insurance
- 12. Research Framework & Research Priorities
- 13. Recent Newsletters & Recently Published Articles
- 14. Evaluation

# **Conference Agenda**

### Day 1: May 20, 2025 – VIP Welcome Reception and Dinner

Location: MIT Samberg Conference Center, 50 Memorial Dr, Cambridge, MA 02142

### 6:00 PM – 8:30 PM

- Welcome & Networking & Cocktails
- Reception Keynote Speaker

### **Developing Artificial Adversarial Intelligence**

Una-May O'Reilly (Principal Research Scientist, MIT CSAIL)

Una-May O'Reilly: "Investigating how to stop the destructive and escalating arms races between cyber attack actors and cyber defenders."

Dinner & Discussions

### Day 2: May 21, 2025 – Conference & Workshops

Parts of this conference will be available for remote participation via Zoom. In-person attendance is encouraged for the full conference experience.

### Morning Session 8:00AM – 12:45PM

Location: MIT Samberg Conference Center, 50 Memorial Dr, Cambridge, MA 02142

### 8:00 AM – Registration & Breakfast

### 9:00 AM – Opening Remarks and Welcome

Conference Overview & Goals (Michael Siegel & Stuart Madnick)

### 9:15 AM – MIT Keynote Speaker

### Generative AI and Security: DeepFakes and Super-Human Performance

**John Williams** (Professor of Information Engineering and Civil and Environmental Engineering at MIT)

John William: "We don't fully understand the properties of generative AI, which makes it difficult to predict how it will behave."

10:00 AM – Panel: AI for Cybersecurity Discussion (Moderator Michael Siegel; Panelists: Nelson Novaes Neto, C6 Bank; Arjun Ramakrishnan, Mastercard; Viditkumar Baxi, Safe Security; others TBC )

10:45 AM – Break

### 11:15 AM – Industry Keynote

### Harnessing Generative AI for Cybersecurity

**Peter Bailey** (VP of Google Cloud and General Manager of Security Operations for Google, formerly COO of Mandiant)

Peter Bailey: "Understanding the key threats targeting your industry and prioritizing the right defensive measures across people, processes, and technologies has always been critical to a successful cyber defense program."

### 12:00 PM Panel: Cybersecurity for Al Discussion (Moderator: Stuart Madnick; Panelists: Michael Coden, BCG; Bugra Karabey, Microsoft; Boris Sieklik, MongoDB; Robert Lembree, Schneider Electric)

### 12:45 PM – Working Lunch

### 1:45 PM — Nobel laureate Keynote

### Technology and Inequality in the Age of AI

**Simon Johnson** (Professor of Entrepreneurship at the MIT Sloan School of Management, and head of the Global Economics and Management group. In 2024, Johnson received the Nobel Prize "for studies of how institutions are formed and affect prosperity.")

Simon Johnson is co-author of the 2023 book "Power and Progress: Our 1,000-Year Struggle over Technology and Prosperity" (copies will be provided to all CAMS members)

### Afternoon Session & Cyber Security Workshop 2:30PM – 4:45PM

The following sessions are available for in-person attendance only.

### 2:30PM – Hot Topics Discussions: AI and Cybersecurity

- **Regulation and Compliance** (Moderators: Joram Borenstein, GM Microsoft and Jeffery Proudfoot, Bentley University and CAMS Research Affiliate)
- **Cyber Insurance** (Moderators: Katrina Hill, Cyber Security Consultant, Gallagher Re and Ranjan Pal, Research Scientist, CAMS)
- Supply Chain Management (Moderators: Industry Participant TBC, Academic Participant TBC)

### 3:30 PM – Break

4:00PM – Planning Now for the Future: Industry Partners Discussion (Moderator: Michael Siegel)

4:45 PM –Next Steps for CAMS and Members (Stuart Madnick and Michael Siegel)

All are welcome to join for a drink at Locke Bar, after the conference. Located at: **6 Broad Canal Way, Cambridge, MA 02142** 

# **CHATHAM HOUSE RULES:**

To encourage interactivity, we will use Chatham House rules ("Under the Chatham House Rule, participants are free to use information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant may be revealed")

**Reception Keynote Speaker Una-May O'Reilly** 

May 20, 2025

### **Developing Artificial Adversarial Intelligence**

Una-May O'Reilly (Principal Research Scientist, MIT CSAIL)



Since the beginning of my interest in Artificial Intelligence, I have focused on learning and adaptation. My central inspiration is Nature's process of evolution because it generates compelling examples of intelligent organisms and behavior. This is why I work with evolutionary algorithms. Neither evolution or evolutionary algorithms are efficient, but I am devoted to the open question of how to use the latter to computationally replicate intelligence.

Adversarial learning, i.e. behavioral adaptation under the pressure of adversarial competition, is an under-explored facet of intelligence, despite being so common and important to understand. For example, consider biological arms races of predators and prey, viruses and their hosts, the never-ending challenges of cybersecurity, generative adversarial network training, and even squirrels versus bird feeder owners! Adversarial Intelligence is the thinking underlying adversarial behavior. It recruits planning, learning, technical skills, expert knowledge and other facets of intelligence. From these concepts, I have coined the moniker **"Artificial Adversarial Intelligence"**. ALFA's North Star goal is to computationally replicate Adversarial Intelligence in pursuit of Artificial Adversarial Intelligence.

MIT Keynote Speaker John Williams

May 21, 2025

### Generative AI and Security: DeepFakes and Super-Human Performance

(Professor of Information Engineering and Civil and Environmental Engineering at MIT)



John R. Williams is a Professor of Information Engineering and <u>Civil and Environmental</u> <u>Engineering</u> at MIT.

Professor Williams holds a BA in physics from Oxford University, an M.Sc. in physics from UCLA, and a Ph.D. from Swansea University. His area of specialty is large scale computer analysis applied to both physical systems and to information.

Professor Williams is internationally recognized in the field of computational algorithms for large-scale particle simulators and has authored two books and over 100 publications. His research has focused on architecting of large scale distributed network simulation systems, GeoNumerics of Granular and Powder Systems, Information Technology, Cyber/Physical Security, and Web-Based Education Technology.

He teaches graduate courses on Modern Software Development and on Web System Architecting, including Engineering Computation and Data Science.

Al for Cybersecurity Panel, Moderated by Michael Siegel

May 21, 2025

### **Moderator:**



### **Panelists:**



Michael Siegel (MIT CAMS) Michael Siegel is a Principal Research Scientist at the MIT Sloan School of Management, He is also the Director of Cybersecurity at MIT Sloan (CAMS). Siegel's research focuses on the management, strategy, technology, and organizational issues related to cybersecurity with specific interest in vulnerability markets, cyber risk management, dark web business models, IoT endpoint security, vulnerability management, cybersecurity workforce development, and educating management in cybersecurity. He also has done research in the intelligent integration of information systems, risk management, insurgency and state stability, data analytics, healthcare systems, and systems modeling. Siegel has published articles on such topics as simulation modeling for cyber resilience, cyber vulnerability markets, A.I. and cybersecurity, data management strategy, architecture for practical metadata integration, heterogeneous database systems, and managing and valuing a corporate IT portfolio using dynamic modeling of software development and maintenance processes. His research at MIT has continued for over 35 years and includes a wide range of publications, patents and teaching accomplishments.

**Nelson Novaes Neto (C6 Bank)** Co-founded and CTO at C6 Bank—Brazil's rapidly expanding digital bank and JPMorgan Chase partner—and is an MIT-affiliated researcher with academic credentials ranging from engineering to psychology. Over 20 years, he has driven large-scale cloud, AI and product platforms. A published technologist and sought-after speaker, Nelson is also a mountain-bike enthusiast and Brazilian Jiu-Jitsu national champion. Nelson lives in São Paulo, Brazil, with his wife and two young daughters.



**Arjun Ramakrishnan (Mastercard)** is a Principal Cybersecurity Architect at Mastercard with over 17 years of experience in information security. He leads efforts in developing AI security frameworks, evaluating emerging technologies, and advancing enterprise security architecture. A specialist in data protection and Zero Trust methodology, Arjun plays a key role in guiding strategic IT initiatives and shaping secure digital infrastructure at scale.



Viditkumar Baxi (Safe Security) is the Co-Founder and Chief Information Security Officer at Safe Security. He founded Safe Security in 2012 along with Saket Modi and Rahul Tyagi. Vidit leads Safe's threat research team and ensures the company follows the necessary cybersecurity guidelines & compliances. He also heads multiple product functions and is key in driving the enterprise and product journey forward. Vidit has been featured by Fortune in their 40-under-40 twice and was awarded the Entrepreneur of the Year (2019) by Entrepreneur Magazine.

Industry Keynote Speaker Peter Bailey

May 21, 2025

### Harnessing Generative AI for Cybersecurity

(VP of Google Cloud and General Manager of Security Operations for Google, formerly COO of Mandiant)



Peter Bailey is a seasoned technology executive with over 25 years of operational experience spanning cybersecurity, SaaS, software, and services. In recent years, his focus has been exclusively on cybersecurity, assisting clients in developing sophisticated cyber defense programs and providing robust active threat defense capabilities.

Peter recently joined Cisco Systems as SVP & GM of Security, responsible for Cisco's network and cyber security products and services. Prior to Cisco, Peter served as VP/GM of the Security Operations (SecOps) business at Google Cloud, a rapidly expanding cybersecurity division serving large enterprises and government entities. He joined Google Cloud in 2022 following the Mandiant acquisition, where he previously held the position of EVP and COO. His tenure at Mandiant began in 2019, which included its prior parent company, FireEye.

Before joining FireEye, Peter held various operational leadership roles, including CEO of Vertical Communications, a telecom software and services provider, from 2011 to 2019. Throughout his career as an operator and leader, a consistent theme has been his ability to build high-performing teams, instill a strong sense of mission, and drive exceptional customer outcomes. He has a particular expertise in helping organizations operationalize enterprise software product strategies and execute go-to-market strategies at scale.

Peter currently resides in the Bay Area with his wife, Victoria, and their three sons in middle and high school. Outside of work, he enjoys spending time outdoors with his family, engaging in various activities.

### Cybersecurity for AI Panel, Moderated by Stuart Madnick

May 21, 2025

### **Moderator:**



Panelists:





**Stuart Madnick (Founder of CAMS)** has been a faculty member at M.I.T. since 1972. He has served as the head of MIT's Information Technologies Group for more than twenty years. During that time the group has been consistently rated #1 in the nation among business school information technology programs (*U.S. News & World Reports, BusinessWeek, and ComputerWorld*). He has also been an affiliate member of MIT's Laboratory for Computer Science, a member of the research advisory committee of the International Financial Services Research Center, and a member of the executive committee of the Center for Information Systems Research.

**Michael Coden (MIT)** Recognized as one of the "Top 50 Cybersecurity Leaders" by *The Consulting Report* in both 2021 and 2022, Michael advises boards and C-suites on cybersecurity strategy across IT, OT, and product environments. He is Co-Founder of DBOS, Inc., serves on the Board of Opscura, and is a Senior Advisor to BCG. Previously, he led BCG's global Technology and Cybersecurity Practice and has held executive roles at NextNine, Codenoll (NASDAQ: CODN), and ADC Telecommunications. A CISSP and holder of 17 patents, Michael has appeared on PBS and Bloomberg and holds degrees from MIT, Columbia, and NYU.

Kristy Hornland (KPMG): Kristy Hornland is a Cybersecurity Director at KPMG US, where she leads the development and delivery of AI security frameworks aligned with the NIST AI RMF, MITRE ATLAS, and the EU AI Act. She has guided organizations across sectors—including life sciences, finance, manufacturing, and government—in securing responsible AI deployments. Kristy led the Global Resilience Federation's AI Security Practitioner and Leadership Guides, collaborating with over 20 partners including MITRE, CISA, and Microsoft. A founding team member of Cranium, KPMG's award-winning AI security startup, she also serves as Deputy Lead of KPMG US's Women in Cyber program, advancing inclusion and governance in the cyber workforce.



**Burga Karabey (Microsoft):** Burga is a Principal Group PM Manager at Microsoft, leading the Datacenter Cybersecurity Program Management team. He oversees cybersecurity programs for Microsoft's cloud datacenters and for the Supercomputing AI infrastructure. He holds a BS in Electrical and Electronics Engineering, an MBA, and a PhD in Information Systems. He has multiple security certifications and has authored multiple patents and publications in cybersecurity and AI.



**Boris Sieklik (MongoDB)** is a Senior Director of Information Security at MongoDB and a strong believer in cybersecurity being a business enabler. Boris is a big proponent of SaaS security as a new and emerging cyber security field and has spoken on several conferences and podcasts on this topic. He has 12+ years of experience in cybersecurity leadership roles across different industries including Finance, Anti-malware and Tech companies. Boris holds a number of industry certifications such as OSCP and also discovered and published a new DDoS amplification attack which was covered in international media.



**Robert Lembree (Schneider Electric)** Distinguished Cybersecurity Architect Lembrée is a senior technical leader at Schneider Electric, where he leads the company's Secure Development Lifecycle (SDL) process—an essential framework for ensuring consistent, effective product security across global development teams. With more than 40 years of experience in software architecture and cybersecurity, he focuses on scalable, risk-based approaches that align security practices with business needs in the automation and control systems domain

### Nobel laureate Keynote Speaker Simon Johnson

May 21, 2025



### Technology and Inequality in the Age of AI

(Professor of Entrepreneurship at the MIT Sloan School of Management, and head of the Global Economics and Management group. In 2024, Johnson received the Nobel Prize "for studies of how institutions are formed and affect prosperity.")

Simon Johnson is the *Ronald A. Kurtz (1954) Professor of Entrepreneurship* at the MIT Sloan School of Management, where he is head of the Global Economics and Management group. At MIT, he is also codirector of the <u>Shaping the Future of Work Initiative</u> and a Research Affiliate at Blueprint Labs.

In 2024, Johnson received the Sveriges Riksbank Prize in Economic Sciences in memory of Alfred Nobel, joint with Daron Acemoglu and James A. Robinson, "<u>for studies of how institutions are formed and affect prosperity</u>."

In 2007-08, Johnson was chief economist and director of the Research Department at the International Monetary Fund. He currently co-chairs the <u>CFA Institute Systemic Risk Council</u> with Erkki Liikanen. He is a Research Associate at the NBER and a Fellow at CEPR.

Johnson's most recent book, with Daron Acemoglu, <u>Power and Progress: Our 1000-Year Struggle Over</u> <u>Technology and Prosperity</u>, explores the history and economics of major technological transformations up to and including the latest developments in Artificial Intelligence. *Power and Progress* is currently scheduled for publication in about 20 languages around the world. It was long listed for the 2023 Financial Times and Schroders Book of the Year and for the Baillie Gifford Prize for Non-Fiction, and it was shortlisted for the <u>2024 Lionel Gelber Prize</u>.

Afternoon Session & Cyber Security Workshop

May 21, 2025

### Introduction to Poster Session, Lightening Talks, and Word Cloud with Sander Zeijlemaker



**Sander Zeijlemaker (MIT CAMS)** Dr. Sander Zeijlemaker is a strategist, consultant, and writer who specializes in the predictability and understandability of dynamic, complex, and strategic decisions. He has spent his career advising policymakers and business leaders in the fields of international strategic IT operations, business change, and global cyber risk. Speaking to audiences around the world, Dr. Zeijlemaker provides unique insight into the dynamic and complex nature of cyber risk. He is a research affiliate at the Massachusetts Institute of Technology, an agenda contributor to the World Economic Forum, and former member of the Ad Hoc Working Group on Security Operation Centres of ENISA. Adversary Board Member TU Twente and former President of the Global Security, Stability, and Resilience (SSR) Special Interest Group (SIG) of the System Dynamics Society, Dr. Zeijlemaker mobilizes and connects a group of professors, practitioners, and students in this field.



**Nelson Novaes Neto (C6 Bank)** Co-founded and CTO at C6 Bank—Brazil's rapidly expanding digital bank and JPMorgan Chase partner—and is an MIT-affiliated researcher with academic credentials ranging from engineering to psychology. Over 20 years, he has driven large-scale cloud, AI and product platforms. A published technologist and sought-after speaker, Nelson is also a mountain-bike enthusiast and Brazilian Jiu-Jitsu national champion. Nelson lives in São Paulo, Brazil, with his wife and two young daughters.



**Cynthia Zhang (MIT CAMS)** Cynthia Zhang is a Masters student in the Electrical Engineering and Computer Science (EECS) department at MIT. She is also a researcher with Cybersecurity at MIT Sloan (CAMS) at the MIT Sloan School of Management. Her primary research interest lies in AI and cybersecurity of enterprises/industrial control systems.

Afternoon Session & Cyber Security Workshop May 21, 2025

### **Hot Topics Discussions**

Regulation and Compliance with Joram Borenstein and Jeffrey Proudfoot



**Dr. Jeffrey Proudfoot (MIT CAMS)** is an Associate Professor of Computer Information Systems at Bentley University and a Research Affiliate at the Center for Advanced Modeling and Simulation (CAMS) at MIT. His research focuses on cybersecurity regulations and governance, with over 50 academic publications in leading journals. Dr. Proudfoot has served as a research affiliate with CAMS/MIT for five years and previously worked for four years with the U.S. Department of Homeland Security's National Center for Border Security and Immigration.



Joram Borenstein (Microsoft) is a General Manager at Microsoft, leading Technical Advisory for Microsoft's sales leadership and overseeing the company's Security Go-To-Market (GTM) strategy. He has successfully integrated major security acquisitions including CloudKnox, RiskIQ, and CyberX. In addition to his role at Microsoft, Joram serves as an advisor and board director to multiple cybersecurity start-ups, including Authomize (acquired by Delinea), Kognos (acquired by Devo), and Conjur (acquired by CyberArk).

### Afternoon Session & Cyber Security Workshop

May 21, 2025

### **Hot Topics Discussions**

Cyber Insurance with Katrina Hill and Ranjan Pal



Ranjan Pal (MIT CAMS) is a Research Scientist at the MIT Sloan School of Management who is a cybersecurity expert and broadly conducts and leads research on cyber risk/resilience management through Cybersecurity at MIT Sloan (CAMS) using the interplay of computer science, decision science, and applied mathematics. He is also currently an invited member of the systems cyber-resilience working group (WG) at the World Economic Forum contributing his expert insights on solving the most important societal challenges on cyber resilience - some insights reaching the White House. Ranjan pioneered the field of mathematical models adjudicating the market sustainability of cyber-insurance solutions. He has acted as strategic cyber risk management advisor to corporations and has been an invited expert on government research review panels in science and technology. Ranjan has published/contributed to nearly 100 research articles in premier academic, policy, and global business outlets that include ACM/IEEE/AIS/Elsevier journal and conference proceedings, World Economic Forum reports, Forbes, The Financial Times, The Economic Times, The Financial Express, Re-InAsia, and The Times of India. He is an Associate Editor of the ACM Transactions on Management Information Systems.



**Katrina Hill (Gallagher Re)** is a Cyber Security Consultant at Gallagher Re, where she leverages her unique cyber expertise to benefit the reinsurance industry. She focuses on translating cyber risks into actionable insights and advising on strategic measures to reduce these risks, ensuring that Gallagher Re clients is better prepared to face the evolving landscape of cyber threats. Prior to Gallagher Re, she was at Accenture where she did six years in Incident Response consulting.

# Stratter Government Manage Stratter Stratter</td

### Strategy

- Board-level cyber education
- Cybersecurity Impact on International Trade
- Framework for types of cyber education throughout the organization
- Ethics of cybersecurity
- Cyber warfare

### Governance

- Cyber risk evaluation & metrics
- Board governance of cyber
- Cybersecurity leadership in the organization
- Role of cyber insurance in risk mitigation
- Harmonizing compliance and cybersecurity

### Management

- Impact of cyber risk concerns on innovations
- Comparing national cybersecurity frameworks
- Usability vs security
- Cyber safety: applying research in accident prevention
- Cybersecurity of Industrial Control Systems (ICS)/Cyber-physical
- Cybersecurity for Cloud-based systems
- Cybersecurity of IoT Using Blockchain

### Autonomous Vehicles

### Organizational

- House of Security
- Organizational Cybersecurity Culture
- Bridging the IT/OT Culture Gap
- Success factors for cybersecurity
- Cyber information sharing
- Vulnerability research
- Security workforce

# **CAMS Priority Research Areas for 2025**



### CYBERSECURITY RISK MANAGEMENT

How do we manage (and measure) cyber risk? What mechanisms (CAT Bonds, Insurance, etc) are most effective for transferring, mitigating and modeling cyber risk? How do we minimize supply chain/ third-party risk? What role does trust play in managing cybersecurity risk?



### OPERATIONAL TECHNOLOGY

What is the best approach to managing cybersecurity of IoT devices, especially those running in plants and complex systems? How do manage the complexity of systems in a structured manner? How can we use what we know about safety and IT security to make our OT environments more secure?



### CYBERSECURITY GOVERNANCE

What is the role of the Board of Directors in cybersecurity governance? How is the regulatory landscape changing? What regulations are needed going forward?



### CYBERSECURITY CULTURE

How do we reduce the human risk? How do we increase the effectiveness of our cybersecurity culture? How might AI impact cybersecurity culture?



### CYBERSECURITY RESILIENCE

How do we make our organizations cyber resilient? What are the components of a cyber resiliency plan? How can we measure cyber resiliency?

# **MIT CAMS Recent Newsletters**

# Q1 2025 Newsletter

https://cams.mit.edu/wp-content/uploads/Newsletter-58.pdf

# SIG Newsletter

https://cams.mit.edu/wp-content/uploads/MIT-CAMS-CRM\_SIG-Jan-2025.pdf

# Q4 2024 Newsletter

https://cams.mit.edu/wp-content/uploads/Q42024CAMS-Newsletter-57.pdf

# **Recently Published Articles**

May 3, 2025: Dr. Keri Pearlson participated in the video panel <u>"Cyber Resilience in the Age of AI: Threats.</u> <u>Responses & Human Stories</u>" 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, <u>"Harmonizing Cyber Incident Reporting: Challenges in Definitional Consistency,"</u> explored the critical need for standardized definitions across cyber incident reporting frameworks to improve regulatory compliance and organizational resilience.

April 24, 2025: Dr. Keri Pearlson was quoted in the article <u>"Designing for Cyber Resilience, Not Just</u> <u>Defense,"</u>published by BankInfoSecurity. She emphasized the importance of building resilience, not just defense, into cybersecurity strategies.

April 23, 2025: Michael Siegel, Director of MIT CAMS, authored a World Economic Forum article titled <u>"Three key</u> ways to make supply chains more resilient to cyber risks." He highlights the need for coordinated regulation, executive oversight, and secure-by-design practices to strengthen global supply chain security.

March 25, 2025: Stuart Madnick was quoted in an ABC News article, <u>"What to know about Signal, which the</u> <u>Pentagon previously discouraged workers from using</u>" discussing the security implications of encrypted messaging apps like Signal.

March 20, 2025: Professor Stuart Madnick published an article in The Wall Street Journal discussing the risks of proposed regulations targeting online child sexual abuse material (CSAM). In <u>"Stopping Child Porn Online Is a</u> <u>Worthy Goal. But Beware the Proposed Cure"</u> he warns that these policies could weaken encryption, threaten privacy, and introduce new cybersecurity risks.

March 13, 2025: Stuart Madnick was quoted in an article<u>"AI and Cybersecurity: The New "Arms Race"</u> published by the MIT Horizon.

March 13, 2025: Stuart Madnick was quoted in an article <u>"The Future of Cybersecurity"</u> published by the MIT Horizon. This article discusses realistic predictions for what the next five years will bring to cybersecurity.

March 12, 2025: Dr. Keri Pearlson and Jillian Kwong shared research on managing digital risk in supply chains during the SIM DigiRisk SIG: Managing Digital Risk in Supply Chains and Industry 4.0 webinar. Watch the recording <u>here</u> (Passcode: j\$n84?hf)

March 10, 2025: Dr. Ranjan Pal and Sander Zeijlemaker authored an article on the <u>"Importance of boosting</u> <u>insurance-driven cyber resilience in the Generative AI world</u>" The article discusses how cyber insurance serves as a control mechanism to enhance enterprise cybersecurity while addressing the unique challenges posed by GenAI.

February 21, 2025: Our Director of Cybersecurity, Michael Siegel and research scientist Ranjan Pal co-authored an article covering four action items for managers on the most effective ways of using AI as a defense tool to improve APT (Advanced Persistent Threat) cyber-risk management in critical infrastructure. <u>"How Should Managers Use AI for Critical Infrastructure Risk Management?"</u> for Forbes India Magazine

February 11, 2025: Keri Pearlson was interviewed by the World Economic Forum on her research in resiliency and the link is <u>"Radio Davos"</u>

February 4, 2025: The CAMS team shared guidance in a <u>Thinking Forward article</u> published by the MIT Sloan School of Management, on "<u>five critical priorities that demand leaders' attention"</u>

January 28, 2025: Dr. Keri Pearlson's research was featured in an article at CSO magazine titled "<u>5 ways boards</u> can improve their cybersecurity governance."

January 23, 2025: Professor Stuart Madnick, Dr. Keri Pearlson and Michael Siegel authored an article about <u>"5</u> cybersecurity priorities that demand your attention" published by the MIT Sloan School of Management .

January 14, 2025: Dr. Keri Pearlson was interviewed by the World Economic Forum on Cybersecurity Resilience <u>"Radio Davos"</u>

January 2, 2025: Dr. Raphael Yahalom, a research affiliate at MIT Sloan School of Management was quoted in an article by Forbes <u>"FBI Investigates As U.S. Treasury Attack Confirmed"</u>