Cybersecurity at MIT Sloan

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

CAMS CYBERSECURITY INNOVATION SYMPOSIUM (CCIS)

May 15, 2024

The third annual CAMS Cybersecurity Innovation Symposium united over 120 experts, executive, thought leaders, students, and researchers to explore the next five years of cybersecurity and build roadmaps towards the future. A packed day of keynotes, panels, and small group discussions made this the best CCIS to date. Sponsored by CAMS Members, this event was made possible in part by donations from Trustwave, Baker McKenzie, and MIT ILP.

KEYNOTE WITH DARRIN JONES

In his keynote address, Darrin Jones, Executive Director of Partnerships and Planning at Interpol, underscored the evolving landscape of cybercrime and the crucial role of international cooperation in combating it. Based on his 25-year tenure with the FBI's science and technology branch, Jones highlighted Interpol's reliance on advanced databases and operational technology to tackle global crime. He emphasized that while Interpol is not a law enforcement agency, its broad network and data-sharing capabilities are pivotal in addressing universal criminal activities. Key takeaways included the need for better law enforcement cooperation, direct access to data, and significant investment in technology to outpace cybercriminal advancements. Jones warned of the increasing sophistication of transnational crime, such as double supply chain attacks and the corporatization of cybercrime, where even less-skilled criminals can deploy sophisticated operations. He advocated for adopting zero-trust and security by design principles, underscored the importance of transparency and privacy in AI applications, and called for closer collaboration between industry and law enforcement to enhance trust and effectiveness in cybercrime prevention.

PANEL: CYBERSECURITY FIVE YEARS FROM NOW

During the panel on the future of cybersecurity, experts Michael Siegel, Akhilesh Tuteja, Tom Patterson, and Cyrus Vance explored the challenges and innovations expected in the next five years. Tuteja emphasized that while emerging technologies like 5G bring advancements, the coexistence of older, less secure technologies, such as 2G, poses significant risks. Patterson highlighted the rapid advancements in cybersecurity and the need to address potential vulnerabilities associated with these developments. AI and quantum computing will dramatically alter cybersecurity, necessitating new defenses and proactive measures. Vance underscored the need for community-based approaches to safeguard localities against cyber-attacks, advocating for collaborative training and communication strategies. Despite existing disincentives, the panelists collectively stressed the importance of information sharing among companies to mitigate cyber risks. They also called for a bottom-up approach to cybersecurity education and policy, urging earlier and more comprehensive training. Additionally, they warned that integrating AI into security must be managed carefully to avoid exacerbating threats and called for an international cooperative framework to address the rising tide of cybercrime.

KEYNOTE WITH GRETCHEN BUEERMANN

Gretchen Bueermann, the Lead for the Centre for Cybersecurity at the World Economic Forum and an esteemed Keynote speaker, has issued a pressing call to action for organizations worldwide. She emphasized the need to address the alarming 30% decline in confidence regarding cyber resilience, especially among SMEs. To combat this, leaders must urgently enhance support for these vulnerable entities by developing community-driven security measures that transcend competitive boundaries. CEOs and cybersecurity leaders must collaborate to integrate cyber strategies into core business functions, ensuring cohesive and informed responses to threats. With cybersecurity costs rising, it's critical to innovate in funding and modernize legacy systems to stay resilient. Advocating for streamlined, international regulatory frameworks will reduce compliance burdens and fortify security. As

Cybersecurity at MIT Sloan

generative AI emerges as a new frontier for cyber threats, proactive investment in robust AI defenses is crucial. Finally, closing the cybersecurity skills gap through targeted education and flexible credentialing will empower all organizations to respond effectively to evolving cyber challenges.

PANEL: NEXT GENERATION (SOFTWARE) BILL OF MATERIALS

In the panel on the next generation of Software Bills of Materials (BOMs), industry experts underscored the critical need for widespread adoption and integration of BOMs into software development and business processes. BOMs are essential for building trust and managing software-related risks. To achieve this, organizations need to automate BOM processes, use standardized data formats, and embrace BOMs as valuable assets for risk management rather than just compliance tools. With the emergence of AI and cryptographic BOMs, businesses must prepare to incorporate these into their risk assessment frameworks. Stakeholders should advocate for policy and practical tooling to make BOMs easy to implement and understand. Collaboration through industry standards and audits will be essential to validate and maintain the reliability of BOMs. Organizations can significantly improve their cybersecurity posture by addressing these areas in the next five years.

PANEL: NEXT GENERATION SECURE BY DESIGN

The panel on next generation secure by design highlighted the urgent need for organizations to integrate security principles from the inception of software development. CISA's Lauren Zabierek emphasized the importance of establishing secure technology as the foundation for building resilience and trust, urging companies to adopt secure-by-design practices proactively. Bernard Gavgani of BNP Paribas stressed that security should be a collective responsibility across all business functions, not just the purview of cybersecurity teams, and that products must adhere to security benchmarks before going to market. Roger Grimes from KnowBe4 pointed out the persistent nature of common vulnerabilities, advocating for improved education and tools to enforce secure coding practices. To make secure-by-design a reality, organizations must demand security in their supply chain, automate vulnerability management, and incorporate security into their development culture and processes. Effective patch management, radical transparency in vulnerability reporting, and a focus on reducing hardcoded passwords are immediate steps that can bolster security efforts. Ultimately, the panelists agreed that without a strong commitment to secure-by-design principles, the industry risks falling behind in an increasingly complex cyber landscape.

PANEL: NEXT GENERATION OF AI

The panel on the next generation of AI focused on AI's transformative impact on cybersecurity. The experts stressed the need for immediate and strategic action to leverage AI effectively. Ray Huang from Microsoft emphasized that current AI capabilities are strong enough to significantly speed up security operations through automation and threat modeling. He urged organizations to integrate AI now to stay competitive. MIT CSAIL's Stephen Moskal warned about the limitations and complexities of AI, such as the inadequacy of current models to execute code, and emphasized the importance of transparency and trustworthiness in AI applications. Lisa Einstein from CISA pointed out that AI amplifies existing inequalities and requires rigorous frameworks for security and trust. She advocated for clear guidelines and robust evaluation mechanisms for AI's integration into critical infrastructure. Andrew Stanley of MARS advised focusing on clear problem definitions and using AI to enhance operational efficiency. He emphasized the necessity of a balanced approach between innovation and control. The panel collectively underscored the need for defenders to use AI to scale up operations and mitigate risks while remaining vigilant against the accelerated threats posed by advanced AI in the hands of malicious actors. To stay at the forefront, businesses must invest in AI now, focusing on automation, transparency, and rigorous security practices.