CAMS Cybersecurity Innovation Symposium (CCIS): A Cybersecurity Vision for 2027

June 2, 2022

CAMS held their first Cybersecurity Innovation Symposium to discuss the questions *what does cybersecurity look like in 5 years* and *what are the innovations we need to get us there*? CAMS Members and other CISOs and CIOs, researchers, thought leaders, innovators, policy makers, and students came together for a day of panels, presentations, and small group discussions on these two topics. Sponsored by CAMS, this event was made possible by donations from Arctic Wolf, ForgePoint Capital, and BitSight. Following the Chatham House Rule, only keynote speaker names are used in this summary. All other speaker, panel, and participants names have been removed.

"The innovations we need to keep us safe in 5 years are already in the labs and being developed today. Let's see what they are so we can prepare our organizations."

- CAMS Director

Dmitri Alperovitch: Cybersecurity is a Human Battle

In the morning keynote presentation, Dmitri Aperovitch, former CTO of Crowdstrike, said that, at the end of the day, cybersecurity is a human battle. The way organizations 'win' is by outsmarting the average person so they do the right thing. A community-immunity approach, where organizations focus on technologies that can enable their vendors to be more efficient and scale better, and share tools, solutions, and data are what will keep us secure in 2027. Every nation is planning for a catastrophic cyber attack, and the overlap in their response plans is nearly zero. Sharing response plans and collaboration is needed. To meet cybersecurity needs of 2027, metrics and measurement processes will be key; organizations need ways to calculate actionable and appropriate metrics for measuring cybersecurity posture without turning the process into simply a checklist. One approach is to measure speed-based metrics, such as time to respond or time to detect. These types of metrics are important for discussions with the Board (as one input to reduce risk) and are actionable, pointing to specific ways to improve.

Visionary Perspectives Panel: Infuse Code, Processes, and Organizational Design with in Cybersecurity

A panel of thought leaders shared their vision on what cybersecurity looks like in five years. Software security used to be a question of "why" and is now a question of "how," and the market is continuing to grow at break-neck speed- indicating that we have not yet found the answer to keeping us secure. In a world where everything is code-based, the key is finding ways to secure this code, and this is projected to be a $150 billion dollar market. New processes for software development, training developers to write secure code, motivating engineers to prioritize security in their designs, and implementing a supportive culture are some of the needed mechanisms.

Maintaining security is an issue of organization dynamics, great innovation, and new technologies. The staffing shortage must be fixed; hiring staff with backgrounds outside of cybersecurity provides diversity to the defense team. When it comes to organizational dynamics, supporting design teams to secure their products from the start will become the standard way to approach secure product design. Managers will continue building bridges between developers and integrators. Security is a collaborative effort beyond the designated security team; it needs to be a part of every team's mindset and plan. A holistic approach to cybersecurity, rather than a sub-optimal process of securing just through technologies, must be the mindset going forward. From the day a project is conceived, a process is designed, or an organization is formed, it needs to have cyber as part of the code, design, and the culture of the team.

About Cybersecurity at MIT Sloan

Cybersecurity at MIT Sloan brings together thought leaders from industry, academia, and government with MIT faculty, researchers and students to address strategy, management, governance and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

For more information, visit https://cams.mit.edu

Stephen Boyer: Regaining Control in an Era of Transparency

Investors, the SEC, credit-rating agencies, insurers, board members and other non-cyber leaders, are more concerned about cyber risk than ever before. Gartner suggests that cyber leaders are losing control in part because of stakeholder engagement, third party risk, and risk quantification needs. By 2026, 30% of large organizations will have publicly shared goals that include cybersecurity. This means executives need the right information to make decisions and most are not getting that today. Boards report getting reports that are too technical, not performance based, and don't contain enough benchmarking and peer comparison. Further, most boards lack enough cyber expertise. CISOs are learning that improved security performance measurement would significantly improve company financial performance, and Cyber Risk Quantification (CRQ) metrics show promise. CRQ analyzes data, identifies cyber risks, and projects costs for response/recovery from an incident, combining data with predictive analytics. This type of metric holds promise for greater transparency to all stakeholders of an organization, raising the conversation from a technology discussion to a risk management discussion. Cybersecurity management in the next five years will include new and more accurate CRQ metrics.

Technology Roadmap: AI, ML, MFA, and Data Analytics

This panel considered the technology roadmap needed to meet security needs in five years. Cybersecurity is no longer an add-on; it must be considered infrastructure. Many different technologies were discussed including multi-factor authentication (MFA), data analytics, machine learning (ML), and artificial intelligence (AI). AI and ML alone are not the solution of the future. These technologies can assist in identifying unusual behavior in systems, but not see every anomaly. Instead of focusing on technology to stop breaches, a better focus is to decrease the response times combining the power of technology and human beings. Data collection, training models about the real world, sharing to build a bigger data base, and building on historic threat info are part of the roadmap. To curb the access vulnerabilities, MFA holds promise, but not as designed today, which is still highly insecure. New architectures that provide access controls are on the drawing board.

Policy Roadmap: Partnerships, Regulations, and Incentives

This panel discussed the policy roadmap for better security. Mandatory cyber requirements for critical infrastructure, new workforce incentives, and disaster mitigation policies are on the horizon. Public- private sector partnerships empower companies and impose greater costs on adversaries. Underpinning policy is a better understanding of who and how to trust. Collaboration leads to situation awareness across the entire cyber landscape. There is a broader obligation for governments and big industry across the globe and one opportunity is to study the most effective parts of every government's approach. The British system's permeability is promising. Finding the best proxy actions, the right balance of industry/government investment, and better models for information sharing are on this roadmap.

Organizational Roadmap: Human Risk Management, Motivation, and New Social Contract

This panel shared thoughts on the organizational changes needed for cybersecurity. Human risk management is the single biggest obstacle. Training, when frequent, entertaining, redundant, and attitude-changing, instills motivation for secure behaviors and healthy skepticism about anomalies. Combating human nature includes combating security fatigue and remote work vulnerabilities. Phishing isn't going away; current responses such as encryption, firewalls, training, and awareness are inadequate. A new social contract is needed with the general population that creates and ensures a cyber ecosystem. This includes a culture of good cyber hygiene, approachable end-user security, and ingrained security through all organizations, on every level. All stakeholders have a role to play, and need motivation, examples, clear instructions, and technology support.