CAMS Cybersecurity Innovation Symposium (CCIS)

Vision of Cybersecurity in 2028

May 11, 2023

The second annual CAMS Cybersecurity Innovation Symposium gathered a collection of thought leaders to discuss the near future of cybersecurity. A morning of visionary perspectives paved way for an afternoon of action plans. Sponsored by CAMS, this event was made possible in part by donations from KnowBe4, Panzura, Trustwave, and Akamai. Per the Chatham House Rule, only keynote speaker names are identified, while all other speakers, panelists, and participants names have been removed.

Keynote with Stuart Madnick: Looking back and Looking Ahead

Cybersecurity has dynamic enemies. The better the ‘good guys’ get, the better the ‘bad guys’ get. Whether or not new cybersecurity capabilities are used for good or evil is often dependent on resources. At this time, AI is not quite as convincing as a human and deepfakes fool only a percentage of the population. Every company, however, is planning for these technologies to evolve rapidly- and preparing for increased threats. Due to a lack of human resources, automating security functions is essential. Transitional times with new technologies, policies, and regulations lead to a high-risk state. When it comes to keeping your business secure, plan for these issues now even if the threats seem futuristic. The human factor continues to be the most demanding threat for every organization- increasing the responsibility of employees to behave in secure ways should be top of mind for every executive.

Visionary Perspectives Panel: Our Picture of Cybersecurity Five Years from Now

Will cyber risk increase in the next five years? It depends on the efforts and actions of everyone and the new and defined pathways to filling cybersecurity jobs. The panel agreed that AI will be a powerful force; it will be our co-pilot in the coming years as we all adapt to this tool knowing everything from how much milk is left in the fridge to constructing a plan to improve the user’s mental health. Currently, products and software are not necessarily built with security in mind. Building with security in mind vs. building in security at the end will no longer be an innovative idea in five years, it will be standard practice. When it comes to SaaS, low-code, and no-code software, one challenge will be maintaining the security of applications and programs. The business will need to be held accountable for keeping software patched. As security grows, the need for hiring strong cybersecurity teams grows with it. As a society, encouraging skilled people to find their niche in security will improve the pathways to filling cybersecurity jobs with strong candidates.

Keynote with Craig Adams: Artificial Intelligence in Security

Technology is a useful servant but a dangerous master. AI is lowering the barrier for cyber attackers- one example is its ability to be trained to build malware. There is no choice to stop AI: it must be accepted and managed because the ‘bad guys’ already have it and will continue to learn it. Any limitations of AI at this point would simply prevent the ‘good guys’ from building defenses. We need to be smarter and think about agency, not blocking AI. The biggest concern is where the data is going when it is fed to AI. ChatGPT is a search engine capable of cybercrimes- any information it has can be used for evil. The only effective lane is privacy; constructive engagement regulation around privacy may be the main way to reign in AI. Regulation zone will be around privacy and how submitted information may be used. Crypto-agility is one method of protecting information and can be used as an incident response mechanism. Encryption replacement would be a very significant effort larger than solving the millennium bug.

> ***“It’s a pretty sure bet that the cybersecurity innovations that protect us today will not be sufficient to keep us secure five years from now. We must start now to create our secure future.”***
>
> ***- CAMS Director***

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

Innovation Panel: Quantum Computing

If quantum computing becomes operational, all forms of encryption are useless (credit cards, VPNs, etc). This threat becomes more imminent as AI can be powered by quantum computing. Putting QC on the agenda of the board becomes its own issue: the risk is still perceived to be distant in comparison to other challenges organizations face. A couple of quick actionable items to begin preparing for the threat of QC are to have a comprehensive understanding of what data is stored where and used by whom. Ensure you know how this data will be transferred to different locations and users. Include encryption agility, meaning that current encryption functionality in technology would be able to be replaced by a QC alternative. This agility should be included in vendor contracts. Increasing awareness of quantum will enable organizations to address future problems.

Innovation Panel: Next Generation Cloud

Defined briefly as “redistribution of computing”, next generation cloud may run at the edge of the internet- the surface where all devices connect. This would mean the ability to run at thousands of locations simultaneously; triggering the need for services and capabilities that only partially exist today. People will still be a threat at this level; a nonnegotiable component is protecting people from breaking the systems. Advocating for digital trust and design helps organizations stay ahead of threat actors. The only way forward may be a shared resilience model and shared exercises. Right now, insurance policies for clouds are adapting to the market; insurance becomes expensive when dealing with correlated failures. If you can decorrelate, the price of insurance goes down. In the hybrid cloud model, asset management is important to know what, where, how, and why of IT delivery. This knowledge is critical to establish correct parameters.

Innovation Panel: AI/ML and Chat GPT

In a system context, AI changes the paradigm of cybersecurity as it provides opportunities to learn much faster and try to do better. Statistical ML allows for learning from data repositories. The application of AI/ML allows us to act faster because it can process significant amount of what-if analysis, it can automate fixed resolution paths, and fix remaining issues. AI increases the attack surfaces because AI systems can be attacked and the evolution cannot be stopped. The worst scenario is that the good side pauses AI/ML adoption while the bad side continues to evolve. We should learn and explore this technology; most importantly, users and decision makers should receive guidance about how to use, what to do, and how AI affects their day-to-day life. It is essential to partner between stakeholders and decisionmakers.