Cyber Risk Management – Special Interest Group

(CRM-SIG)

CRM – SIG proposed meetings

Q1 2025
Virtual CRM-SIG Meeting

Q2 2025
Virtual CRM-SIG Meeting

Q3 2025
Virtual CRM-SIG Meeting

JOIN CAMS TODAY TO PARTICIPATE IN CRM - SIG in 2025

IDEAS MADE TO MATTER

CRM – SIG founding meeting

Last October we had the first Cyber Risk Management Special Interest Group (CRM-SIG) meeting focused on cyber risk management and cyber resilience. Through interactive dialogue with CAMs members this collaboration on the future in cyber risk and resilience research was shaped and will address issues such as:

- Harmonizing cyber risk & resilience management
- Limits to risk; how bad can it really get?
- Approaches to scale cyber insurance markets
- Levering AI to boost cyber risk management
- Systemic and supply chain cyber risk management and resilience

Managing the Ransomware Threat through an Interactive Gaming Environment

How can organizations effectively persuade their boards to allocate funds for cybersecurity? During last October's MIT CAMS members event participants utilized a ransomware simulator to evaluate the costs and benefits of ransomware defenses. Here, we share key insights from the participants' experiences.

An interactive and exploratory gaming environment allows organizations to tackle real-world problems without incurring actual risks. This approach accelerates the learning process, as the potential downsides are purely hypothetical. Think of it as learning to fly on a training simulator is both more effective and safer. Through management simulations, participants can explore various ransomware scenarios, assess the long-term impacts of their decisions, and gain an understanding of the inter-connections between security, business operations, and finances.

About CRM - SIG

The MIT Sloan School of management is the home of the Cybersecurity at MIT Sloan (CAMS) research consortium. The Cyber Risk Management Special Interest Group (CRM-SIG) is a dedicated collaborative community of executives, strategists, policy officers and researchers with a shared interest in advancing this field. More information can be found at https:// cams.mit.edu or by contacting us:

Michael Siegel
Director
msiegel@mit.edu

Ranjan Pal
Research Scientist
ranjanp@mit.edu

Sander Zeijlemaker
Research Affiliate
szeijl@mit.edu

The central question in this simulation is how, as the CEO of a fictitious organization, you can effectively safeguard against ransomware attacks over a five-year period. Players can allocate a percentage of their IT budget annually toward prevention, detection, response, and recovery initiatives.

During the first round of simulation exercises participants explored their best strategy to combat the ransomware threat. Next some heuristics about the criticality of timing, the importance of recovery. and the necessity of limiting the spreading of ransomware were shared with the participants.

Finally, during the second round of exercises participants could strengthen their best strategy with additional investment in network segmentation and anomaly detection to limit ransomware spreading.

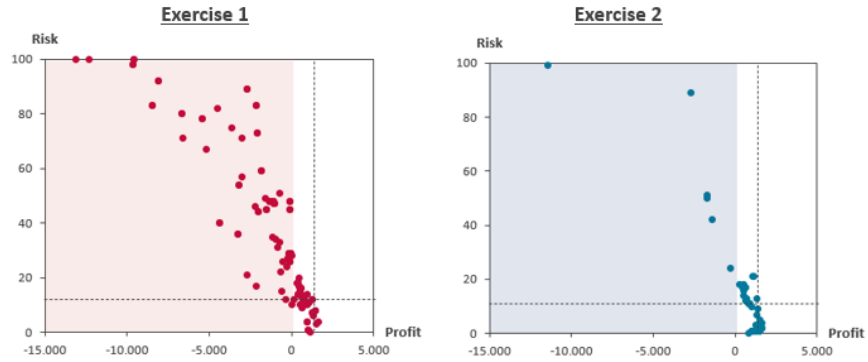

Figure 1. Accumulated profits and risks (compromised systems) outcomes from exercise 1 and 2

Figure 1 shows the simulation results of both exercises. In the first exercise 97% had an insufficient strategy. During the second exercise defense strategies were much stronger as 22% participants had an optimized strategy. Only 38% of the participants maintained high exposure to ransomware threat through under investments.

Scaling Cyber Insurance Markets to Improve Cybersecurity

Cyber insurance markets act as enterprise security controls inducers to improve enterprise cybersecurity and provide guardrails for cybersecurity strategy. However, due to the modestly effective cyber vulnerability data science that adversely affects the profitable economics of the cyber insurance market, the latter is far short of capital to service industry demand of covering exposed (systemic/aggregate) cyber-risk. The need of the hour is the design of alternative and radical cyber risk management solutions that help overcome the drawbacks of existing cyber insurance markets.

At MIT CAMS, we propose cyber insurance markets to transfer modern cyber risk through catastrophic (CAT) bonds – a financial tool widely known to boost traditional insurance capital in general. CAMS researchers leveraged the idea of the use of CAT bonds in

the traditional insurance space in the cyber insurance space and conducted a data and economic analysis to make CAT bond driven insurance markets scalable. The CAMS research team proposed conditions, pivoted upon the quality of cyber-posture information of enterprises on an insurance portfolio, when (a) CAT bonds would help boost cyber insurance capital and grow such markets, (b) self-insurance would be the effective modus-operandi for enterprises, and (c) cyber insurance and self-insurance would be ideal without the need for CAT bond product intervention.

READ ALL ABOUT IT! CRM – SIG publications

August 10th – 12th , 2023
Ranjan Pal, Stuart Madnick, and Michael Siegel, AMCIS 2023, "Catastrophe Bond Trading Can Boost Security Improving Cyber (Re-) Insurance Markets"

August 27th, 2024
Ranjan Pal , Michael Siegel and Bodhibrata Na "Three action items for sustainable cyber insurance-linked security markets"

August 4th – 8th, 2024
Prem Segar, Sander Zeijlemaker, and Michael Siegel, ISDC 2024. "Decision-making in Ransomware Capability Development: Persona-Driven Simulation"