Cybersecurity at MIT Sloan

About Cybersecurity at MIT Sloan (CAMS)

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.

Human Risk Management
Special Interest Group Virtual Meeting Summary

Dr. Keri Pearlson
April 1st, 2025

Human Risk Management Special Interest Group (SIG), more informally called the Culture Club, met on April 1, 2025 to discuss hot topics and current research on measuring cybersecurity culture. This summary covers key topics from both sessions.

HOT TOPICS DISCUSSION:

The hot topics discussed were derived from questions raised by members attending the meeting. First up was a rich discussion about how to get management buy-in on awareness. Some insights shared included managerial support starts at the top and without that support is a big uphill battle; use hard data to show that uninformed users are a risk to the company; start with 'why' and bring out short examples; use the on-boarding process to set the stage about the role managers play in preventing bad things from happening. A follow up question sought ideas for changing the view of cyber from being a blocker to being an enabler and one insightful response was to work with data science teams to undo the politics and silos.

Further discussion sought ways to increase engagement around cybersecurity other than offering points and rewards. Some suggestions included requiring engagement through quarterly simulations, offer knowledge they can apply at home and in personal life, and highlight ramifications with a 'bolo' or 'be on the lookout' campaigns that show offensive and defensive actions team members can take both personally and for the organization. Putting the 'fun hat' on was a popular approach, too. Find ways to make the engagements so fun and, well, engaging that team members look forward to the next one.

The next topic asked about individual risk scores. Who has investigated creating or using 'individual risk scores' on people and what might be included. The attendees suggested training completed, phishing scores, building specific inputs based on privilege access and reinforced training, phishing reporting (and 'see something, say something').

The final topic asked about handling repeat offenders on phishing without being punitive. Other than training and 'just in time' learning modules to show repeat offenders how to recognize phish, attendees suggested that one-on-one conversations with repeat offenders might be really useful because there might be mitigating circumstances (such as multitasking, inability to really read a email without opening it, or job descriptions that require all emails to be opened and read).

RESEARCH DISCUSSION: MEASURING CYBERSECURITY CULTURE:

Keri Pearlson, the leader of the SIG, presented ongoing research she and her team are conducting to build a measurement tool and process for evaluating cybersecurity culture and suggest actionable insights on how to improve effectiveness. Building on the MAPS framework shared at the CAMS October 2024 members meeting, Keri shared a process for measuring culture that includes both an assessment of employee and leader perceptions and attitudes, and an inventory of specific components that create culture. She then shared early results from a pilot test of these tools and plans for the next steps. She's seeking 1 or 2 additional organizations who might want to better understand how their investments in cybersecurity culture are working to be pilot testers of this methodology. If your organization is interested, please contact Keri at kerip@mit.edu for more information.