Perusing Watermelon Risks to Strengthen Cyber Resilience

GOAL: Combatting the illusion of control that foster unintended lapses of control

Dr. Sander Zeijlemaker, Dr. Ranjan Pal, Dr Michael Siegel

Cybersecurity at

MIT Sloan

1. Watermelons: only green on the outside

Watermelon risks* are categories of risk that seems to be under control (green) but only by detailed and thorough analysis their real nature (red) becomes visible. An example:

Senior management report states customer care process is under control while the unit has a massive number of customer complaints.

Principles of materiality and control tolerance makes them very hard to observe and they often remain hidden.

*Ellis, G. (2018). The "watermelon effect" -- does a green dashboard mean a healthy facility? Loss Prevention Bulletin . Dec2018, Issue 264, p21-23. 3p
* White paper (2017). Avoiding the 'watermelon' effect. Are we doing enough in the process industry to prevent the next major incident? ABB Process Safety
* Ellis, G. & Ellison, C. (May 1, 2019). Avoiding the 'watermelon' effect in the process industry, IIoT world.com
* Ibrahim, S. (September 20, 2017). Avoiding the watermelon effect, PCN Europe.

3. Simulation allows for timely intervention

Individual reasonable functioning security controls as confirmed in the strategic dashboarding caused the current cyber risk management strategy to be perceived as reasonable.

Our simulation approach allows to aggregate the effect of individual lapses of control across the different steps of a cyber attack.

This aggregation effect in terms of number of incidents was beyond managerial risk appetite and made watermelons risks visible, providing management insights to take timely action.
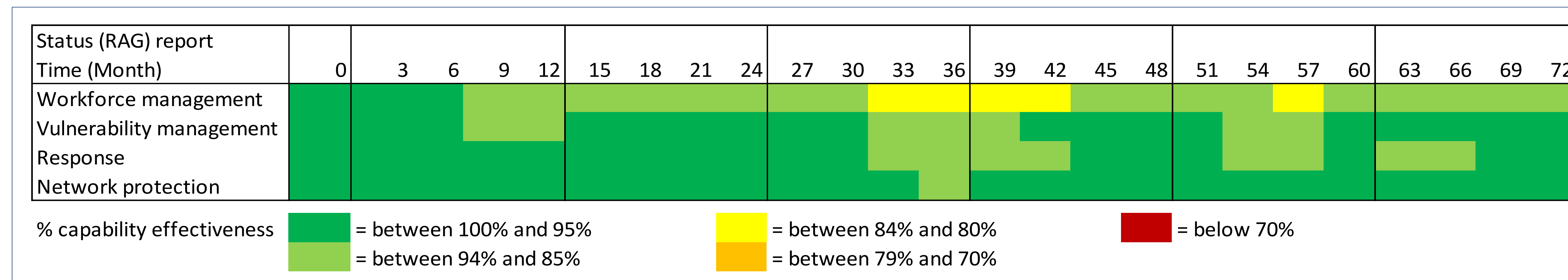
We advocate to augment strategic dashboarding with digital twin technology

We want to hear your watermelon risks
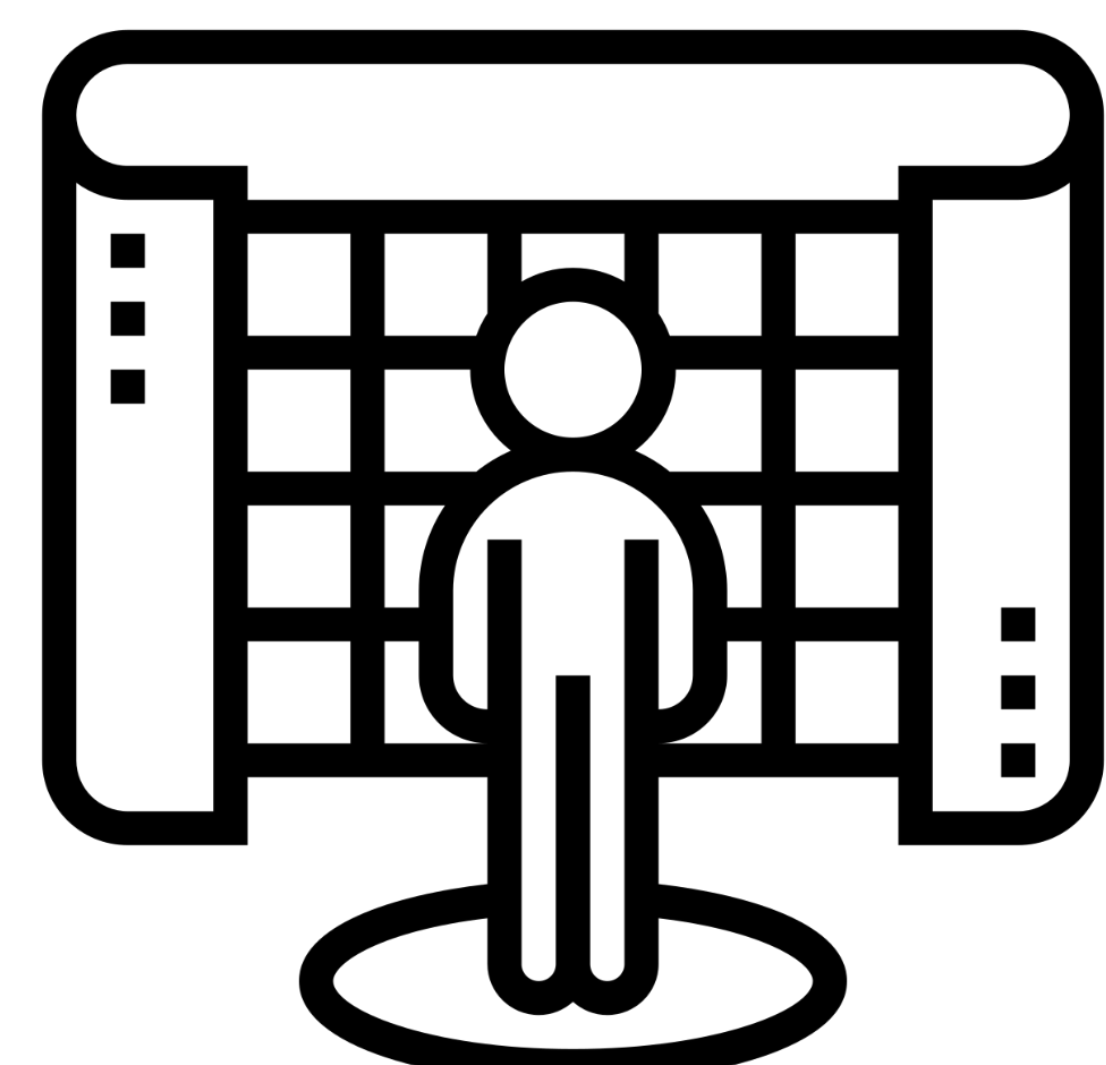Contacts: szeijl@mit.edu, ranjanp@mit.edu, msiegel@mit.edu

2. 4 – step approach to identify watermelon risks through digital twin usage

1. Get understanding about company and strategic dashboarding

4. Compare results

Status (RAG) report Time (Month)	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72
Workforce management																									
Vulnerability management																									
Response																									
Network protection																									

% capability effectiveness
= between 100% and 95%
= between 94% and 85%
= between 84% and 80%
= between 79% and 70%
= below 70%

2. Mimic organisation in calibrated strategic digital twin

3. Simulate future performance of cyber risk management strategy and capabilities (groups of security controls)

Security Incidents — historical data / simulated future performance; Risk appetite; Number of incidents vs Time (Month); 50%, 75%, 95%, 100%

Response; Vulnerability management; Workforce management; Network protection (maturity vs month)