



# Human-centered interface design for a cyber-risk group-based training game

Dr. Tony Delvecchio, Dr. Sander Zeijlemaker, Dr. Giancarlo De Bernardis & Dr. Michael Siegel

BV'TECH



## 1. Group-based game for Cybersecurity training

Board members who are responsible for financial, operational, and business decisions also need to decide on cybersecurity investments. However, they are often not skilled in this last matter.

This brings to two focal points: (1) decision making is a group process, and (2) cybersecurity training is crucial. We developed a security game with a specific user interface that leverages collective intelligence and strengthens cyber risk management decision-making.

## 2. Guided learning in understanding performances

Our learning framework (Figure 1) guides the learning process and helps participants to understand how their actions affect the financial performance and risk exposure.

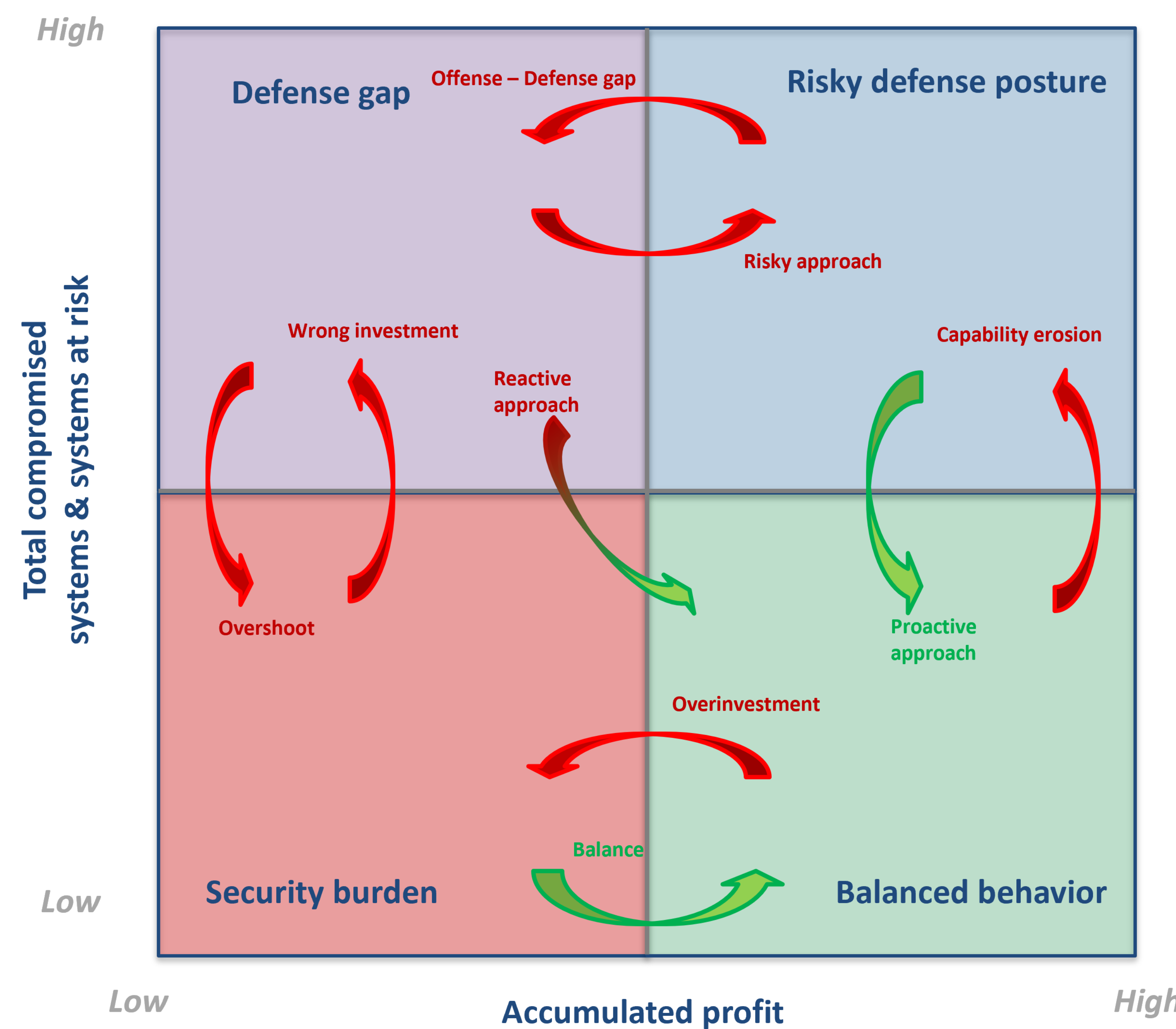


Figure 1. Learning framework

## 4. Leveraging on collective intelligence makes better results

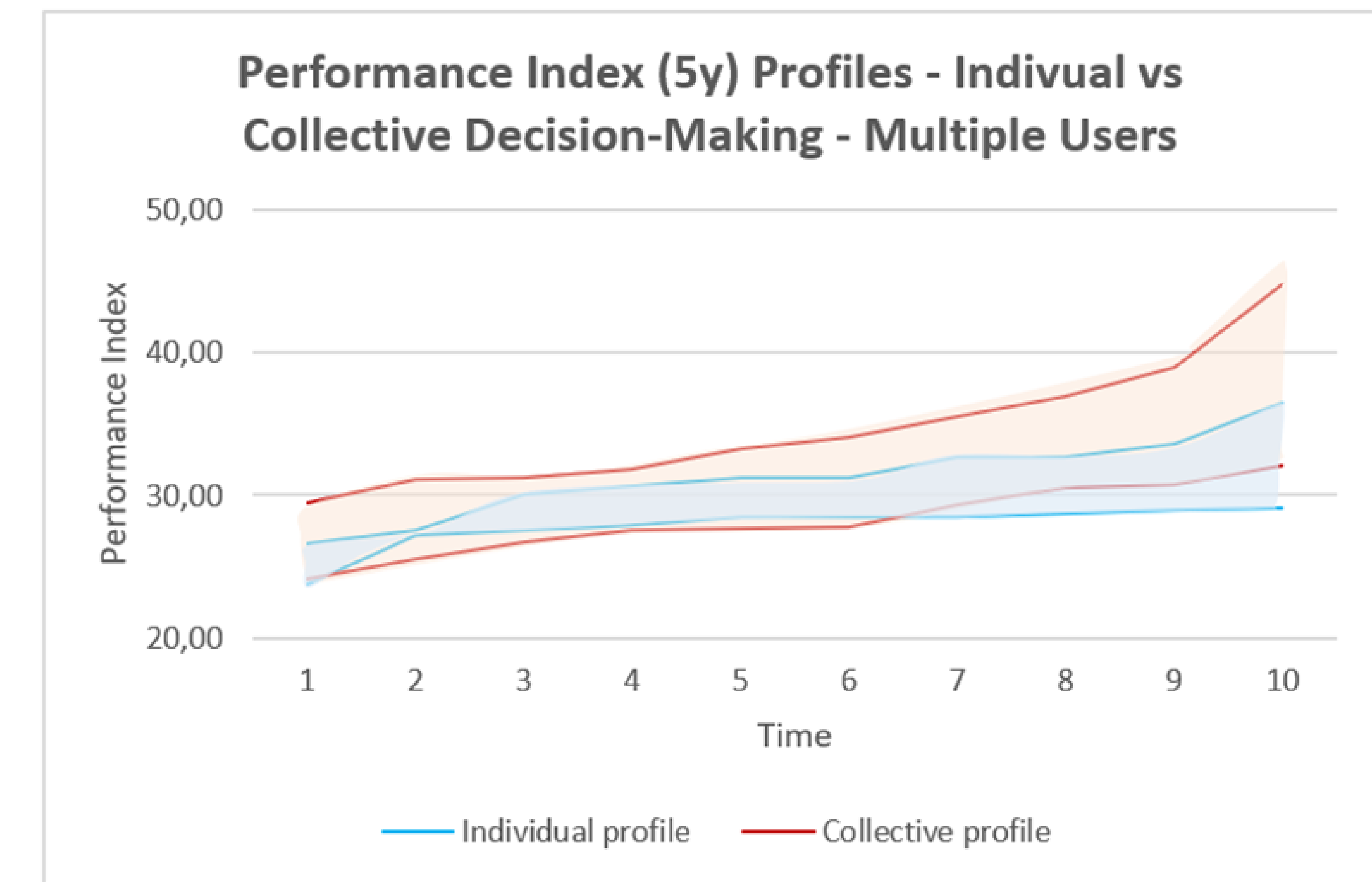


Figure 2. Comparison of groups vs individuals

Groups perform better and learn faster compared to single users (Figure 2). The gap between skilled and unskilled users is narrowed and that helps in reducing the impact of cyber-attacks. Through collaboration a better understanding of cyber risk management can be achieved, and this improves financial performance and reduces risk levels substantially.

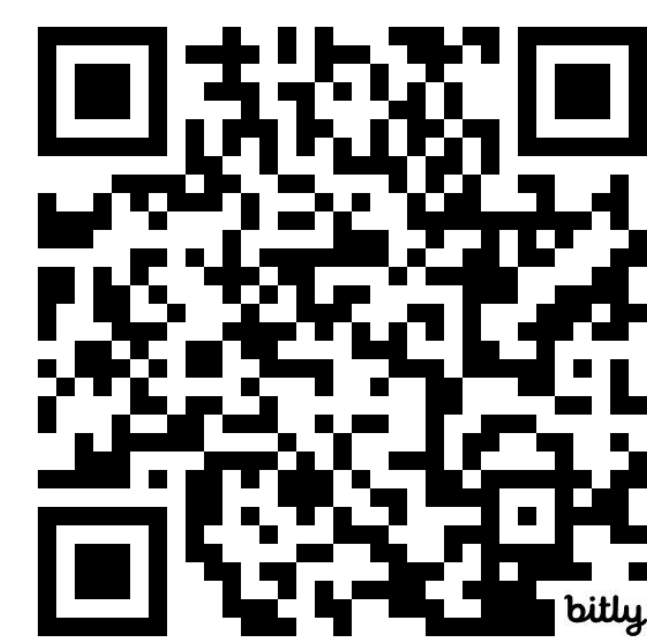
## 3. Importance of understanding cyber-risks

The game output allowed us to establish learning paths: - from a high risk with low profits to a high risk with high profits, and finally to a low risk with high profit - demonstrating how important it is to understand cyber-risk's financial and business consequences.

## 5. Game application

The game can provide valuable support to CISOs in helping other executives (such as CEOs, CTOs, and CIOs) realize the value of investing in cybersecurity as an investment for the company's success.

Access our paper



Inquiries: [tony.delvecchio@bvtech.com](mailto:tony.delvecchio@bvtech.com),  
[s.zeijlemaker@mit.edu](mailto:s.zeijlemaker@mit.edu),  
[giancarlobernardis@bvtech.com](mailto:giancarlobernardis@bvtech.com),  
[msiegel@mit.edu](mailto:msiegel@mit.edu).

This work was supported in part by the Fondo Europeo di Sviluppo Regionale Puglia Programma Operativo Regionale (POR) Puglia 2014-2020-Axis I-Specific Objective 1a- Action 1.1 (Research and Development) Project Titled: CyberSecurity and Security Operation Center (SOC) Product Suite by BV TECH S.p.A., under grant CUP/CIG B93G18000040007.

