1. Uncertain investment paths in cybers risk management

Decision makers face the task of implementing a cybersecurity program to minimize cyber risk and maximize profits. Organizations encounter a multitude of capability investment options, posing the challenge of strategic resource allocation – where, what, and when to invest.

The risk reward paradox shows that similar profit outcomes have different risk profiles and the other way around. All this, while having the same capability investments options available.

2. Business simulation offers forward-looking insights

We use a simulation that mimics the corporate decision environment. This enabled us to collect insights on profits and compromise systems (risk).

Our study (see Fig. 1) found four different strategic investment profiles. The most effective one in Quadrant 4 (low risk, high profits) that:

- Yields 30% less compromised systems (risk) and 6% more accumulated profit (reward).
- Demonstrates proactive investment in prevention followed by strengthening detection & response.
- Shows that investments change over time to align cyber risk with business needs.

3. Four investment profiles; one is highly effective

Figure 1. Quadrant analysis of game simulation

4. Play the simulation and experience the difference

Cybersecurity Simulation

Objective
This simulation is intended to help you experience the complexities in cybersecurity management, and how it may impact your business, given attacks.

Resource allocation
Assume that you are the CEO of a hypothetical company. You have the capability development. You can determine 'what percentage' and 'why' cybersecurity has two main effects:

Contacts: gk103@wellesley.edu, szeijl@mit.edu, msiegel@mit.edu