What is the Optimal Level of Cyber Security Investment?

Background

Cyber risk relevance and its impact on industry recently increased significantly, rising from the fifteenth top business threat in 2013 to third in 2017 [1]. This escalation is due to society's increasing digitisation extending ICT systems' attack surface, which forms the backbone of advanced economies. Securing these systems is often complex and expensive, giving malicious actors numerous opportunities to exploit them [2], [3].

This study aims to produce a model that offers a scientific basis for high-level decision-making concerning the optimal investment in cyber security across various industries. It will consider investment in cyber security tools and human knowledge based on the Cyber Security Body of Knowledge (CyBOK) framework.

The Challenge

Firms must prioritise mitigating specific threats and vulnerabilities due to the probability and scope uncertainties of potential attacks. However, as historical data is a poor proxy and insufficient for well-grounded cyber risk predictions, determining which potential cyber security incidents to prepare for is a challenge [4].

Potential Methodology

Threat Model Attacker-centred threat model to uncover industry-specific vulnerabilities. Also, helps to determine the marginal benefit of cyber security investment.

Game Theory Captures the contradictory goals of defenders and attackers effectively.

Calculating cyber security vulnerabilities and optimal investment from only an economics-perspective is typically unrealistic and restricted without incorporating the technical viewpoint. Integrating an attacker-centric threat model requires less specific organisational data than most asset- and software-centric threat models. Also, it can be more generalisable across various industries. A threat model enables the quantification of the most potentially frequent and critical cyberattacks a corporation faces. This information will provide a more holistic insight into the firms' cyber vulnerabilities as well as the key actors and interdependencies before applying game theory.

Research Questions

- Which industries will be the early adopters of this model? Which ones will have more difficulty?
- What impacts could a model of this nature have on an entire sector?
- How does the model's analysis potentially differ when considering short- versus long-term cyber security investments?
- Which industries would find the model most applicable to their business framework?
- How does the model's pertinence vary concerning firm size?

Key Outcomes

- A model that provides firms with the means to determine the optimal investment in the necessary cyber security tools and human knowledge.
- Incorporating a threat model should expose cyber security vulnerabilities within an industry without relying on restrictive assumptions made in purely economic-based models as well as enable it to reflect cyber security's dynamic nature.
- CyBOK provides a clear and structured framework to better model human knowledge and its value to industry while showing that a knowledge framework can enable this type of modelling.

References

[1] J. Simon and A. Omar, "Cybersecurity investments in the supply chain: Coordination strategic attacker," European Journal of Operational Research, vol. 282, no. 1, pp. 161–171, 2020.

[2] A. Opher, A. Chou, A. Onda, and K. Sounderrajan, "The rise of the data economy: Driving value through internet of things data monetization," International Business Machines (IBM) Corporation, Report, 2016.

[3] J. A. Lewis, "Economic impact of cybercrime," Center for Strategic and International Studies (CSIS), Report, 2018.

[4] A. Asen, W. Bohmayr, S. Deutscher, M. Gonzalez, and D. Mkrtchian, "Are you spending enough on cybersecurity?" Boston Consulting Group (BCG), Report, 2019

By: Zaina Dkaidek
Email: zd420@bath.ac.uk
Supervisors: Dr Joanna Syrda, Dr Adam Joinson, Dr Matthew Edwards

UNIVERSITY OF BATH

University of BRISTOL