Longitudinal Breach Research

GOAL: Understand the systemic structures to drive success and failure in cyber risk management

Dr. Sander Zeijlemaker, Michiru Ishikawa, Dr Michael Siegel

1. Success or failure of cyber risk management

Some organizations are more resourceful after a breach *(e.g., Maersk, Equifax, Norsk Hydra)*, while others may not even survive *(e.g., DigiNotar, Ranch Medical, Yapian)*. Seemingly there are routes to success and failure.

2. Strategic decisions have a major role

The dynamic approach to cyber risk management focusses on unintended long-term consequences. This approach suggests that the route to success or failure is determined by strategic choices prior to the breach or after the breach [1-4].

Critical areas for decision-making are:

- Cyber Risk Strategy Implementation:
  - Cyber Threat Perception.
  - Capability Performance.
- Stakeholder management:
  - Controlling the breach impact.

Contacts: szeijl@mid.edu, msiegel@mit.edu

3. We apply a new perspective to the post-mortem: a longitudinal research approach

Traditional post-mortem research focusses on missing capabilities at the moment of the breach. Following the dynamic approach to cyber risk management, this research takes a longitudinal research approach and considers a longer period before and after the breach. Figure 1 shows our research framework with detailed research questions.

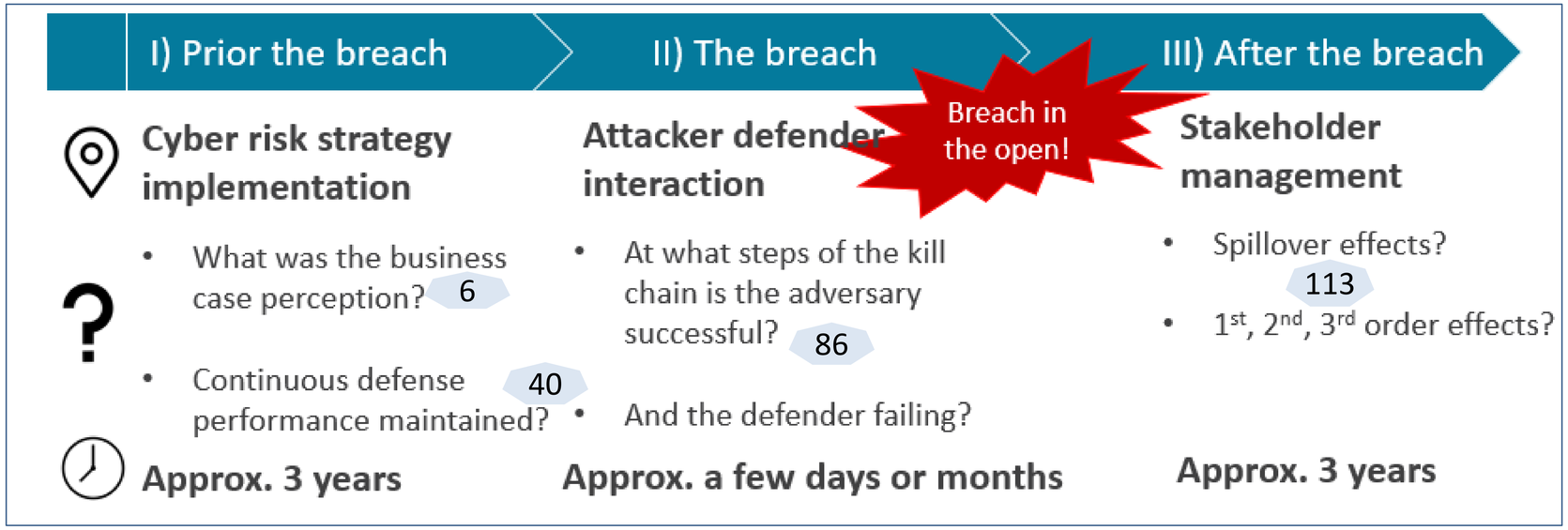

Figure 1. Framework for Longitudinal Breach Research and Plotted Number of Datapoints (6)

4. Work in progress allows early adaptor involvement

So far, our research data base contains:

- 8 well known breaches *(Equifax, DigiNotar, Norsk Hydra, Maersk, Kesaya VSA, Maastricht University, Solar Winds, Colonial Pipeline).*
- Examined 70 breach related documents
- 355 findings *(245 are positioned in the framework (see Fig 1); 110 require further examination).*

5. How do you monitor continuous performance of security capabilities?

Preliminary insights raise the following cyber risk governance questions:

- How do you monitor continuous performance of implemented security capabilities?
- How do you ensure securing the right business value (e.g., maintain right threat perception)?

We appreciate (1) receiving your breach insights, or (2) having an interview with you about this topic

References:

1. Zeijlemaker, S. (2022, March 16). Unravelling the dynamic complexity of cyber-security: Towards identifying core systemic structures driving cyber-security investment decision-making. Radboud University (342 pag.) (S.l.: s.n.) Supervisor(s): prof. dr. E.A.J.A. Rouwette & prof. dr. M. von Kutzschenbach. (Doctoral Thesis).
2. Zeijlemaker, S. & Siegel, M. (2023). Capturing the Dynamic Nature of Cyber Risk: Evidence from an Explorative Case Study, Hawaii International Conference on System Sciences (HICSS) – 56, 2023 January 3rd – January 6th, Hawaii.
3. Zeijlemaker, S., Siegel, M., Khan, S., Goldsmith, S. (2022, August, 4). How to align cyber risk management with business needs. World Economic Forum, Cyber Security Working Group.
4. Zeijlemaker, S., Rouwette, E., Cunico, G., Armenia, S. & von Kutzschenbach, M. (2022). Decision-Makers' Understanding of Cyber-Security's Systemic and Dynamic Complexity: Insights from a Board Game for Bank Managers. MDPI systems, 10 , 1-25.