Navigating through the global cybersecurity landscape: Exploring our ability to mitigate future cyber threats.

Dr. Sander Zeijlemaker, Iris Zeijlemaker, & Daniel Zeijlemaker

1. Digital society evokes cyber threats

The world's increasing interconnectedness and dependence on technology have led to cybersecurity becoming a critical factor for the functioning of society. However:

- 25% of Fortune 500 companies suffer from significant and costly breaches *(Cynthia Institute, 2021)*.
- 60% of SMBs are out of business within 6 months of a severe attack *(Small Business, Big Threat, 2015)*.

2. Cyber threat landscape is complex

Navigating through the complex landscape of cybersecurity is a difficult task due *to* *(Zeijlemaker & Siegel, 2023)*:

- Increasing digitalization of society.
- Faster adversarial evolution.
- Increasing cybersecurity workforce shortage.
- The wider societal impact of materialized cyber threats.

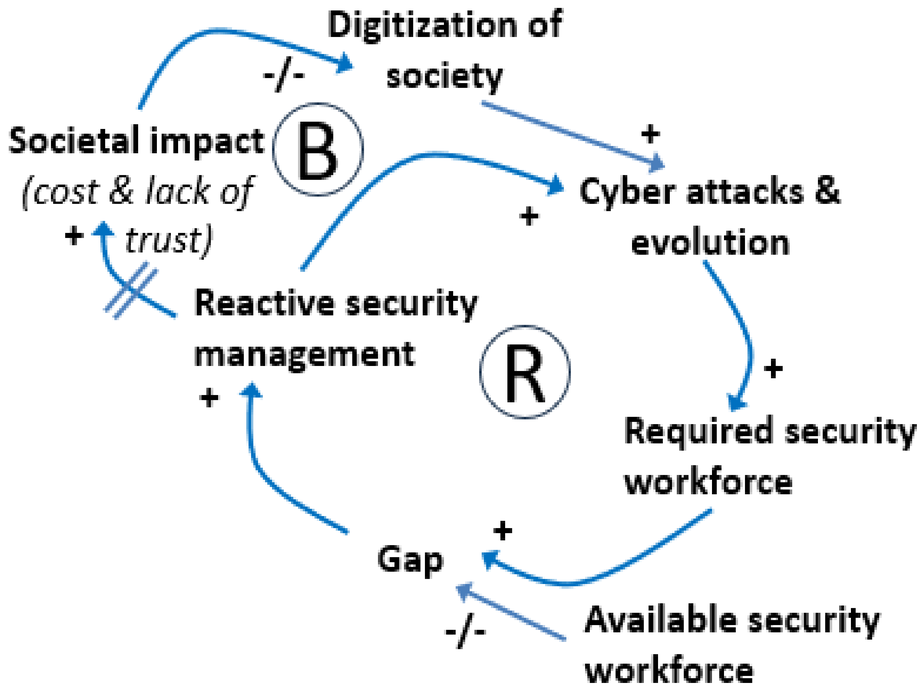

Figure 1. Cyber theat dynamics in digital society

3. Currently, we miss the urgency to anticipate threats

We perceive our society to be secure:

- Only 57% of decision-makers expect to be hit by a cyberattack.
- 93% of decision-makers have confidence in their organizations' implemented cybersecurity best practices.
- 50% of these organizations lack some standard but critical defense measures *(Whitmer 2022)*.

Currently, society faces a significant security staff shortage and a significant cyber cost increase.

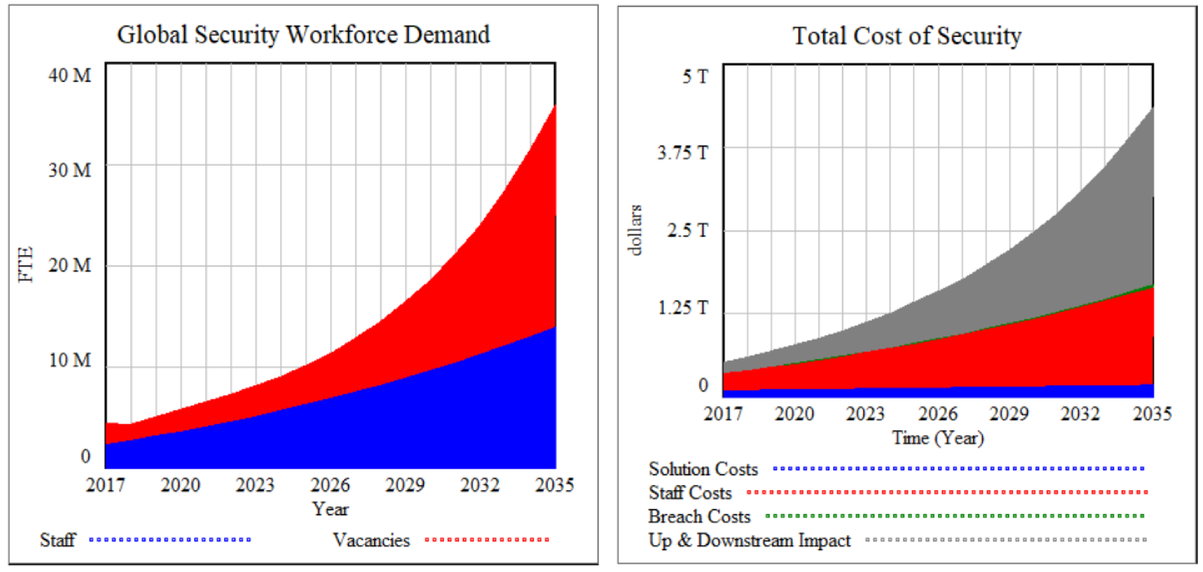

Figure 2. Base run cost of security and security workforce demand

4. Way forward

Currently, increasing the security workforce through training and recruitment is not a sustainable solution. Therefore, we recommend:

1. Increasing the pace of automation and embracing the application of Artificial Intelligence and Machine Learning in the field of cyber security to foster productivity.
2. Focusing on the principles of secure by design to limit vulnerabilities in technology. Product liability, as governed by the cyber resilient act, becomes an essential tools for compliance.
3. Implementing proactive security management to align organizational needs with cyber risk and strengthen security posture before attacks happen *(Zeijlemaker et al., 2022)*.

Contacts: s.zeijlemaker@disem-institute.com