Cyber Risk Management Support Tools

Goal: Identify and compare quantitative methods that can help companies/ firms better their cyber decision making skills

Angela Mgbeke, Dr. Sander Zeijlemaker, Dr. Michael Siegel

Uncertain environment requires tools for quantification

In complex and dynamic environments, cyber leaders need to make decisions regarding cyber risk management strategies that also need to support business strategies (see Fig 1).

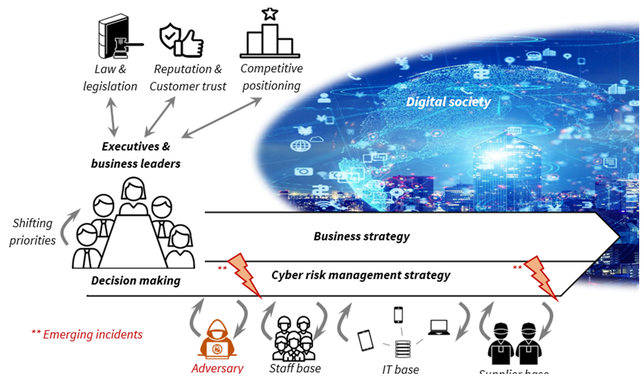

Figure 1. Model: the complex dynamic cyber risk management environment

This creates a dilemma for cyber risk analysts causing them to become uncertain about decision making which has the ability to lead to costly breaches where data is lost or systems can be subject to ransomware. As a result, a vast range of cyber risk management tools are created to help them with this uncertainty and prevent these negative outcomes. This raises the question of what kind of tools help executives and business leaders effectively assess their cyber risk.

Management's needs differ often from acquired tools

"By 2025, 50% of cybersecurity leaders will have tried, unsuccessfully, to use cyber risk quantification to drive enterprise decision making." (1)

Different quantification tools for different purposes

- Doppler: prioritize security investments over criticality of assets.
- System dynamics: prioritize future security roadmap under condition of changing internal and external environments.
- Fair CAM: optimize current control structure (limit loss, reliable performance, decission making)
- BBN: recognize probabilities nature of attack and defense.
- CyVar: expected loss calculation for cyber security

Our framework relates tools to uncertainty

- Defined a framework for distinguishing how different types of cyber risk management decision support tools will address these different forms of strategic uncertainty.
- Analyzed cyber risk management quantification tools in more detail by selecting five leading quantification tools and compared each of these tools using the evaluation criteria we derived from literature research.
- Defined an evaluation criteria consisting of risk management foresight, scope, prioritization, and identify capability erosion for comparing the support tools. (See table 1).

	Evaluation Criteria				
Support Tools	Risk Management Foresight	Optimize Prioritization	Multilayer	Identify Capability Erosion	Scope
System Dynamics	++	++	++	+	++
CyVar	+	0	+	--	0
BBN	+	0	+	--	0
FAIR CAM	+	++	+	+	0
Cyber Doppler	+	++	+	--	++

Table 1: Table with support tools, evaluation criteria, and their rankings. Key is ++ = stronger, + = strong, 0 = neutral, - = weak, -- = weaker.

References:

1. Gartner unveils top eight cybersecurity predictions for 2023-2024. Gartner. (n.d.). Retrieved April 8, 2023, from https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024