## Cyber risk governance as differentiator in resilience

**GOAL:** strengthen control over cyber risk



Dr. Sander Zeijlemaker, Michiru Ishikawa, Dr. Michael Siegel

The often used, technical, and operational focus of cyber security cause barriers in understanding while it is essential to have a strategic focus on cyber risks that is aligned with business and finance. This is why we research breaches\* following the life-cycle of the cyber risk management strategy. Our research focus on 1 to 3 years before and after the moment the breach was in the open.

## Findings:

- The life-cycle of a cyber risk management strategy has four stages.
- Each successful breach\* follows a similar pattern across these (declining) stages.
- Certain decline is self-inflicted (see 2) and therefore improvement is also within our own control by *following* cyber risk governance principles (see 3).
- at every stage and therefore strengthens your cyber risk management strategy (at lower costs).
- You can stay ahead of the curve by *interactive* and explorative learning through digital twin technology.

b	Governance &	Design & implement	Eco-system	Revive or E
1	assess cyber risk	defenses	collaboration	perish
	<ul> <li>Strategic misalignment (50%)</li> <li>Prioritization issues (100%)</li> </ul>	<ul> <li>Eroding defenses create entry points (88%)</li> </ul>	• Lawsuit, settlements & fines (50%)	Owners impacted, or bankruptcy (38%)
	* Unobserved eroding defenses (88%)	<ul> <li>Poor network design (88%)</li> <li>Poor detection &amp; response strategy (63%)</li> </ul>	<ul> <li>Strong (62%) vs poor (38%)</li> <li>stakeholder mgt</li> </ul>	* Improve strategy & cyber enables business (50%)
)	<ul> <li>Use cyber security as business enabler</li> <li>Align cyber risk with business needs</li> <li>Incorporate cybersecurity expertise into board governance</li> </ul>	<ul> <li>Ensure organizational design supports cyber security</li> <li>Understand the economic drivers and impact of cyber risk</li> </ul>	* Encourage systemic resilience & collaboration	"The adherence to cyber risk governance principles determines how organizations will revive or perish in future"
)	<ul> <li>Re-evaluate capability</li> <li>Re-assess threat landscape</li> <li>Discuss risks in business, &amp; financial context</li> <li>Set risk appetite</li> </ul>	<ul> <li>Continuously monitor state of defenses</li> <li>Adhere to architectural design</li> <li>Assess defenses proactively (PtAAS, attack surface mgt, EPSS, etc.)</li> </ul>	<ul> <li>Direct security supplier         management (real-time         evaluations)</li> <li>Strengthen ecosystem (joint         exercises, information sharing,         helping, create network)</li> </ul>	

Digital twin technology allows to simulate (1) future state of defenses & eco-system resilience, (2) identify early unintended lapses of control & capability erosion, and (3) identify early unintended recovery delays & multi order impact after breaches. A typical simulation approach allows to look 5 years ahead.