THORSTEN KRAFT

Executive Security Architect | Cyber & Technology Risk | Critical Infrastructure | Zero Trust

PROFILE

Thorsten Kraft provides independent, academically grounded judgement on cyber and technology risk in highly regulated and safety-critical environments. His work supports boards and supervisory bodies in exercising effective oversight where cyber risk has direct operational, regulatory, and societal impact.

He combines a strong academic foundation in computer science and information security (BSc, MSc, PhD) with a hybrid military and civilian background in security-critical environments. His experience spans analytically driven academic work, military decision-making under pressure, and civilian governance and regulatory contexts, enabling independent judgement across operational, strategic and oversight levels. This hybrid background allows him to assess cyber and technology risk through the lens of accountability, escalation logic and real-world consequence management at board and supervisory level.

EXECUTIVE SNAPSHOT

Independent judgement on cyber and technology risk in regulated and safety-critical environments. Trusted advisor to boards and supervisory bodies on governance, accountability and escalation in high-impact cyber scenarios.

Combines academic depth, military decision experience and regulatory oversight expertise.

CONTRIBUTION

Provides boards and supervisory bodies with clarity, structure and confidence in environments where cyber security intersects with regulation, operations and public accountability. Focuses on oversight, assurance and decision quality — not operational execution.

CONTACT

Thorsten Kraft
Rathausstrasse 28
33397 Rietberg
Germany

Mail: thorsten.kraft.privat@gmail.com
Mobile: +49 1520 3292266

EXPERIENCES

Cyber & Technology Risk Oversight

I have repeatedly supported boards and supervisory bodies in assessing cyber and technology risk, based on direct exposure to complex environments and real executive decision situations where accountability and risk ownership were central.

Zero Trust & Least Privilege (IT & OT)

I have designed, implemented and governed Zero Trust and Least Privilege architectures across heterogeneous IT and OT landscapes, including legacy-heavy, high-availability and safety-critical environments under strict operational constraints.

Critical Infrastructure & Resilience (KRITIS)

I have built extensive experience working in KRITIS-regulated contexts, advising on cyber risk, resilience and systemic dependencies where operational continuity, safety and societal impact must be assessed together.

Regulation, Assurance & Frameworks

I have applied BSI IT-Grundschutz, NIST-based frameworks and related standards across multiple engagements, using them as governance and assurance instruments to support defensible, regulator-aligned board decisions rather than compliance exercises.

Security Operations & Crisis Oversight

I have overseen security operations and crisis governance during incidents exceeding operational control, supporting executive and supervisory decision-making under time pressure and uncertainty, embedding AI-supported decision support within defined governance frameworks, while preserving clear human decision authority and accountability and ensuring forensically robust, audit-ready documentation.

ACADEMIC & EDUDACTIONAL BACKGROUND

I completed the **Talpiot Program of the Israeli Defense Forces between 1996 and 2002**, an elite track combining academic studies in computer science and cognitive psychology with parallel military training and early leadership responsibility in security-critical national defense contexts. Within this framework, I earned my **Bachelor of Science in Computer Science**, while simultaneously serving in demanding operational and training environments. **During and following this period, I served within** Unit 8200 (IDF), gaining operational experience in intelligence-driven analysis and cyber-relevant, high-consequence settings, ultimately leaving the service at the rank of Major. I subsequently pursued advanced academic training at the **University of California, Berkeley**, earning my **Master's and Ph.D. degrees in Computer Science (Information Security) from 2007 to 2010**, with a focus on cyber threat mitigation strategies, security architectures and risk evaluation, forming the scientific foundation for my board-level advisory work.

Microsoft Most Valuable Professional (MVP), 2010
Recognized for contributions to the mitigation and containment of the Conficker malware outbreak, supporting analysis, defensive strategies and coordinated response efforts during a global high-impact cyber incident.

Confidentiality Notice: Due to strict confidentiality and non-disclosure obligations with former clients and contracting partners, I am unable to publicly disclose details regarding specific employment, mandates or engagements. Upon request, I am, however, in a position to facilitate appropriate reference contacts for verification and further discussion.