DOI 10.5817/MUJLT2025-2-8

# BRIDGING THE GAP: A REVIEW OF CYBERSECURITY FÜR MANAGER

*by*

JAN HOSPES *

*Pufahl, M. Paulsen, P. and Arndt, P. (2024) Cybersecurity für Manager Cybergefahren wirksam begegnen – das Kompetenzmodell für die Praxis. Wiesbaden: Springer Gabler, 113 p.*

## 1. INTRODUCTION

As legal and operational consequences of cyber incidents mount, particularly with the EU's NIS2 Directive's provisions aiming at management, the need for cybersecurity literacy among executives is urgent. In this context, *Cybersecurity für Manager: Cybergefahren wirksam begegnen – das Kompetenzmodell für die Praxis*[1] seeks to equip business leaders with a structured and accessible guide to understanding and managing cyber risks. This book is aimed squarely at non-technical executives—CEOs, managing directors, board members—and emphasizes management-level accountability, strategic integration, and practical measures. English-language markets have rather long offered management-oriented cybersecurity texts.[2] Starting around 2020, there has been an increase in the number of cybersecurity books aimed at management in English[3] In 2022, the German-speaking region was served

* Ph.D. student, Masaryk University, Faculty of Law, Institute of Law and Technology. E-mail: jan.hospes@gmail.com

1 Pufahl, M. Paulsen, P. and Arndt, P. (2024) *Cybersecurity für Manager Cybergefahren wirksam begegnen – das Kompetenzmodell für die Praxis*. Wiesbaden: Springer Gabler, 113 p.

2 Touhill, G. J. and Touhill, C. J. (2014) *Cybersecurity for Executives: A Practical Guide*. New Jersey: Wiley & Sons, 386 p.

3 Blum, D. (2020) *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*. Berkeley: Apress, 333 p.; Parenty, T. J. and Domet, J. J. (2019) *A Leader's Guide to Cybersecurity: Why Boards Need to Lead–and How to Do It*. Brighton: HBR, 240 p.; Houchin, D. (2021) *Cybersecurity for Executives, Managers, and Leaders: Arcane Knowledge of the Dark Art for Superior Decision Making: The Cyber Kill Chain*. Ad Hoc Press, 89 p.

with *Chefsache Cybersicherheit*[4] published in 2022, with which the book in question, *Cybersecurity for Managers* shares the market and which tends to focus on sources of risk and measures. By contrast *Cybersecurity for Managers* presents a more abstract perspective that includes governance principles, which can certainly be seen as a unique selling point in the German-speaking market.

## 2. STRUCTURE AND KEY AREAS

The book opens with a suite of cybersecurity trends including high-level technologies—such as artificial intelligence, quantum cryptography, and Zero Trust architectures. In the following *Cybersecurity für Manager* is structured around a conceptual "Cybersecurity Competence Model" composed of a core and concentric rings. The model addresses the fundamental question: *Why* should an organization care about cybersecurity? Here, legal obligations, reputational risks, and financial exposure are discussed. The middle ring concerns *what* needs to be protected, spanning data, human factors, and infrastructure. The outer rings focus on *how* to protect it—covering governance, assessments, security operations, digital identity management, and Zero Trust architectures.

This is followed by the main part of the book, which is dedicated to the outer rings of the mentioned model. Risk management is presented as the central element of implementation, detailing a process that includes asset identification, threat modeling, and prioritization of countermeasures. Further key points of implementation include digital identity and access management and the application of Zero Trust principles are introduced.

The final chapter contains interviews with cybersecurity experts who provide insight into topics covered in the book, such as identity management and zero trust architectures, as well as new topics such as management of cybersecurity during large-scale events.

[4] Köhler, T. R. (2021) *Chefsache Cybersicherheit: Der 360-Grad-Check für Ihr Unternehmen*. Campus Verlag, 272 p.

## 3. ASSESSMENT OF THE CONTENT

The introduction of advanced topics seems more akin to optimization layers than foundational building blocks of a cybersecurity management system. For managers who engage with cybersecurity as a governance and compliance challenge, this emphasis may obscure more immediate priorities: understanding their current risk posture, ensuring incident readiness, and establishing basic control structures. In this sense, the book opens with the "cherry on top" of a cybersecurity strategy, potentially diverting early attention away from the groundwork most urgently needed in non-technical leadership circles. For comparison, *Cybersecurity for Executives* provides guidance on how to develop a cybersecurity strategy.[5] In addition, the mechanisms described here tend to be purchased from third-party providers. This gives the impression that a high level of cybersecurity is rather to be achieved by purchasing external tools than through an internal management structure. This is particularly evident in the parallel reading with *Chefsache Cybersicherheit,* which also addresses newer security concepts such as use of artificial intelligence, but in a more reflective and less prominent manner.[6]

As a conceptual framework, the Cybersecurity Competence Model is elegantly simple and visually intuitive and offers a coherent logic that mirrors how many executives are accustomed to thinking about strategic priorities. This structure lowers the barrier to entry for non-specialists, allowing them to grasp not only the technical domains of cybersecurity, but also the rationale behind them. In a landscape saturated with fragmented tools and checklists, this integrated approach is a strength.

Yet the model also reveals certain limitations when examined through a practical lens. While it organizes areas of concern effectively, it does not always provide clear prioritization within them. Managers who are early in their cybersecurity maturity journey may struggle to distinguish between foundational tasks and aspirational ones—an issue compounded by the model's outer rings, which package advanced strategies alongside more basic governance steps without clearly sequencing them. Moreover, the model relies heavily on abstraction; it tells managers *what kinds* of measures they should pursue, but only loosely connects those categories to concrete examples, metrics, or decision points. For organizations seeking operational guidance rather than structural orientation, the model offers a compass—but not a map. A certain prioritization is made by emphasizing identity management and zero trust in Chapter 3, but it should be noted here as well that these are also rather newer and specific concepts which leads

[5] Touhill, G. J. and Touhill, C. J. (2014) *op. cit.* p. 95 seq.
[6] Köhler, T. R. (2021) *op. cit.* p. 185.

the conscious reader to ask why particularly these are presented. The same applies to the interviews in the final chapter. It is not entirely clear why focus is set on novelties or, with regard to the interview on cybersecurity at major events, on topics that are not actually mentioned in the book and are not part of its core subject matter.

Legal frameworks such as the GDPR and the NIS/NIS2 directives are woven into the discussion, reinforcing the point that cybersecurity is not optional but mandatory—and increasingly enforceable at the individual executive level. Indeed, under the NIS2 Directive, executives can be held personally liable for the consequences of a cyberattack in cases of proven gross negligence, placing cybersecurity squarely within the scope of fiduciary and compliance duties at the top of the corporate hierarchy. However, the information provided does not seem sufficient to allow for a legal assessment, for example, to enable managers to determine when it is better to refer an issue to a legal expert.

*Cybersecurity für Manager* appears prescient, yet it presents blind spots. The book strongly emphasizes the importance of management commitment, framing it as the foundation of effective cybersecurity. Throughout the text, the authors argue that security cannot be left solely to the IT department, and they explicitly call for board-level oversight, formalized risk governance, and clear responsibility structures. However, while the book clearly communicates that leadership must "own" cybersecurity, it stops short of exploring how such commitment can be cultivated within organizations.

*Cybersecurity für Manager* offers a well-organized, accessible, and legally informed guide to cybersecurity for non-technical executives. Its model is conceptually sound and practically actionable. Yet the book gives little priority to internal levers such as incentive structures, role modeling, accountability mechanisms, or integration into strategic KPIs. In this respect, it outlines the necessity of commitment without fully equipping readers to implement or sustain it—especially in organizational cultures where cybersecurity has traditionally been viewed as a peripheral issue. While *Cybersecurity für Manager* briefly acknowledges the increasing importance of interconnected digital ecosystems, it stops short of offering concrete guidance on how executives should evaluate and secure third-party dependencies—whether through contractual controls, supplier audits, or cross-organizational risk assessments.

## 4. CONCLUSION

First and foremost, *Cybersecurity für Manager* should be read as a wake-up call—a well-structured alert to the fact that cybersecurity is no longer an operational afterthought but a central pillar of corporate governance. It succeeds in making the issue approachable for non-technical executives and provides a clear introduction to the key methods, frameworks, and standards shaping contemporary cybersecurity practice. For managers looking to move beyond awareness into execution, further reading is necessary, particularly to understand how to prioritize controls, sequence maturity steps, and implement technical and procedural safeguards in detail. The strength of the book lies in showing the breadth of the field and the strategic stakes involved; its limitation is that it offers orientation more than instruction when it comes to setting up a cybersecurity strategy.

## LIST OF REFERENCES

[1] Pufahl, M. Paulsen, P. and Arndt, P. (2024) *Cybersecurity für Manager Cybergefahren wirksam begegnen – das Kompetenzmodell für die Praxis*. Wiesbaden: Springer Gabler, 113 p.

[2] Touhill, G. J. and Touhill, C. J. (2014) *Cybersecurity for Executives: A Practical Guide*. New Jersey: Wiley & Sons, 386 p.

[3] Blum, D. (2020) *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*. Berkeley: Apress, 333 p.

[4] Parenty, T. J. and Domet, J. J. (2019) *A Leader's Guide to Cybersecurity: Why Boards Need to Lead–and How to Do It*. Brighton: HBR, 240 p.

[5] Houchin, D. (2021) *Cybersecurity for Executives, Managers, and Leaders: Arcane Knowledge of the Dark Art for Superior Decision Making: The Cyber Kill Chain*. Ad Hoc Press, 89 p.

[6] Köhler, T. R. (2021) *Chefsache Cybersicherheit: Der 360-Grad-Check für Ihr Unternehmen*. Campus Verlag, 272 p.