International Journal of Cybersecurity Intelligence & Cybercrime

Volume 3 | Issue 1 Article 5

2-28-2020

Book Review: The Cyber Risk Handbook By Domenic Antonucci

cybersecurity, cyber risk management, enterprise risk management, cybercrime, frameworks

Recommended Citation

Mierzwa, S. (2020). Book review: The cyber risk handbook. International Journal of Cybersecurity Intelligence and Cybercrime, 3(1), 56-58. https://www.doi.org/10.52306/03010520TZHA3208

Mierzwa, S. (2020). *International Journal of Cybersecurity Intelligence and Cybercrime, 3* (1), 56-58.

Book Review: The Cyber Risk Handbook By Domenic Antonucci

Stanley Mierzwa*, Kean University, U.S.A

Keywords; cybersecurity, cyber risk management, enterprise risk management, cybercrime, frameworks

***Book ReThe Cyber Risk Handbook Creating and Measuring Effective Cybersecurity Capabilities* by Domenic Antonucci. Hoboken, NJ: John Wiley & Sons. pp. 412**

Introduction

This book review provides an overview of Domenic Antonucci's edited book titled *The Cyber Risk Handbook*, published in 2017 by Wiley Publishing. The book begins with a scenario situation where the CEO (Tom) presents to the board regarding his firm's cyber risk management status and capabilities. The CEO has one day to gather all the relevant information to present, and he cannot delegate the task to the CIO or CISO. As the chief leader of the organization, he has the sole responsibility of accomplishing the aforementioned task. The CEO considers the perspectives of all the functions in the organization, the stakeholders, technology specialists, information security staff, and subject matter experts to obtain full knowledge and create a cyber-risk handbook. The CEO used the COBIT 5 framework, developed by ISACA, to divide his handbook into the seven COBIT 5 enablers which include: 1)Principles, Policies and Frameworks; 2)Processes; 3)Organizational Structures; 4)Culture, Ethics and Behavior; 5)Information; 6)Services, Infrastructure, and Applications; and 7)People, Skills and Competencies.

Each of the twenty-six chapters includes a variety of perspectives and requirements related to cybersecurity risk management from different international contributing authors and organizations that are subject matter experts. The chapters vary in lengths and provide a general overview of the topics. Each of the chapters are interrelated, allowing for a holistic view of cybersecurity, and focusing on threats to the organization, from a non-technical approach.

*Corresponding author

Stanley J. Mierzwa, M.S., Center for Cybersecurity, School of Criminal Justice, Kean University, 1000 Morris Avenue, Union, NJ 07083 USA
Email: smierzwa@kean.edu

International Journal of Cybersecurity Intelligence and Cybercrime, Vol. 3, Iss. 1, Page. 56-58, Publication date: February 2020.

Chapters Review

As the name of a handbook indicates, readers can read each chapter independently based on their focus topic. The book provides a useful list of functions, such as Compliance, Board, Insurance, Information Security, Physical Security, and Legal functions. This list assists the reader to focus on which chapters refer most to the interest of the reader. In following the COBIT 5 framework, an enterprise end-to-end view of IT is possible to ensure that organizations create an optimal value of IT but maintain a balance between the benefits and risk levels and resources available.

Several chapters make references to the International Organization for Standardization (ISO) 31000 risk management framework. Mapping relationships are provided for the ISO 31000 tasks and principles to the COBIT 5 enablers. This is helpful and valuable since COBIT 5 enablers are described and followed throughout the book. One concern about referencing ISO 31000 is that although the book provides some of its principles, the ISO guidelines are not freely available to the general public, and require purchase. This is unlike COBIT 5, in which documentation is freely available to ISACA members for download.

One of the larger chapters includes a deeper dive into the policies that the CEO's organization had in place for cyber risks. This breakdown of policies is helpful to understand what an organization may need to consider in order to demonstrate how they deal with the varying cyber risks that may arise. This chapter also contained policies for Social Media, Ransomware, Cloud Computing, Third-party Vendors, Big Data Analytics, Internet of Things (IoT), and Bring-your-own-device (BYOD)/Mobile devices. Recommendations for policy formatting and content are provided (e.g., a personal social media policy as well as a ransomware policy).

Given the importance of frameworks in the field of cybersecurity, one chapter is dedicated to providing a list of eight different models. The framework references include ISO/IEC 27000, NIST Cybersecurity, COBIT 5, ISF Standard of Good Practice for Information Security, SANS Top 20, Payment Card Industry Data Security Standard (PCI-DSS), World Economic Forum Cyber Risk (WEG-CRF), European Union Agency for Network and Information Security (ENISA). Each framework is detailed with enough knowledge to know its focus as well as the author of the framework, extent or documented length, the region it is utilized, the industry that best suits the framework, and the primary audience of those who would benefit most from the documented standard.

In addition to a chapter on identifying, analyzing, and evaluating cyber risks, there are several chapters dedicated to treating risks through processes and using insurance and finance. These chapters offer smooth transitions to help one assess best practices of prioritizing risks and prevention methods based on organizations' overarching goals. The chapter on using insurance and finance also provides a valuable lesson in understanding the role of cyber insurance, including thoughts about doing a cost-benefit analysis.

Several chapters were written by subject matter experts from outside the United States. This is valuable in providing a necessary global perspective in dealing with cybersecurity risk. For example, the chapter on the incident and crisis management is written by information security experts from France. In addition, chapters dedicated to organizations' internal context, culture, physical security, and human factors were written by experts from Saudi Arabia, India, Belgium, South Africa, and Australia. These international contributions to the book are positive and help the reader gain valuable international insights.

Given the variety of content provided in The Cyber Risk Handbook, which demonstrate the varied facets of cybersecurity risk, several chapters include background on physical security and access control. As with any security risk defense strategy, one cannot underestimate the importance of physical access to facilities and minimizing access control to systems, resources and physical locations. This helps to bring into view the idea of least privilege.

Conclusion

This book provides a broad landscape perspective into the work-related nature of cybersecurity risk management. Technology guidance, methodologies, and frameworks change frequently, and since the book was published in 2017, COBIT 5 has been replaced with COBIT 2019. It would be beneficial for an updated version of the book to be produced, adjusting references to the most recent framework. Some of the chapters will go into greater detail than others, but the book offers the right amount of information to obtain introductory knowledge on the topic.

Throughout the book, there are mentions or reminders that cyber risk is no longer a technology or information systems and security issue, but one that faces all departments, and in particular, assigned to leadership so that it remains focused and aligned with organizational goals. Furthermore, it is advocated that true organizational collaboration is required to ensure that risks are addressed. For example, it is crucial that groups such as finance, human resources, product development, marketing, information technology, and information security work together, where pertinent, to develop solutions or processes to minimize cyber risk.

The world of cybersecurity covers the entire planet; given the global information and communication technologies infrastructure, it is valuable to have concepts and chapters written by experts and organizations from different parts of the globe. Topics that may not necessarily be covered in cybersecurity technical books such as the subjects of culture, people risk management, and human resources, provide an excellent introduction and overview to students and those who seek an introduction to cybersecurity capabilities. This book is helpful in explicating a true varied and vast amount of content related to cybersecurity risk, the maturity level of an organization, cyber-functional awareness, and what leaders in any organization need to be familiar and concerned with.

Declaration of Interest Statement

The author declares that they have no conflicts of interest.