PM WORLD BOOK REVIEW

Book Title: ***Cybersecurity: The Insights You Need from Harvard Business Review***

Author: Various Authors

Publisher: Harvard Business Review

List Price: $22.95 Format: Soft Cover, 176 pages

Publication Date: 2019 ISBN: 13:978-1-63369-787-4

Reviewer: **Edward Raibick, PMP**

Review Date: April 2020

Introduction

The **Harvard Business Review** book titled **CYBERSECURITY** is one in a series of books pertaining to protecting a company's valuable assets. The series is dedicated to providing insight on today's fastest moving issues. The other books in this series from **HBR** include **Agile, Artificial intelligence, Blockchain, Monopolies and Tech Giants and Strategic Analytics**.

The book touches on the cyber security topics relevant to businesses in this fast paced, network connected society. Topics include cyber security and risk mitigation, security investment and budgets, C-level metrics and reporting, employee training and awareness, and Artificial Intelligence / automation. It also provides insights from several perspectives for things to avoid, based on previous lessons learned throughout the industry.

Overview of Book's Structure

- **Chapter 1**.- **Internet Security by Alex Blau** discusses the modern internet-connected society, recent cyber-attacks and the three physical pillars of security. He discusses the critical infrastructure sectors that are vital to the U.S. Department of Homeland Security. He also dives into the need for regular operating system patch updates and the consequences of ignoring this security maintenance task. Disaster recovery and backup systems are also discussed.

- **Chapter 2**.- **Security Trends by the Numbers by Scott Berinato and Matt Perry** introduces the reader to the average number of attacks and breaches

per company, the average cost of cyber-crime, external cyber-attacks by business sector, internal attacks, and what is attacked most often.

- **Chapter 3 - Why Boards Aren't Dealing with Cyberthreats by J Yo-Cheng and Boris Groysberg** dives into the reasons many Board of Directors are not ready or concerned about cyberthreats. It provides survey results of the several questions pertaining to cybersecurity and the strategic threat and average costs of data breaches in an organization.

- **Chapter 4 – The Behavioral Economics of Why Executives Undervest in Cybersecurity by Alex Blau** discusses determining the return on investment (ROI) choices faced by executives, behavioral economics and the use of the wrong mental models in making investment decisions. The reader ins introduced to the National Institute of Standards and Technology (NIST) and the Federal Information Security Modernization Act (FISMA). The chapter touches on peer-review surveys and weakest link in cybersecurity management.

- **Chapter 5 – Why the C-Suite Needs to Use the Same Metrics for Cyber Risk by Jason J. Hogg** discusses the down-side of the C-suite using and measuring the potential impact using different metrics in financial, regulatory, technical and operational organizations. The critical need for communication and transparency is reviewed as a method to collaborate and address exposures. This chapter discusses several steps that the CEO should take in preparing the organizations for robust cybersecurity and incident response during a cyberattack.

- **Chapter 6 – The Best Cybersecurity Investment You Can Make is Better Training by Dante Disparte and Chris Furlow** reveals that the major sources of cyberthreats are not technological, with prepared leaders and employees being the first and last lines of defense. This chapter also touches on Artificial intelligence, machine learning, and self-teaching algorithms as defense tools for an organization.

- **Chapter 7 – Better Cybersecurity Starts with Fixing Your Employees' Bad Habits by Alex Blau** covers methods for increasing cybersecurity compliance, readiness, and participation within the organization.

- **Chapter 8 – Keys to Better Cybersecurity – Keep the Rules Simple by Maartain Von Horenbeeck** recommends simplicity, and easy-to-follow rules and "bite size" training on security and cyberattack prevention.

- **Chapter 9 – The Avoidable Mistakes Executives Continue to Make After a Data Breach by Bill Bourdon** details four mistakes that are made when a cybersecurity incident occurs and recommended alternative actions.

- **Chapter 10 – Active Defense and "Hacking Back" – A Primer by Scott Berinato** discusses the ethics, legality and practices of attacking the attackers who are actively targeting your assets. Distributed Denial of Service (DDoS) is also discussed as well as encryption of resources.

- **Chapter 11 – Cybersecurity is Putting the Customer at the Center of Competition by Andrew Burt** discusses the need for security and data privacy as it relates to consumer confidence in your products and services. It emphasizes the need to maintain this trust and cannot be earned by marketing and branding.

- **Chapter 12 – Privacy and Cybersecurity are Converging – Here's why it matters for People and Companies by Andrew Burt** details the trend for consumers to move away from platforms they cannot trust. It points to the fact that legislation is being introduced to ensure compliance and protect consumers.

- **Chapter 13 – What Can Companies do When Trade and Cybersecurity Overlap by Stuart Madnick, Simon Johnson, and Keman Huang** discusses the recommended options that countries and companies have in dealing with cybersecurity.

- **Chapter 14 – AI is the Future of Cybersecurity, for Better or Worse by Roman V. Yampolskiy** reviews the use of Artificial Intelligence as a defense to combat cyber-attacks. It also discusses the consequence of a failure in these AI systems.

Highlights

The HBR book titled CYBERSECURITY provides a critical look at the complex subject of cybersecurity and the difficult decisions that business leaders must make on a regular basis to protect these assets. In our network-connected society, it is becoming increasingly challenging to protect our privacy and assets from those who wish to exploit the vulnerabilities in the infrastructure used to conduct business. This book helps the reader understand these issues and offers recommendations for business and decision makers in addressing this topic.

Highlights: What I liked!

CYBERSECURITY is written as a compilation of subject matter from various authors with experience in the subject. Each chapter provides a unique insight on the subject from individuals with different unique perspectives on cybersecurity. The book allows the reader to review and comprehend the topics in contained "bite-sized chunks" and provides chapter summaries for review of the key points of each chapter. An "about the authors" section is also provided, offering a synopsis of the experience of each author, as well as contact information for several of the content providers.

Who might benefit from the Book?

This book will serve executives, business professional and decision makers involved with cybersecurity, regulatory compliance, privacy and asset protection. It also is a good reference for professionals interested in pursuing a career in cybersecurity. The topics are clear and concise and provide insights to the complexity of asset protection and the consequences of ignoring the need for consumer privacy and asset protection.

Conclusion

The **HBR** book titled **CYBERSECURITY** provides fourteen chapters containing unique insights on the subject of cybersecurity. Having worked on several cybersecurity related projects, as well as C-level risk mitigation reporting and cybersecurity, I found the book helpful in gaining additional insight on the complexities and perspectives on this subject. Overall, I would give this book a 4 out of 5-star rating for its content and organization.

For more about this book, go to: https://store.hbr.org/product/cybersecurity-the-insights-you-need-from-harvard-business-review/10280

Editor's note: This book review was the result of a partnership between the PM World Journal and the PMI Dallas Chapter. Authors and publishers provide the books to PM World; books are delivered to the PMI Dallas Chapter, where they are offered free to PMI members to review; book reviews are published in the PM World Journal and PM World Library. PMI Dallas Chapter members can keep the books as well as claim PDUs for PMP recertification when their reviews are published.

If you are an author or publisher of a project management-related book, and would like the book reviewed through this program, please contact Editor@pmworldjournal.com.

About the Reviewer

Edward Raibick, PMP

Texas, USA

Edward Raibick, PMP is a Senior Project Management Consultant with extensive experience in software engineering, managerial and IT Project Management. Edward holds a Master's degree in Information Technology with a concentration in Internet and IT security, a Bachelor's degree in Information Technology and an Associate in Specialized Technology degree in Electronics. His career includes over 10 years with the IBM Corporation and over 15 years with Texas Instruments. His consultant projects include major clients such as Experian, United Airlines and Southwest Airlines.

Edward is a member of the Project Management Institute, Dallas Chapter, having acquired his PMP certification in 2011. Edward is also currently the Director of the Dallas PMI Chapter Book Review Program.

Contact: Email address: raibick@sbcglobal.net
Phone: 1+ (469) 667-3792