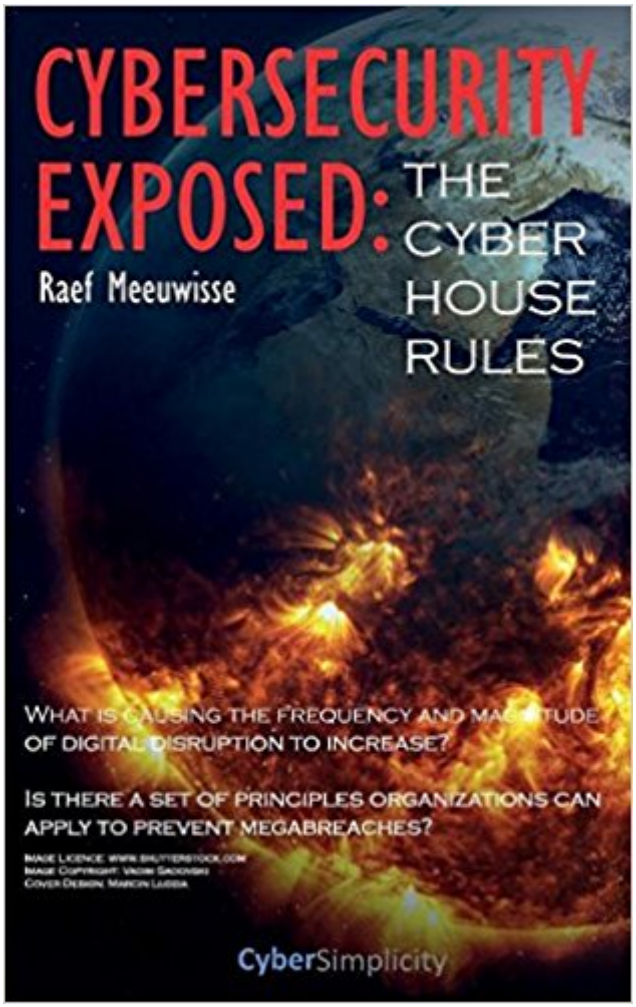
Cybersecurity Exposed: The Cyber House Rules



Synopsis

Mind the gap...between the actual level of cybersecurity and the amount required to protect you.Ever wondered what exactly is going so badly wrong in society that the fastest booming industry in the world is cybercrime?Psychology meets technology as this book explores how the rapid progression of technology is luring us all forwards at a pace that outstrips the human comfort zone.This book exposes the reasons that many organizations decide it is cheaper, easier and less painful in the short term to leave their security broken.Is security fixable?Ã Â Or are we destined to remain at the mercy of cyber criminals?We take a look at the cyber house rules, a set of principles that lead to what makes cybersecurity effective or, if not addressed, leaves large gaps that cyber criminals, rogue insiders and other hostile parties can take advantage of.What is causing the frequency and magnitude of digital disruption to increase?Ã Â Is there a set of principles organizations can apply to prevent megabreaches?

Book Information

Hardcover: 176 pages

Publisher: Cyber Simplicity Ltd (March 30, 2017)

Language: English

ISBN-10: 1911452193

ISBN-13: 978-1911452195

Product Dimensions: 6 x 0.4 x 9 inches

Shipping Weight: 14.4 ounces (View shipping rates and policies)

Average Customer Review: 5.0 out of 5 stars 9 customer reviews

Best Sellers Rank: #19,179,714 in Books (See Top 100 in Books) #81 inÃ Â Books > Arts & Photography > Architecture > Security Design #1677 inÃ Â Books > Computers & Technology > Security & Encryption > Encryption #1784 inÃ Â Books > Computers & Technology > Security & Encryption > Cryptography

Customer Reviews

Raef Meeuwisse holds multiple certifications for information security and authored the security control framework for a Fortune 20 company. He also created AdaptiveGRC, the world's first single data source / zero replication governance, risk management and compliance suite. He is an interim CISO for hire and an entertaining international speaker.

Although this book contains some very scary facts about how cyber predators are reaching their

creepy tentacles into cyber networks large and small, it discusses a topic that everyone who uses digital devices should know about, since few individuals and organizations have not been impacted by cyber breaches. The book uses language that non-IT-savvy people can understand to reveal an industry insider's look at what actually goes on in the evolving field of cybersecurity, and also includes his recommendations about how the ever-growing cyber menace can be counteracted and contained. The upside of all this is that the future of cybersecurity does not look all that dismal - if industry professionals and the companies that hire them are willing to change their outdated approach to dealing with existing and emerging cyber challenges. I would especially recommend this book to corporate decision-makers who should be aware that unless they empower their cybersecurity departments to protect their organizations from these threats, these organizations may not survive. Individuals who use computer systems at home or work would also benefit from reading this book to gain an understanding of what they personally can do to help diminish these threats.

Tells it like it is - any cybersecurity professional can learn from this book - helps to know why upper management has blinders on about cybersecurity.

This book is not intended to blind you with the level of technical detail in which you can get lost, and while it recognises that cybersecurity can be difficult, the book sets out some straightforward guidance to show how good cybersecurity is achievable.I can see two separate but importantly connected audiences for this book.- The executive or director whose customers or business processes use the internet- Any security officer in such a company.The book should be of value to both in setting out an agreed approach in bringing their cybersecurity to an appropriate level.The book includes many real examples of how this does not work in many organisations and depending on how close the examples are to home, the reader will either laugh or wince. If the IT and security function use this short book as the basis of an honest discussion with the executives and directors there should be a rapid meeting of minds and recognition of the realities.It is an easy read (even for busy directors) - I read it in the course of one decent train journey ÃƒÂ¢Ã â ¬Ã â œ and there are some blank pages at the back to take notes for later reference.

Given this topic is in the news all of the time, it was refreshing to get an up to date book that seems to tell it how it is. I found the points made were illuminating, logical and backed up with nice, clear examples. This book is a really expose of the world of cybersecurity, especially all the board room

shenanigans and pretence that security is unachievable when the evidence shows that major data breaches seem to always be a result of a collection of major deficits in the security that was in place. A great read and I would gladly push a copy across the table at any company that claimed they lost my personal details due to supposedly clever attacks.

If you are a frustrated security professional who is not being listened to, or an executive being told that security is unfixable and that you have to learn to live with all the intrusions, or just a person interested in understanding why the megabreaches keep hitting the media, then this book is for you. It debunks the myth that robust security is unachievable and sets out the reasons that security is often knowingly left broken. It also has some amusing examples of how these circumstances play out in the real world.I like my books to be engaging and informative and I found this to be both.

This book deliberately approaches cybersecurity from a non-technical perspective and will not bamboozle the reader with jargon. It is a great reference for anyone trying to understand how the evolution of cybersecurity is affecting their business and maybe even their home IT. I think it would be especially useful for CISOs wanting to improve the responses they get from their directors, or for the directors themselves to better appreciate the risks they face. Overall five stars.

Cybersecurity Exposed: The Cyber House Rules is not the first book I have read by Raef Meeuwisse, and I do hope this will not be his last publication.The first thing I will point out is that it is crystal clear he really knows the cybersecurity area. His opinions and advice are backed up throughout the book by relating real-life experiences in the field (without naming any individuals or organizations, of course), and his writing style is refreshingly direct. He tells it how it really is, using a conversational writing style that keeps the narrative moving at a good pace. And what I also like about all of RaefÃƒÂ¢Ã â ¬Ã â„¢s books is that they do not get bogged down in unnecessary technical jargon; although where technical terms are needed, they are always clearly defined, both at the relevant points in the book, as well as summarized in his aptly-named ÃƒÂ¢Ã â ¬Ã ËœCybersecurity to EnglishÃƒÂ¢Ã â ¬Ã â„¢ section at the back.However, this is not to say that this book is too ÃƒÂ¢Ã â ¬Ã Ëœdumbed-downÃƒÂ¢Ã â ¬Ã â„¢ for security professionals. It most certainly is not, as the content is of course specifically aimed at these individuals. This book really succeeds by being an excellent resource for security professionals working in ALL areas of information-/cybersecurity, from very technically-focused areas like server/database admins or Incident Responders, all the way to the

ÃƒÂ¢Ã â ¬Ã Ëœsofterâ ¬Ã â„¢ areas related to information classification and records management.Another ÃƒÂ¢Ã â ¬Ã Ëœmust-haveâ ¬Ã â„¢ for all information security professionals from Cyber Simplicity.

From page one it grips you and expalins the Cyber threats that face us. Another great read from the author. I was lucky enough to meet the Author at an ISACA event last year and the knowledge that he has on the field is inspiring! Would recommend any of his titles if you are entering the field or already work in this sector.

Cybersecurity Exposed: The Cyber House Rules CYBERSECURITY COMPLIANCE:: New York's Cybersecurity Requirements For Financial Services Company (NYCRR 500) The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn To Use the Internet Safely and Responsibly Tiny Houses: MinimalistÃ¢â ¬â„¢s Tiny House Living (Floor Plans Included) (tiny house construction,tiny homes,tiny house design,small houses,small homes,tiny house building,tiny house lifestyle,micro homes) House Plants: A Guide to Keeping Plants in Your Home (House Plants Care, House Plants for Dummies, House Plants for Beginners, Keeping Plants in Your Home, DIY House Plants Book 1) Striking Power: How Cyber, Robots, and Space Weapons Change the Rules for War Cybersecurity for Beginners Cybersecurity and Cyberwar: What Everyone Needs to Know Cybersecurity: Home and Small Business The Devil Inside the Beltway: The Shocking Expose of the US Government's Surveillance and Overreach Into Cybersecurity, Medicine and Small Business The Cybersecurity to English Dictionary Cybersecurity and Infrastructure Protection The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations Cybersecurity Ethics: An Introduction Cybersecurity (Special Reports) CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001) How to Measure Anything in Cybersecurity Risk Tiny Houses: The Ultimate Beginner's Guide! : 20 Space Hacks for Living Big in Your Tiny House (Tiny Homes, Small Home, Tiny House Plans, Tiny House Living Book 1)