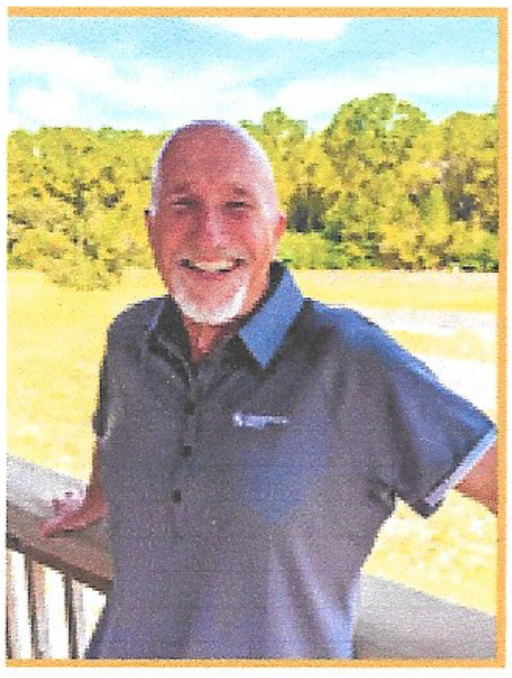


Book Reviews

By William J. (Jay) Carson

Disclaimer: These are the author's subjective opinions, and do not necessarily reflect the opinions of any organization or other individual.

Book reviews like mine are meant to encourage your professional reading. Two books are reviewed in this article. The first is a general cybersecurity book (Fancy Bear Goes Phishing), and the second is more of a cybersecurity/business book, (The Cyber Elephant in the Boardroom). Both books are well-written and affordable, and by use of 'war' stories will make their lessons stick in your memory. They are particularly great for entry-level cybersecurity practitioners. If nothing else, Fancy Bear Goes Phishing will make you the coolest storyteller at the coffee urn. The book The Cyber Elephant in the Boardroom will even teach you how not to talk to C-Suite people, a trait the author finds too frequently in our profession. The more-seasoned practitioners will love the stroll down cyber memory lane in Fancy Bear Goes Phishing and ways of teaching cyber and cyber law concepts. The Cyber Elephant in the Boardroom will give the senior types better ways to convey the cybersecurity message.

A prestigious professional publication like ours, the *ISSA Journal*, should have a monthly cybersecurity book review column. As a professional society, we need to encourage more members to be selective in the time they have for reading. Please bear with the next two paragraphs on what we are trying to accomplish, *you will not see these words again!* I attempt to blend professionalism and my apprehensions with humor, so well accomplished by the established *ISSA Journal* columnists like Robert Slade and Luther Martin.

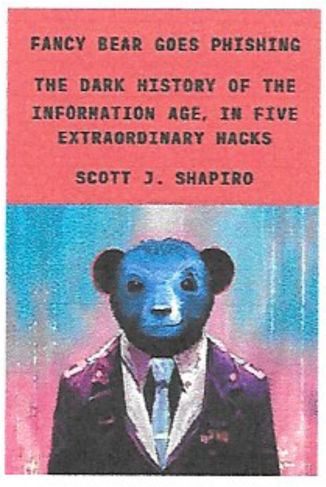
These book reviews go into more detail than other professional journals' book reviews. Although the titles are cool and the book jacket designs are eye-catching, these books should be read, not just showing behind your head on a video call. By the way, these are not "book reports," or study guides that summarized material. Book reports are something you did in elementary school to prove to a teacher you read the book. Study guides might help you skip reading the actual book. Book reviews, on the other hand, are done to encourage colleagues, particularly younger colleagues, to read and improve their overall cyber knowledge. Except for cybersecurity classics, I am hesitant to read anything over a few years old, for the obvious reason; the speed of innovation in the field.

A personal note: I am writing some of these words at 0530, while on travel, in a hotel lobby hoping the breakfast people will fill the coffee urn soon. Many of you will have a sympathetic similar remembrance, I woke up to anxiety: *Suppose someone reads my article, and I do not gush enough?* I have not yet authored any books but understand it to be arduous. How dare I do anything but applaud and coo at their baby? What will the authors say if I do not have enough superlatives? What will their publishers and marketing people say? Will this be like the servers in restaurants, the voice from my auto insurance, the person at my auto service shop, where anything less than a five-star rating is a total failure, and I am brow-beaten for taking bread from their family's table?

No gushing. Here we go:

Shapiro, Scott J. Fancy Bear Goes Phishing: The Dark History of the Information Age in Five Extraordinary Hacks. Farrar, Straus, and Giroux (2023).

Sound Bite: Cool title, and great true stories from a 'much more than' cyber-excellent author.



I got a great tip from a cybersecurity professor to read this book. If I ever break my "no gushing rule," this book will make the short stack. It reads well, and the analogies explaining cybersecurity concepts in lay terms are terrific. As the subtitle states, this is a book about hacking, using the histories of five infamous hacks as examples. This is a great history writers' technique you often see, taking an object like beer, wine, bread, etc., and then writing a world history. In this case, hacks are the beer. But this book is not just a dry rendition of the hacks themselves. Professor Shapiro goes into fascinating detail on the psychology of the people, the social science of the human population, and the level of technology at the time of the hacks. You will learn more about the thinking of greats like Alan Turing, John von Neumann, etc. Do you understand the conceptual details of how viruses and anti-viruses work? You will after reading the applicable chapter. Could you explain what an operating system is to a non-cyber knowledgeable person? How about a Structured Query Language injection attack, and how it captured Paris Hilton's private emails and photos? These, and other well-narrated examples, fill the book.

You are going to take a ribbing from your non-cyber family and friends for the title. "Daddy or Mommy, it is time for my bedtime story. Read to me from *Fancy Bear Goes Phishing!*" Nonetheless, CrowdStrike-named Fancy Bear, aka Mandiant's Advanced Persistent Threat (APT) -28, or more formally the Russian Army Intelligence Glavnoye Razvedyvatelnoye Upravlenie (GRU) – Hacker Division, is a tough operator. This is the story of the hack of the Democratic National Committee system before the 2016 US Presidential election.

The author also put a great deal of cybersecurity law throughout the book, well explained for non-attorneys like me. General legal concepts, like tort and contract law, are also explained clearly. You will learn some of the intent behind the law, and how it is applied. The writing on human psychology related to cybersecurity is just as good, if not better. For example, a malicious 'nudge' to your brain, is termed a 'mudge.'

The Author

Scott J. Shapiro is a very impressive guy. A law professor at Yale, and the book introduction gives evidence of extensive cybersecurity experience. This is a man

that knows his subject matter well. I personally like attorneys that share the way they have been trained to think. Professor Shapiro will take your mind in a different direction.

The Metadata

A *2023* publishing date! The online ordering cost, including shipping, is under $20.00. If you use an electronic reader, you can cut the cost by about a third. The hardcover book is slightly over 400 pages, including notes. These are superb 'notes' pages. Do not fail to read them. For example, the notes defining a 'side channel act' are a clear explanation.

There are two copies on order in my local public library system, so it is liable to be in your system. But unless you are incredibly lucky, you will have to wait your turn for such a book destined to be a 'must-read.'

I took a one-page sample of the text to analyze for readability. Measured by a Wikipedia article about the Flesch-Kinkaid Readability Test, the writing level and style is roughly college level. But - there was only 10% passive voice in my sample, so it reads well. This article is about 6% passive voice, for comparison. A reviewer told me some readers may not be familiar with passive voice, so I included a reference in the sources. My take is that passive voice can be useful, but a little goes a long way in terms of readability.

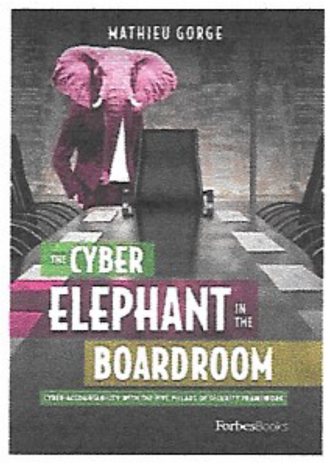
Table of Contents (abbreviated/modified and annotated in bold font by me):

- Introduction: The Brilliant Project **Morris Worm Hack #1**
- Chapter 1 – The Great Worm **Morris Worm Hack #1**
- Chapter 2 – How the Tortoise Hacked **Achilles Morris Worm Hack #1**
- Chapter 3 – The Bulgarian Virus Factory **Dark Avenger Hack #2**
- Chapter 4 – The Father of Dragons Dark **Avenger Hack #2**
- Chapter 5 – Winner Take All Paris **Hilton Hack #3**
- Chapter 6 – Snoop Dog Does His Laundry **Paris Hilton Hack #3**
- Chapter 7 – How to Mudge **Democratic National Committee Hack #4**
- Chapter 8 – Kill Chain **Democratic National Committee Hack #4**
- Chapter 9 – The Minecraft Wars **Mirai Botnet Hack #5**
- Chapter 10 – Attack of the Killer Toasters **Mirai Botnet Hack #5**
- Conclusion: The Death of Solutionism

I highly recommend this book to anyone interested in cybersecurity!

Gorge, Mathieu. The Cyber-Elephant in the Boardroom: Cyber-Accountability with the Five Pillars of Security Framework. Forbes Books (2021).

Sound Bite: Useful book, is extremely useful for PCI/DSS cyber practitioners, especially useful if you deal with C-Suite people.



My tip to read this book came from ISSA President Candy Alexander's recent article saying the ISSA Cyber Executive Forum was reading it for their book club. To me, this is a business book, an international business book, which is probably why Forbes Books is the publisher. This book is well worth reading, although my take on the author's point, that even in this day and time C-Suite people are not acting as if they are cyber-threat aware, is depressingly painful to read. They should know better. I did like a great deal Mr. Moks' Foreword to the book, where he commends two company CEOs, at Anthem and The Home Depot, for their breach responses. For active-duty military cyber professionals reading this review, I see no difference in the way of working with general officers and C-Suite personnel. They are all mission-focused, want direct answers, and are probably a bit sleep-deprived.

You will read about Mr. Mathieu's five pillars repeatedly throughout the book: Physical Security, People Security, Data Security, Infrastructure Security, and Crisis Management. He also recommends valuable resources such as the Verizon Data Breach Investigations Report. While, as I said, the book has a lot of Payment Card Industry Data Security Standard (PCI DSS) material, I personally did not previously appreciate the value understanding PCI/DSS would enhance general cybersecurity understanding. That is why I am reading and reviewing a PCI/DSS book next month (see the end of article for particulars).

Here is my "key to improved cyber-thinking" takeaway: the amount of information (who, what, when, where) C-Suite personnel put on business and social media allows cybercriminals to refine their attacks. This can include family members' data and postings. Oh, we all knew that in general. But if a cybercriminal can review company leadership duties by system from sources such as LinkedIn, they may know where exactly to go "whaling." It is great target identification!

I liked the author's discussion on trying to transfer risk to third-party vendors. We used to say in the military you could delegate authority but not responsibility. The author emphasizes not to just transfer to a third-party some business portion and not monitor their cybersecurity performance. Some liability probably remains with you. If I were responsible for overseeing a third-party firm where my firm had transferred some risk, I would pull the book off the shelf, turn to the applicable pages, and check off each item the author suggests on monitoring risk transference to third parties.

In full disclosure, while overall the book gives innovative ideas, I felt there is some amount of marketing at the end. There were no formal notes pages or an index.

The Author

Note Mathieu Gorge spells his first name with one 't' in case you look him up on LinkedIn. He has 20+ years of business and cyber experience, most notably as CEO and Founder of VigiTrust.

The Metadata

A *2021* publishing date! The online ordering cost, including shipping, is under $25.00. If you use an electronic reader, you can cut the cost by about a third. The hardcover book is about 270 pages. This is not a long book to read, a good one you can finish on a domestic airplane trip. If fact, if I were on a plane trip to brief the C-Suite of a client, that is exactly how I would re-read this book. There are no copies in my local library, and unless you have access to a great business book library you may also have a problem.

I took a one-page sample of the text to analyze for readability. Measured by a Wikipedia article about the Flesch-Kinkaid Readability Test, the writing level and style is roughly college level. But - There was 20% passive voice in my sample, so it is more challenging for me to enjoy. I also took a sample of one of the guest articles, with a similar result.

continued on page 17

https://www.weforum.org/agenda/2022/03/three-reasons-why-cybersecurity-is-a-critical-component-of-esg/

5. "A closer look at the Locky ransomware", Avast, 10 March 2016. https://blog.avast.com/a-closer-look-at-the-locky-ransomware
6. "Growing malware families in MENA demand increased threat intelligence, says expert", ITP.net, 18 April 2023. https://www.itp.net/security/growing-malware-families-in-mena-demand-increased-threat-intelligence-says-expert
7. "List of Countries which are most vulnerable to Cyber Attacks", Cybersecurity Insiders. https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/
8. "Government response to the call for views on proposals to improve the UK's cyber resilience", 30 November 2022. https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience/outcome/government-response-to-the-call-for-views-on-proposals-to-improve-the-uks-cyber-resilience
9. "Nordic Council seeks deeper regional cybersecurity cooperation", Defense News, 27 March 2023. https://www.defensenews.com/global/europe/2023/01/17/nordic-states-to-develop-common-cybersecurity-strategy/

Book Review (continued)

continued from page 6

Table of Contents (abbreviated/modified and annotated in bold font by me):

- Forward – **Christopher Moks, Director of eCrime, Digital and Cyber Forensics, Deloitte, France**
- Introduction – Cyber-Accountability for CEOs, CXOs, and Boards
- Chapter 1 – A Veteran's Feedback from the Trenches **(Great stories, including a must-read author's mistake in dealing with a C-Suite board)**
- Chapter 2 – Cyber- Accountability for C-Suite AND Boards
- Chapter 3 – Risk Landscape
- Chapter 4 – The 5 Pillars of Security Framework **(Physical Security, People Security, Data Security, Infrastructure Security, Crisis Management)**
- Chapter 5 – 5 Pillars of Security Framework Detailed Overview
- Guest Chapters
- Chapter 6 – Breaching the C-Suite (CEOs, CXOs, and Boards) – **James O. Grundvig**
- Chapter 7 – Protecting Data as the New Currency – **Nina Shulepina**
- Chapter 8 – The Intersection of Cybersecurity and Business Digitization – **Cathy C. Smith**
- Chapter 9 – Handbook for C-Level and Board Members – **Marco Antonio Soriano, The Soriano Group & Family Office**
- Chapter 10 – Managing the Cyber Risk Impact of Capital and Valuation – **Robert K. Gardner, New World Technology Partners**
- Chapter 11 – Cyber Risk Impact on the Board – **Nick Vigier, Coalfire**
- Chapter 12 – Software-Catalyst for Today's Digital Business – **Ed Adams, Security Innovation**
- Chapter 13 – To Comply with PCI/DSS – and Keep Cardholder Data Secure –**Marie-Christine Vittet, Accor**
- Chapter 14 – Cybersecurity Risk in Human Resources – **Cecille Martin and Thibaud Lauxerois**
- Chapter 15 – Education for Decision Makers – **Alexander Abramov**

I recommend both books, for the uses and reasons stated. To show you how good Scott Shapiro's writing is, I have ordered of his works (not cyber), 'The Internationalists.' Regarding Mathieu Gorge's writing, I look forward to seeing future books by him, especially his stories of when things go wrong.

Happy Reading!

PS – If you have a book you want me to read & review, please use the email address in my bio and let me know!

PPS - If this column works for you (and the ISSA Journal editor), up next month:

- Espinosa, Christian *The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity. Lioncrest* (2021).
- Cooper, Arthur B. Jr., Jeff Hall, David Mundhenk, and Ben Rothke. *The Definitive Guide to PCI DSS Version 4: Documentation, Compliance, and Management* 1st ed. Edition. Apress (2023).

About the Author

William J. (Jay) Carson, ISSA Senior Member, Aka 'Dad' The Cyber Librarian is the ISSA-Colorado Springs Executive Vice President. He is part-time 'Cyber Librarian' of Semper Sec, LLC. Holding Security+ and CIPP/E certifications, he is a former high school math/science teacher, civil servant, contractor, and retired USAF Lieutenant Colonel. He can be reached at Runningjay51@gmail.com

References:

1. https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests
2. https://en.wikipedia.org/wiki/Fancy_Bear
3. https://www.grammarly.com/blog/passive-voice/