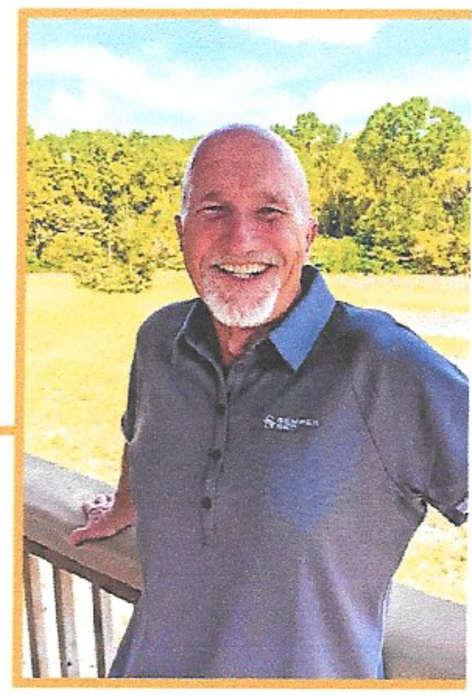
Book Reviews



By William J. (Jay) Carson

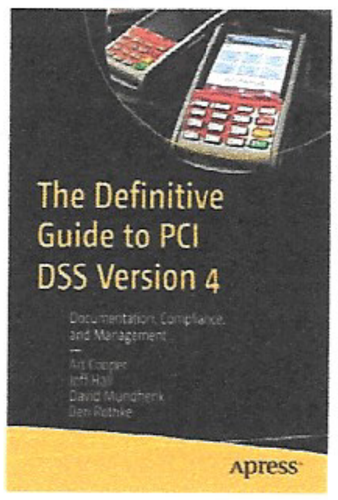
Disclaimer: These are the author's subjective opinions, and do not necessarily reflect the opinions of any organization or other individual. This article was prepared by a human, with assistance from Microsoft Editor and Grammarly.

Book #1, The Definitive Guide to PCI DSS Version 4 is a book designed for the Payment Card Industry / Data Security Standard practitioner, but I found it great for the general cybersecurity readers' awareness. This is fundamentally a "how to comply" book but told in a manner filled with war stories and the "why" of each compliance rule. PCI/DSS compliance rules are conceptually useful throughout cybersecurity. For the PCI/DSS person, remember Version 4 goes live on April 1, 2024. Book #2, The Smartest Person in the Room, is especially worthwhile if you have identified problems with motivating cybersecurity technical subordinates or are personally feeling burned out and can't understand why. This is a self-help book, with the story focused on cybersecurity practitioners. It does not contain as much about cybersecurity as I would like but does contain a great deal about human practitioners.

I actually got feedback from last month's Book Reviews article for the ISSA Journal. I was asked, "If you only had time to read one book of the two you review, which would it be?" That is a tough question because I try to review books for readers with different purposes for reading. However, in the interest of responding to any (please!) feedback, I will always pick the first book in the reviews as my "if I have to choose" only book.

I won't review a book for the ISSA Journal unless I have read it twice. In both these cases, I am glad I did. Here we go:

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).



Sound Bite: Everybody that uses a credit card should have at least a passing familiarity with what cybersecurity is behind the card.

Why, if you don't deal with PCI/DSS, should you read this book? I asked myself the same question: it is not my preferred cyber genre. But I do want to have a solid general knowledge of all cybersecurity topics, to pass cybersecurity certification exams, and to protect credit card use by myself and my family members.

I am spending more time in the compliance world generally, and personally, I am seeing a lot of overlap. My short answer in all the compliance systems: Think holistically, do the smart things, document like the dickens so you can really prove it, as well as keep doing the smart things through great systems. If you have never read a book devoted to cybersecurity in the payment card industry, this one will instruct and, believe it or not, entertain you. The most interesting parts of the book are "Pitfalls" and "Famous Fails" in a number of chapters. For example, I did not know about the 2015 POODLE vulnerability, involving TLS and SSL. If you are in the Red Team and/or Penetration Tester part of the business, don't miss this book for tips!

The Authors

Always, always, check the authors' credentials of books you read for knowledge, especially in cybersecurity. In this case, I am pleased to report all the authors are more than well-credentialed and experienced to authoritatively write on this subject. Together, "the authors have more than 50 years of combined PCI experience." The first name I personally know well.

Art "Coop" Cooper, CISSP, Payment Card Industry Professional (PCIP), PCI Qualified Security Assessor (QSA), and other certifications, 2019 ISSA Security Professional of the Year, and decades of PCI/DSS experience. I have served with "Coop" Cooper on the ISSA-COS Board of Directors, and also enjoyed his presentations to our local community. Get Coop talking PCI/DSS cyber-war stories, and the audience is mesmerized. If you are the next speaker up in a program, you might be delayed because the audience refuses to let him go!

Jeff Hall, CISSP, PCI QSA, and other credentials. Also "started into the world of PCI compliance before PCI was even an acronym." I like that!

David Mundhenk, CISSP, PCIP, PCI QSA, decades of experience including IBM and Coalfire.

Ben Rothke, CISSP, and other credentials, decades of experience. Mr. Rothke apparently initiated this PCI team concept. Do not skip his author introduction which includes other PCI books if you need to start a library.

When it comes to PCI/DSS, these guys are not called 'The Dream Team' for nothing!

The Metadata

A *2023* publishing date! The online ordering cost, including shipping, is going to be about $40-45.00. The paperback version is about 240 pages. You can cut that cost if you use an e-reader. No notes or bibliography. There are no copies in my local public library system, so unless you have access to an extensive cybersecurity library system, you will have to resort to other means to buy or borrow a copy.

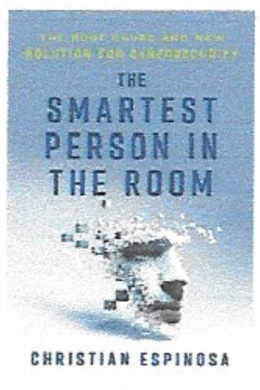
I took a one-page sample of the text to analyze for readability. Measured by a Wikipedia article about the Flesch-Kinkaid Readability Test, the writing level and style is early college level. There was 30+% passive voice in my sample, but surprisingly I did not find that onerous. This article is about 7% passive voice, for comparison. I have two criticisms that I hope the authors will correct in any later books. First, the book reads a little like A wrote a part, B wrote another, C wrote a third, and D a fourth part. This really shows up in the abbreviations, where each chapter spells out many of the same abbreviations. While I like some of that, a little goes a long way. If they are concerned people will only reference a specific chapter, an abbreviation guide as an appendix would fix the problem. Second, I hope they stay away from phrases like "It is imperative that…," as that is grossly overused in compliance books.

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

- Chapter 1 – A Brief History of PCI **Great Stuff!**
- Chapter 2 – Install and Maintain Network Security Controls
- Chapter 3 – Apply Secure Configurations to All System Components
- Chapter 4 – Protect Stored Account Data
- Chapter 5 – Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks **Apple users: Learn about the Shlayer trojan downloader.**
- Chapter 6 – Protect All Systems and Networks from Malicious Software
- Chapter 7 – Develop and Maintain Secure Systems and Software
- Chapter 8 – Restrict Access to System Components and Cardholder Data by Business Need to Know
- Chapter 9 – Identify Users and Authenticate Access to System Components
- Chapter 10 – Restrict Physical Access to Cardholder Data
- Chapter 11 – Log and Monitor All Access to System Components and Cardholder Data
- Chapter 12 – Test Security of Systems and Networks Regularly
- Chapter 13 – Support Information Security with Organizational Policies and Programs
- Chapter 14 – How to Read a Service Provider Attestation of Compliance **Things to watch out for!**
- Chapter 15 – Segmentation and Tokenization
- Chapter 16 – The Customized Approach, Compensating Controls, and the Targeted Risk Analysis **Danger: Customization is a Double Black Diamond ski slope! Expert skills only!**

I was initially drawn to this next book because I like the title, and the book cover is really cool. The concept is that cybersecurity practitioners strive to be the "smartest person in the room," but it becomes a detrimental obsession to themselves, their clients, and their companies.

Espinosa, Christian. The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity. Lioncrest (2021).



Sound Bite: Cybersecurity professionals can be brilliant, but also quirky, and successful business leaders need to know techniques for leading them.

I am seeing so much material in the literature and on LinkedIn about the "mind" of the cyber-smart technical person. Many people say we need to capture the technically bent person's smarts, before we lose them, or they might turn to mischief or crime. That is all well and good, but how? This author gives some ideas that work for him. Let's say you are a cybersecurity supervisor and you just had to let go of a highly-skilled, but socially antagonistic employee who had caused a serious problem within the team or worse with a client. You feel bad, and you surely don't want it to happen again! The author walks you through what he has experienced as a supervisor.

The author is heavily into neuro-linguistic programming, and according to the Wikipedia source I list that subject is controversial, to say the least.

A reviewer of a draft of this article said I am talking about the value of self-discipline in cybersecurity practice. Yep, guilty as charged. But there is more to it. Frankly, I am not as much of a fan of self-improvement leadership books as I was in my younger days. I have just seen the same good ideas repeated. However, if you are facing challenges dealing with technical professionals, this book might be right for you. My criticism of this book is I did not see a direct mention of the most valuable self-improvement advice I ever got in government or business service: "Work on your boss's problems!" If it was there, I missed it.

The Author

Christian Espinosa is a United States Air Force Academy graduate, had six years of USAF active duty, and holds the CISSP certification as well as many others. He is in admirable physical shape and can be quite proud of his being an Ironman triathlete. I bring that up because it shows his self-discipline, and that the principles he believes in work for him.

The Metadata

A *2021* publishing date! The online ordering cost, including shipping, is going to be about $10-$20. The paperback book is slightly under 280 pages. No notes or bibliography pages, but it does list some references. There are no copies in my local public library system, so it may not be in your system.

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 high school level. There was only around 8% passive voice in my sample, so it reads well. This article is about 7% passive voice, for comparison.

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

- Chapter 0 – Why Are We Losing the Cybersecurity War?
- Chapter 1 – Who Is Protecting Your Data?
- Chapter 2 – The Secure Methodology **See the steps below.**
- Chapter 3 – Step 1: Awareness
- Chapter 4 – Step 2: Mindset
- Chapter 5 – Step 3: Acknowledgment
- Chapter 6 – Step 4: Communication
- Chapter 7 – Step 5: Monotasking **Especially important**
- Chapter 8 – Step 6: Empathy

Continued on page 16

Community Corner

Mark Your Calendar for the Annual ISSA Membership Meeting

Thursday, September 7 at 1:00PM EDT

Don't miss out on the all the latest happenings and future plans for your organization.

Register Now: https://register.gotowebinar.com/register/3308799256182498651

2023 ISSA International Awards

The 2023 ISSA International Awards Gala was held on August 5th, 2023, at the Las Vegas Park MGM in conjunction with BlackHat USA. To see the replay of the gala and find out about the winners, inductees, and scholarship recipients watch here:

https://www.issa.org/annual-award/2023/

Cyber Executive Forums

The Adolphus, Autograph Collection. Dallas, TX. Nov 2 & Nov 3, 2023

To find our more or apply to attend:

https://www.issa.org/event/november-cyber-executive-forum-2023/

An Exclusive Event for Cyber Executives. By Invitation Only!

Looking for Journal Authors and Contributors

Want to get your thoughts and opinions published? We are looking for you!

- Share your wisdom and expertise through thought leadership articles.
- Gain peer recognition.
- Add to your professional portfolio.
- Possible CPE credits for your cybersecurity certifications.

https://www.members.issa.org/page/journal-contribute

ISSA Chapter Leader Meetings:

Mark your calendars for the next 2023 Chapter Leader Meeting

September 15, 2023 - 1:00 PM Eastern Time - Register Here

ISSA Members receive discounts to a variety of industry events and conferences such as:

- SECtember
- SecTor

To learn more about all the exclusive opportunities and offers available to you as a member visit: https://www.members.issa.org/general/custom.asp?page=SpecialOffers

Visit our new community events page to find local and virtual events.

https://www.members.issa.org/events/event_list.asp

There's always a webinar worth viewing either live or On Demand.

Visit and bookmark our events page to see our latest offerings. https://www.issa.org/events/

Visit our past webinars and view them on demand. https://www.issa.org/past-web-conferences/

Join One Of The Special Interest Groups Available Only to ISSA Members

ISSA Privacy SIG Join here: https://www.members.issa.org/members/member_engagement/groups.aspx?id=229802

ISSA Women in Security SIG Join here: https://www.members.issa.org/page/WomenInSecurity

ISSA Cyber Resilience SIG Join here: https://www.members.issa.org/members/member_engagement/groups.aspx?code=Cyber+ResilienceA

Want to start a new special interest group? Contact Candice.Benson@issa.org with your thoughts and ideas on a new area of interest.

Book Reviews (continued)

Continued from page 11

- Chapter 9 – Step 7: Kaizen **(Continuous Improvement)**
- Chapter 10. Growth and Contribution

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 - Up next month: I start going after Artificial Intelligence and the future that is already here!

Metz, Cade. Genius Makers: The Mavericks Who Brought AI to Google, Facebook, and the World. Dutton (Random House) (2021).

Ball, Matthew. The Metaverse: And How It Will Revolutionize Everything. Liveright Publishing Corporation (W.W. Norton) (2022).

William J. (Jay) Carson

Aka 'Dad'

The Cyber Librarian

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/Neuro-linguistic_programming
3. LinkedIn profiles for authors listed, where available.