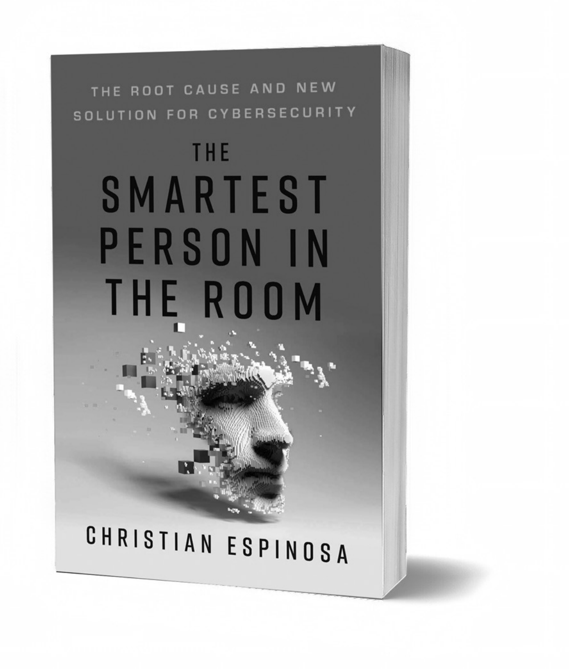
# The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity

By Christian Espinoza

Reviewed by
Cadet Aaron Calhoun



## EXECUTIVE SUMMARY

Christian Espinoza's *The Smartest Person in the Room* provides a creative approach to understanding and improving company culture. While the book emphasizes improving highly technical employees' communication and interpersonal skills, it ensures broad applicability through simplistic language and relatable personal anecdotes. The "Secure Methodology" lists in-detail human-centric goals for technical employees who experience challenges communicating with co-workers. Tailoring a technically-oriented methodology to advance social development makes Espinoza's book a useful, thought-provoking read.

## REVIEW

Christian Espinoza, CEO and founder of Alpine Security, now part of CISO Global, brings 30 years of cyber security expertise service derived as an Air Force communications-computer systems officer and private sector executive. His book *The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity* draws upon his experiences, and explains why his team-building approach, the "Secure Methodology," works.

**Aaron Calhoun**, a 4th year cadet at the United States Military Academy, is a nuclear engineering major and has focused research on computational simulations of fission and inertial fusion reactors. Following his freshman year, he created a database of nuclear reactor parameters and a respective Python analysis program for Sandia National Laboratories. Through Stamps Scholarship Foundation he continued his research at Cambridge University, where he built the first full-scale nuclear reactor in the experimental code SCONE.

Eleven chapters cover two central topics: (1) why current methodologies of cyber defense are failing to overcome cyber criminals, and (2) why his "Secure Methodology" will overcome this failure. The "Secure Methodology" focuses on cyber security industry issues, but it is readily applicable to any technical or leadership environment. Espinoza's seven steps, in order, are awareness, mindset, acknowledgment, communication monotasking, empathy, and *kaizen* (Japanese for "improvement"). To explain his steps, Espinoza provides a framework of team-level exercises and personal anecdotes that enhance reader comprehension and application.

These seven steps were formulated around Espinoza's belief that the root cause of modern cyber security infirmities is weak interpersonal skills – often from highly-technical employees. Espinoza explains that these employees are the very heart of any successful cybersecurity company, and the effective hiring and training of this workforce is mission essential to the company at large. Technical proficiency must always remain a defining factor in a company's hiring process, but Espinoza explains why social skills and the ability to self-reflect must also be a top priority – particularly for long-term positions. This means finding individuals resolved to overcome insecurities, defensive instincts, and any desire to be "the smartest person in the room." Technical teams will never realize their full potential unless their members prioritize technical understanding and interpersonal communication over individual egos.

> **Awareness:** Espinoza's first step is developing awareness, specifically the need for meaningfully practicing self-reflection. In this chapter, Espinoza notes that common "blind spots" which limit self-awareness stem from entrenched mental patterns – these neurological "ruts" often are difficult to identify and eliminate as they are commonly subconscious actions and outlooks formulated over

many years. Thus, one's level of self-awareness often is best analyzed with the help of other people; knowing how one's actions impact others requires communication. Clear, simplistic "coaching" sessions can effectively enable employee self-reflection and awareness.

**Mindset:** Mindset, likewise, is an extension of awareness. It is "how you view the objective or the problem." Espinoza asserts that the most successful are those who maintain a constantly growing, "I can learn/overcome this" outlook. The growth mindset operates optimally when the driving rationale is an innate interest in their field of expertise – not a bigger salary. Espinoza's conclusion – hiring processes must account for the recruit's "why" factor. A passion for financial success alone will not motivate cyber security teams to outpace criminals.

**Acknowledgment:** Espinoza defines "acknowledgment" as the expression of genuine appreciation for the work of others, which requires the leader to stop and meaningfully reflect on the progression of a project or individual, rather than yet uncompleted tasks. Espinoza views this acknowledgment-based approach as far more effective in building teams that are motivated by positive affirmation and respect rather than by fear and anxiety. For cyber security executives, this also entails keen awareness and acknowledging the differences between areas of expertise. "Technical employees" are not a monolith of expertise. As a result, company leadership needs to acknowledge and understand their employees' boundaries. Lastly, he discusses how lack of acknowledgment from leadership "trickles down" and leads to a systemic culture of resentment and unappreciation. Open acknowledgment lies at the very foundation of a positive company culture.

**Communication:** The desire to be "the smartest person in the room," often further exacerbated by what is industry-wide reliance on inscrutable technical abbreviations, impairs effective communications in the cyber security team. In short, cyber security is often unnecessarily complicated. Espinoza urges language simplification and punctuality of body language. The author explains that body language and tone are more important even than word choice in effective communication. Both technical and executive positions need to be capable of adapting comprehensible language conducive to a shared understanding. Espinoza describes various techniques, like mirroring body language and adapting linguistic patterns, to help build a common, collegial form of communication. Unless overcome, insecurities regarding personal intelligence can seriously impair inter-disciplinary cooperation.

**Monotasking:** Monotasking is Espinoza's primary tool for improving focus. He explains that instant communication tools, like email, have created an environment where employees easily conflate the completion of many inconsequential tasks with productivity. Projects that require intensive focus commonly take a back seat to the implicit need for constant connection. He later observes that a culture of instant communication can cause anxiety, where every message is viewed as urgent, thereby enslaving employees "to other people's time." Espinoza explains that monotasking focuses on one task within a given time "block." He also explains why people develop communication-oriented anxiety from a psychological perspective and how monotasking utilizing the "block" methodology allows for productive periods of uninterrupted work.

**Empathy:** Espinoza's chapter on empathy explains why interpersonal skills are essential for all members of a cyber security team, particularly the leaders. In line with his "acknowledgement of difference", as discussed before, Espinoza notes that the failure of employees to empathize and appreciate the talents of others limits their ability to effectively solve problems. He notes this is especially true for highly technical employees with limited understanding or appreciation for the work of non-technical employees. An overweening desire to be the smartest person in the room will further exacerbate a lack of understanding and empathy. Communications driven by a desire to maintain intellectual superiority are seldom accompanied by offers or requests for help, making technical problems harder to solve, and team members otherwise impeded by a culture of unproductive intellectual insecurity. Espinoza concludes this chapter discussing two primary forms of empathy (affective and cognitive) and how, at an individual level, they can be introduced into company culture.

**Kaizen:** As Espinoza states, Kaizen is the seventh and final step in the "Secure Methodology" and "gives you permission to start and then continuously improve." The importance of Kaizen stems from the assumption that "the only thing certain is uncertainty." Enabling an organization to set goals without black-and-white expectations creates an environment of adaptability and resiliency. Focusing on the problem(s) at hand rather than remaining upset at changes in circumstance optimizes the overall team effort in any given project. While Espinoza's summary of Kaizen philosophy is limited, he uses much of the chapter to discuss root-cause analysis, the tool he offers to better understand fundamental causation, and how to embrace uncertainty. His discussion of Kaizen is a broader debate of how to frame fears surrounding failure and uncertainty, not an in-depth discussion of Kaizen itself. Improvement and reflection of the other six steps require Kaizen.

## CONCLUSION

*The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity* is written with a cyber security focus, yet Espinoza's "Secure Methodology" should apply to myriad fields and is understandable to a general audience. Despite the initial self-help guru feel of the book, Espinoza's "Secure Methodology" provides a clear roadmap on improving the cohesion of highly technical teams. The future of cyber security, for Espinoza, can be greatly improved if companies from the outset prioritize inter-personal skills in their hiring and training practices; moreover, the adoption of the "Secure Methodology" provides specific human-centric goals for highly technical employees who are challenged in interpersonal settings. This review broadly summarizes each step of Espinoza's "Secure Methodology;" the book provides specific examples, exercises, and considerable detail as to how his suggestions can be implemented. In summary, Espinoza's "Secure Methodology" provides an excellent, easy to read, overview of skills that are essential to any highly technical team, particularly cybersecurity, where the technology is evolving at warp speed.

Full citation (as seen in this CDR Book Review):

Title: ***The Smartest Person in the Room:***
***The Root Cause and New Solution for Cybersecurity***

Author: Christian Espinoza

Publisher: Author's Republic (January 22, 2021)

Paperback: 280 Pages

Price: $18.97 Paperback
$8.97 Kindle