International Journal of Nuclear Security

Volume 5 | Number 1 Article 9

12-19-2019

Book Review of "Insider Threats" by Matthew Bunn and Scott D. Sagan

Arjun Banerjee
University of Tennessee Knoxville

Recommended Citation
Banerjee, Arjun (2019) "Book Review of "Insider Threats" by Matthew Bunn and Scott D. Sagan," *International Journal of Nuclear Security*: Vol. 5: No. 1, Article 9.
https://doi.org/10.7290/ijns050109
Available at: https://trace.tennessee.edu/ijns/vol5/iss1/9

International Journal of Nuclear Security, Vol.5, No.1, 2019

Book Review

Insider Threats

Matthew Bunn and Scott D. Sagan

Cornell University Press, New York, NY; 2017, 216 Pages
$22.95, ISBN-13: 978-1501705168

Reviewed by Arjun Banerjee
University of Tennessee, Knoxville

While books on various kinds of insider threats do exist, meticulously compiled information on the topic in the context of nuclear security is hard to come by. Information in the nuclear domain rarely comes to light for security reasons and makes this strain of insider threats a challenging topic to write about. This edited volume entitled *Insider Threats*, compiled by two of the most respected Professors in the field of nuclear security today, namely Matthew Bunn of Harvard University, and Scott D. Sagan of Stanford University, arrived on bookshelves as a timely publication.

Insider threats can be defined as "a security threat that originates from within the organization being attacked or targeted, often an employee or officer of an organization or enterprise." Further, in this book, Bunn and Sagan define an insider as "a person with authorized access to items that an organization wishes to protect – information, people, and dangerous or valuable materials, facilities, and equipment." Insiders are then categorized into several distinct varieties according to either the role they play – *passive* (passing on sensitive information about security vulnerabilities to external agents), *active* (someone perhaps unlocking a door in the guarded facility for an outsider), or *violent* (attacking or killing a colleague in the facility to further their own agenda) – or according to how they morph into an insider threat – *self-motivated* (having their own agenda), *recruited* (already in an organization but then motivated by external agents to be part of a plot), *infiltrated* (someone in an adversary group is able to join a high security organization as a kind of 'sleeper' individual who will strike at an opportune time), *inadvertent* (making errors without desiring to that leave an organization open to external threats), and *coerced* (loyal to organization but under duress from external agents who perhaps have threatened to kill their family, for instance.)

Insider threats are not a frequent occurrence, but when an incident does occur, rare as they may be, they can be devastating. For instance, the book talks inter alia about a $200 million bill resulting from economic damage caused to the Doel-4 nuclear reactor in Belgium in 2014 wherein an insider, unknown to this day, was suspected to have sabotaged a single turbine.

Beyond the chapters contributed by editors Bunn and Sagan, this book also brings together some of the brightest minds in the field in the Western Hemisphere as contributors, each considering insider threats from a specific angle. For instance, Thomas Hegghammer and Andreas Daehli's piece does a deep dive

on not only on what Jihadists have done with respect to nuclear materials, but also their communications and plans concerning such materials and facilities. The next chapter by Amy Zegart focuses on Nidal Malik Hasan, the perpetrator of the notorious Fort Hood shootings. Zegart tries to discern why the United States Department of Defense as well as the United States Army failed to observe clear red flags in Hasan's behavior for years until it was too late. In the third chapter, Jessica Stern and Ronald Schouten discuss the strange case of Bruce Ivins – a loner who used the cover of the 9/11 attacks to threaten high-ranking US government officials with letters laced with spores of the deadly anthrax virus. This was also a case where obvious red flags about Ivins' personality were overlooked when they should not have been. In his piece, Austin Long writes about Afghan troops killing their American trainers and why it skyrocketed in 2014, and thereby the lessons to be learnt from that scenario to apply in the context of nuclear security. The penultimate chapter derives examples of insider threats stemming from casinos and the pharmaceutical industry and once again their applicability to the nuclear industry. The authors do concede here that it is easier to perhaps learn lessons from casinos due to the field having far less to do with national security. Finally, in a concluding chapter, Bunn and Sagan do an encore with a worst-practices guide to insider threats which sums up the material in the other chapters and draws ten generalizable lessons learned of how organizations should try and avoid falling prey to insider woes.

Insider Threats discovers that cognitive, as well as organizational biases, can lead to insider issues. Nuclear insider threat related plans mentioned rarely to never in jihadist writings. The reader would possibly heave a sigh of relief based on that information, only to find out about a sabotage in a nuclear plant in the news the next day. Thus, it is precisely to overcome any possibility of complacency leading to such disasters and to ensure that organizations today do not repeat the same mistakes other organizations made in the past leading to insider problems that this book was written, as Bunn states in a lecture. Otto von Bismarck's quote is appropriately utilized here, roughly translating from the original German as: Only fools learn from experience. I prefer to learn from others' experiences and mistakes.

Insider Threats is a very accessible book. The main text is less than 180 pages long and neatly divided into six enriching chapters. The language is lucid and engaging. Though the intended audience perhaps primarily remains scholars and practitioners of nuclear security, the use of simple language can make it equally interesting for the lay reader with either an interest in this topic or possessing a curious disposition. It is ideally a must-read for professionals working in the nuclear security industry to remain well-versed with the various red flags they may encounter at the workplace.

This book also underscores the importance of preventing sensitive organizations from missing red flags about insiders and is a genuine embodiment of the maxim "it is better to be safe than sorry". What it does less of is focus on the type of error that may occur when the organization perceives just about everyone working there as insiders, who do not exist, to the point of paranoid obsession. Overall, this book is useful for a certain audience – primarily those working in security-related organizations, especially of the nuclear variety. It is also useful for scholars in the nuclear security field to develop their knowledge on a pertinent issue, though not extremely common yet, to prevent the potential Chelsea Mannings and Aldrich Ames' of their organization to successfully strike.