Journal of Strategic Security

Volume 5
Number 4 *Volume 5, No. 4: Winter 2012*

Article 4

Managing the Insider Threat: No Dark Corners. By Nick Catranzos. Boca Raton, FL.: CRC Press, 2012.

Mark J. Roberts

pp. 127-130

Recommended Citation
Roberts, Mark J.. "Managing the Insider Threat: No Dark Corners. By Nick Catranzos. Boca Raton, FL.: CRC Press, 2012.." *Journal of Strategic Security* 5, no. 4 (2012): : 127-130.
DOI: http://dx.doi.org/10.5038/1944-0472.5.4.10
Available at: http://scholarcommons.usf.edu/jss/vol5/iss4/4

JSS
Published Quarterly by Henley-Putnam University Press
with support from the University of South Florida Libraries

***Managing the Insider Threat: No Dark Corners*. By Nick Catranzos. Boca Raton, FL.: CRC Press, 2012. ISBN 978-1-4398-7292-5. Figures. Tables. Text Boxes. Notes. Sources cited. Index. Pp. xxi, 341. $69.95.**

Spies. Betrayers. Traitors. Insiders. The names change over time but the concept remains constant. Those with access and insider knowledge are in an advantageous position to betray the trust bestowed upon them by revealing information to outsiders whether for profit, revenge, boredom, ideology, or myriad other types of motivation.

In his new book, Nick Catrantzos encapsulates the numerous challenges faced by employers due to insider threats and offers concrete, actionable courses of action to root out and protect against those who would betray their employer. Catrantzos' background is formidable and credible in that he has a wide range of corporate, public and private sector experience. This book is an extension of an award winning thesis he wrote at the prestigious Naval Postgraduate School enhanced and expanded to meet the needs of a market in need of his perspectives and expertise. This book is comprehensive in scope and suitable for graduate, undergraduate, public sector, private sector, and executive training and seminars.

Throughout each section of the book, the author first establishes the context for his material and then outlines a series of questions to help guide the reader to better understand the concepts with which they must grapple. The situations and questions are not cast into a linear "right answer/ wrong answer" framework; they are guideposts to help the reader learn to examine the issues through the prism of critical thinking in order to question their own assumptions. In so doing, the reader is encouraged to ask the right questions and think through the known and unknown factors of a given situation. Practical exercises help to reinforce the learned concepts and stimulate discussion, brainstorming, and critical thinking. Catrantzos utilizes a multi-disciplinary approach incorporating, history, psychology, sociology, anthropology, asymmetric warfare, and various business, management, and leadership practices.

Catrantzos opens by challenging conventional wisdom. He takes an historical look at the motivations of traitors using case studies and folds in the very real and modern issue of cyber security. He warns that linear

thinking bolstered by long held biases is a structural defect in a security posture and pose an intrinsic threat. He offers evidence of new research that an (new) employee vice a (long-time) legacy employee poses more of a threat because they are mission-focused to infiltrate, penetrate, gather information, and exploit vulnerabilities.

Within this context, he examines the corporate dynamics of the work environment and provides a detailed look at how infiltrators who then become insiders can navigate through and exploit these factors. Some of the factors he analyzes are imperial overreach, cronyism, procedural controls, pre-employment screening, personal safety, self-defense, workplace violence, and the ever-present dilemma of how to balance security needs in the face of constantly changing workplace civil rights parameters.

Having set forth a framework, Catrantzos outlines how workplace leaders need to posture themselves. They need to understand their environment, start somewhere, and ask questions. He outlines the pitfalls and stumbling blocks and then offers a number of practical solutions to take charge of extant threats and contain them. One of the most helpful discussions is how to vet potential hires through background investigations identify potential red flags. Another vetting tool given detailed treatment is ferreting out deception through the use of the polygraph and the Reid interrogation technique. He puts a great deal of stock in the many facets of behavioral detection as a tool for weeding out insiders.

One of the most useful chapters is an examination of how to disrupt the insider threat by leveraging disruptive behavior already present in the workplace. By placing a suspected infiltrator in a workgroup with a disruptive personality, the infiltrator is constantly off balance and spends more time fending off the dysfunctional coworker's idiosyncratic behavior. As a security mechanism, it is psychologically brilliant and an outstanding example of how to harness the negative energy of workplace ne'er do wells to make safeguard the workplace. Some of the behaviors he discusses are the Tank, the Sniper, the Grenade, the Know-It-All, the Think-They-Know-It-All, the Yes Person, the Maybe Person, the Nothing Person, the No Person, and the Whiner. Catrantzos discusses the relative value (or lack thereof) of each personality type and possible outcomes the pairing may generate. Far from being a prescriptive template, it offers many possibilities to work a problem whose very boundaries may be undefined.

The author's treatment of existential insider threats builds on previous chapters and outlines the responsibility of management—to protect people and property. He also discusses the principal threat forms with threat

http://scholarcommons.usf.edu/jss/vol5/iss4/4
DOI: http://dx.doi.org/10.5038/1944-0472.5.4.10

negation strategies. The first existential threat is sabotage with cascading impacts. The cascading impacts are the unforeseen ripple effects flowing from some act. They can range from limited to catastrophic. The next existential threat is assassination as a form of political or corporate decapitation. By removing a strong leadership figure through assassination, the country or corporation may sink into chaos, mired by competing factions who vie for control or due to the fact that the assassinated person commanded loyalty and respect through sheer force of personality. The last type of existential threat is espionage yielding decisive victory, which has high potential to be a death knell for a country or a corporation.

Having outlined the three existential threats, the author enthusiastically recommends Red Teaming. While ardently praising the approach, he seems to cast it in linear fashion as a be-all, end-all approach to the insider threat, which is inconsistent in his up until now holistic approach to the insider threat. He also places a great deal of trust in the Department of Homeland Security and it Protective Security Advisor (PSA) program. His treatment of both DHS as a solution and the PSA program as valuable tools against insiders suggests the author is has now crossed from practical reality into an ephemeral dream state of hypothesis as the roles he outlines for them are not aligned with their extant roles. His repeated suggestion throughout the book to hire contractors to work insider threat issues rather than existing employees comes off more as an endorsement of a thriving industry that charges large fees with sometimes impractical or unworkable results. His eagerness to garner more business clouds an otherwise sold book that often does offer practical and workable solutions.

Overall, Catrantzos' book is a solid tome that has great value to better inside how to cognitively frame and practically combat the insider threat. Just as he calls for critical thinking to work the problem, the reader needs to invoke critical thinking as well to understand the occasional pitfall or leap of logic.

Mark J. Roberts

Journal of Strategic Security

http://scholarcommons.usf.edu/jss/vol5/iss4/4
DOI: http://dx.doi.org/10.5038/1944-0472.5.4.10