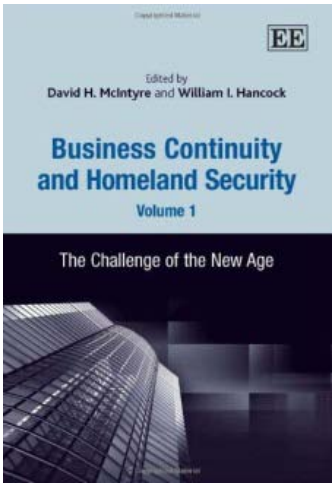
Text Review: Business Continuity and Homeland Security, Volume 1–The Challenge of the New Age

STEVE RECCA Naval Postgraduate School, Center for Homeland Defense and Security



TEXT AND AUTHOR INFORMATION

McIntyre, D. H., & Hancock, W. I. (Eds.). (2012). *Business continuity and homeland security, volume 1*: *The challenge of the new age*. Northampton, MA: Edward Elgar

Paperback: 192 pages
Publisher: Edward Elgar Pub (Jan 30, 2012)
ISBN-13: 978-1847202505
List Price: $99.95

EDITOR INFORMATION

David H. McIntyre is the Director for Homeland Security and Defense at the National Graduate School for Quality Management and is the former Director of the Integrative Center for Homeland Security at Texas A&M University. He spent 30 years in the Army, serving in both strategic and educational capacities. Before spending six years advising the Army Chief of Staff and the Commander of U.S. Forces in the Pacific on strategy, he served in airborne and reconnaissance units in the U.S. and Germany. He taught English at West Point and strategy at the National War College, where he served as Dean until 2001. In 1999, Dr. McIntyre developed the first graduate course on homeland security and from 2001 to 2003 he served as the Deputy Director of the ANSER Institute for Homeland Security. Since then he has taught graduate courses in strategy, terrorism and homeland security at the National Defense University, the George Washington University, the LBJ School at the University of Texas, and the Bush School at Texas A&M. He currently serves on the Editorial Review Board of the Journal for Homeland Security Education.

William I. Hancock is the Deputy Director for Homeland Security and Defense at the National Graduate School, and is a former Fellow and Adjunct Professor of business and homeland security at Texas A&M University's Bush School of Government and Public Service. He has a Master of Arts degree in international relations from the University of Southern California, an Advanced Professional Certificate in international business from New York University, and a Bachelor of

Science degree in engineering, national security, and public affairs from the U.S. Military Academy at West Point. He teaches business courses at several undergraduate and MBA programs in New York and Connecticut. Mr. Hancock is a business development consultant and has launched new technology products and services for more than 25 years.

TABLE OF CONTENTS REVIEW

Business Continuity and Homeland Security is divided into three parts: "Business in Dangerous Times: The New Reality," "Real Dangers Demand Real Answers," and "Disaster Stories We Can Learn From." These three sections comprise 16 chapters (articles) from leading experts in homeland security and related disciplines. The text also includes a forward by Christopher Shays, a preface by Dr. McIntyre, an introduction and conclusion by the coeditors, as well as an appendix to Chapter 9, author biographies, and an index. Several chapters include endnotes and reference documentation.

TEXT REVIEW

We have come to view homeland security as a public sector good, focused on what the g*overnment* (and *governments*—at all levels, and across sectors) can and should do to provide for a secure United States. Particularly in the early years following 9/11, as the field evolved both operationally and in the classroom, the federal government was identified as the keeper of strategies, policies, and regulatory structure— and the *decider* of requirements and *allocator* of resources. The private sector was present and considered, but in a largely subordinate role. As a community, we mentioned the private sector infrequently, and usually in conjunction with critical infrastructure (Readers likely have heard or used this line: "70% of all critical infrastructure is owned by the private sector." Funny, we have watched that figure climb over the past few years. This spring, a colleague announced with certainty that "at least 85%" is owned and operated by private enterprise. Numbers are a wonderful thing.). Even the current emphasis on *Whole Community* approaches to security and emergency management is federal government-derived and led, although the concept is a significant step toward deepening the bench of homeland security players.

So, it is quite striking to find a homeland security publication that is not government-centric. Volume 1 (the editors are promising more soon) places the private sector — American business in all shapes and sizes— if not at the forefront of securing the Republic, at least as a coequal partner with government. McIntyre and Hancock have been around the block, with *bona fides* in government and academia, and backgrounds in the development of the homeland security discipline. All the more refreshing that they have turned their considerable experience and expertise to addressing the role of the private sector in a post-9/11 world. *Business Continuity and Homeland Security* should fill a

major gap in highlighting the unique and extensive capabilities that business brings to the fight.

With Volume 1, the editors have patched a pretty big hole in the *Whole Community* framework. *Business Continuity and Homeland Security* is the first serious effort to align understanding of what private sector motivations and resources, as well as what businesses can and should do within the homeland security construct. The editors address the key challenges that have plagued (and likely will continue to niggle) policymakers: communication among the players, cultural and motivational differences, and how the public and private sectors truly can partner. A concluding insight from the introduction sets the tone for the chapters that follow: "…business leaders and government managers have a great deal to learn from each other."

Where *Business Continuity and Homeland Security* runs into a bit of difficulty is settling on an audience. The chapters range from short essays (vignettes) to full-on articles. Some are clearly designed to apprise private sector leaders of the new security landscape and help them take action to prepare their businesses for when bad things happen. As Dr. McIntyre describes in the preface, the intent is to "help business understand new challenges and new concerns." However, other chapters focus more on educating government managers and educators on business: what drives it, who owns it, and what motivates it (Not to tell you how the story ends, but the answer, by the way, is "profit" and the ability to sustain and grow). Having appeal to multiple audiences may add a more comprehensive picture of business and homeland security, but it also makes it tough for a single audience (business, government, or academia) to value the entire book.

What to look for. Highlights include:

- An impressive array of notable business leaders, academicians, and homeland security scholar-practitioners share knowledge and experience in business continuity.
- Peter Leitner's essay on "Business Continuity and Enterprise Value" (Chapter 3) is superb. For the layman (reviewer included), Leitner describes in readable detail how businesses estimate their value, and through which, how they can make rational security decisions. This is a must-read section.
- In Chapter 9, Elin Gursky dives into the practical elements of disease and pandemics, and how the private sector might prepare and respond. Business continuity during/after a disease outbreak is a tough, real-world issue; one that is often described as "too hard" for government planners, but is of critical importance for business survival.
- For the academics using *Business Continuity and Homeland Security,* Part III—Disaster Stories We Can Learn From— offers solid near-case-study quality essays on Hurricane Katrina and public–private sector challenges.

What else. If the business of America is business, McIntyre and Hancock have started the process of realigning homeland security to value the private sector appropriately. *Business Continuity and Homeland Security* goes a long way in framing the questions and the conversation we *should* be having with regards to a secure homeland through secure business. Some thoughts on where the editors—and our community— might take the next steps:

- Christopher Shays' Forward provides a straight-forward challenge to the private sector: "Businesses must help government." While this theme finds some threads in the subsequent chapters, more in terms of practical application and cases would be useful. See Michael Chumer's essay in *Introduction to Homeland Security* (reviewed in this issue) for more detail.
- To repeat the refrain used elsewhere: Case studies, case studies, case studies. The good news is that subsequent volumes may provide more in this area. While *Business Continuity and Homeland Security* introduces a major case in Katrina, additional studies that highlight public–private partnerships, private sector contributions, and business resilience (in other than Katrina-size packages) would be useful.
- Thinking enterprise and innovation, *Business Continuity and Homeland Security* would be an excellent choice e-reader format, particularly when considering the hefty price-tag (no fault of the editors).

Business Continuity and Homeland Security provides the first meaningful salvo in the battle to make "private sector" more than a filler term for government managers and educators. The book is a useful tool for anyone hoping to understand where business fits in homeland security (just about everywhere). Among the academic community, McIntyre and Hancock seem to be aiming for graduate students, and principally those headed to mid to senior-level positions in industry and government. While *Business Continuity and Homeland Security* might find its way as a classroom text, Volume 1's true sweet-spot is to serve as essential reading for graduate and undergraduate faculty— and govvies—to help mature our understanding of the private sector's essential role in the nation's security.