# THE QUIET THREAT

## ABOUT THE AUTHOR

**Ronald L. Mendell** worked as a legal investigator for thirteen years inquiring into diverse cases ranging from product liability to medical malpractice to financial investigations. He holds a B.S. degree in the Humanities from the University of the State of New York and a Master of Science (M.S.) degree in Network Security from Capitol College. In addition, he holds the Certified Informa-tion Systems Security Professional (CISSP) designation. Currently, he writes on science, technology, security, and investigative issues. His prior books, *How to Do Financial Asset Investigations*, *Document Security*, *Investigating Computer Crime in the Twenty-first Century*, and *Probing into Cold Cases* were published by Charles C Thomas, Publisher, Ltd. He currently works in technical support for a high-tech company in Austin, Texas. And, he also teaches computer security at Austin Community College in Austin, Texas.

Second Edition

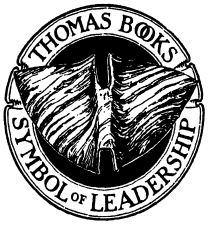
# THE QUIET THREAT

## Fighting Industrial Espionage in America

*By*

**RONALD L. MENDELL, M.S., CISSP, C.L.I.**

*Master of Science in Network Security*
*Certified Information Systems Security Professional*
*Certified Legal Investigator*
*Adjunct Associate Professor Computer Science*
*Austin Community College*
*Austin, Texas*




CHARLES C THOMAS • PUBLISHER, LTD.
*Springfield • Illinois • U.S.A.*

*Published and Distributed Throughout the World by*

CHARLES C THOMAS • PUBLISHER, LTD.
2600 South First Street
Springfield, Illinois 62704



*First Edition, 2003*
*Second Edition, 2011*

ISBN 978-0-398-07962-8 (hard)
ISBN 978-0-398-07963-5 (paper)
ISBN 978-0-398-07968-0 (e-book)

Library of Congress Catalog Card Number: 2010024896

*With* THOMAS BOOKS *careful attention is given to all details of manufacturing and design. It is the Publisher's desire to present books that are satisfactory as to their physical qualities and artistic possibilities and appropriate for their particular use.* THOMAS BOOKS *will be true to those laws of quality that assure a good name and good will.*

*Printed in the United States of America*
*SM-R-3*

**Library of Congress Cataloging-in-Publication Data**

Mendell, Ronald L.
The quiet threat : fighting industrial espionage in America / by Ronald L. Mendell. -- 2nd ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-398-07962-8 (hard) -- ISBN 978-0-398-07963-5 (pbk.)
1. Business intelligence--United States. 2. Trade secrets--United States. 3. Industries--Security measures--United States. I. Title.
HD38.7.M456 2011
658.4'72--dc22

2010024896

# PREFACE

In the years since the first edition, industrial and corporate espionage have not diminished. There has been, however, an increase in awareness about the issues. More graduate-level programs in business and in security are offering courses and training on intelligence gathering in the commercial sector. Training in the protection of confidential documents and materials forms a part of security certification programs. And, security professionals in the various sectors of American business and industry make reasonable attempts at safeguarding intellectual property.

Unfortunately, with the large amount of outsourcing in the technological sector overseas, information transfer and leakage continues to be a serious problem. As long as corporations see outsourcing as a way to save money in the short term, dangers will persist as to the draining of intellectual capital to overseas entities. The security community will need to continue to pursue this issue politically and socially.

As far as this new edition goes, two added chapters cover the tradecraft of the industrial spy and the uses of data mining in gathering business intelligence. By being knowledgeable about the spy's techniques, the security professional may detect activity earlier in the spy's campaign. Earlier detection may reduce the success and impact of a collection effort. Mining for data about a target is something both the spy and the security professional should be doing. The more information the security professional detects about his or her client that is available on the Web or in the public sector, then the more awareness there will be of potential vulnerabilities and avenues of attack.

Gathering intelligence about one's own company or enterprise is one of the best methods of defense against industrial espionage. Finally, the new edition offers an outline for planning an intelligence campaign against a target and a sample strategic intelligence report

about a business. And, a glossary of terms related to industrial espionage is also included in this new edition. These additional tools should increase a security professional's awareness of the corporate spy's mindset, which is a major portion of the battle.

R.L.M.

# PREFACE TO THE FIRST EDITION

Industrial espionage is a craft that has evolved over the centuries which remains persistent in its threat. During World War Two, organized espionage countermeasures came into American business practices. And these countermeasures met with success in a Cold War environment based upon industrialism where the prime adversary was a slow moving neo-medieval empire. The collapse of the Soviet Union ushered in two new factors. First, every nation became an adversary since competition moved from a military focus to an economic one. (Friendly competitors don't exist, whether foreign or domestic.) And second, keeping information "under wraps" became much harder. In a world where information resides more and more in electrons, secrecy resembles trying to stop a blizzard by waving a butterfly net. Berlin Walls or chain link security perimeters will not keep information contained within borders of our choosing. The Soviet Union could no longer hunker down behind the Kremlin's walls ignoring a world of the Internet, cellular telephones, and digital communications. We are in the same situation.

American security professionals cannot combat industrial (or corporate) espionage in the post-industrial information age without fully understanding its techniques. In fact, the term "industrial" may mislead; much of the spying now takes place against firms that do not manufacture a traditional industrial product, hence the alternate term "corporate espionage." But, history shows us that the techniques used today are adaptations of those developed in the sixteenth century and honed through the twentieth century. The text, accordingly, focuses on the similarity of industrial spycraft through time with examples from Anglo-American history. A primary goal of the book is giving the reader a real sense of how industrial spies are persistent and clever in circumventing defenses.

Another sense the book imparts to the security professional (or the student of security) is that industrial espionage creates paradoxes rather than straightforward, easy solutions. Rarely will the battles be set-piece confrontations with clear outcomes. Information's portability in an age of global digital networks may mean all the people who have your proprietary data can't be identified. Since copying, not stealing the original, can get the job done, thefts may go undetected for long time periods, making investigations difficult. Political dynamics within a company may aid industrial spies. And, constant change within a business often renders static, established security procedures obsolete rapidly.

The continuities in corporate and industrial espionage attacks are observation, knowledge, politics and power. Observation techniques range from aerial photography and satellite imagery to a spy jotting notes after a factory tour. Knowledge tools include patent research, induction, data analysis, and inference. Understanding the politics, the social dynamics within the modern corporation continues to be a powerful resource for the industrial spy. Exploiting jealousies and turf wars within corporate bureaucracies enables spies to penetrate inner sanctums. Power plays take several forms on the spy's stage: exercises in sexual power, in deception, or in prying secrets from a target through financial clout.

The effective twenty-first century security professional needs to be both a spy catcher and a spymaster, a collector of intelligence, an agent on the offensive, not just someone who implements countermeasures, a purely defensive strategy. So, the text examines both the defensive and offensive tactics necessary to fight industrial espionage. Living with paradox should be the theme for the security professional, and the book draws wisdom from political philosophers like Machiavelli to aid in that perspective.

However, the text strives to be more a history lesson or a discussion of security doctrine. It offers clear plans for action to deal with industrial espionage in a fluid, mobile, information-rich business environment. Creating new warriors against the quiet threat is its chief mission.

R.L.M.

# CONTENTS

# THE QUIET THREAT

# INTRODUCTION

## PARADOX AND SECURITY

A young man in an age of well-defined conflict, my father knew why he was fighting Germans in Europe. Influenced by Churchill and Roosevelt, he understood the purpose behind the mud, shivering nights, killing men before they tried to kill him, and the strange mixture of brotherhood and loneliness that is warfare. The enemy had a clear face of unquestioned evil. And while he may have not gone to war with the zeal of a crusader, at least he understood and recognized the crusade.

Leaders such as Churchill could rally the average citizen with the threat's overwhelming reality. Protecting freedoms from tyranny motivate the otherwise comfort-seeking man or woman to make sacrifices. Roosevelt cited "Four Freedoms" to the American public: Freedom from Fear, Freedom of Speech and Expression, Freedom of Worship, and Freedom from Want.

"Freedom from Want" requires two foundations: free markets and economic strength. Economic strength in our time relies upon knowledge, intellectual capital. Threats against or attacks upon our physical infrastructure, our factories and transportation systems, historically we have responded to quite well. But the erosion of our intellectual capital can be slow and insidious without any drama, headlines, or tragedy on the nightly news.

And, unlike for my father or for his leaders, the enemy engaged in industrial espionage often lacks a clear face. No public crusade calls them into the light. For the evil behind the thievery may remain in the darkness, an obscured undercurrent, not perceived, even among corporate executives as a daily foe. This quiet threat robs us of jobs, economic resources, and the industrial strength to respond to crises both

foreign and domestic.

The threat carries paradox. Traditional security thinking calls for the assessment of risks and the deployment of appropriate countermeasures. Clear, logical thinking to be sure, but threats may unfold outside of the game plan. So, a new paradigm emerges, which recognizes the limitations of countermeasures, and it embraces contradiction. We learn to think paradoxically, not everything is defendable. Security in the twenty-first century will resemble an ebb and flow.

Perhaps the hardest business problems are important but not urgent. Problems filled with urgency receive the attention and the resources. Stockholder meetings, quarterly earnings, market share issues, and profits all speak like thunderclaps. Industrial espionage remains a background whisper, a will-o'-the-wisp conjured by "security zealots." This demon of the information universe doesn't appear on management's daily radar, nor does it fray nerves until events are too late.

The first paradox of twenty-first century security totters on impossibility's slender edge. People do not recognize the threat, but they expect security to do everything, usually with sparse resources, to protect them against its consequences. Business leaders may authorize rudimentary expenditures for employee badges and a low-paid security force. But, if operational changes become necessary to fortify defenses, their hairs bristle, and the sidestepping of countermeasures or controls rears its head. And this reaction should not surprise the savvy security professional. American businesses dwell on short-term thinking, even about matters central to their core business. Why would they think differently about a security problem like industrial espionage? The riddle becomes: "When will the client worry about industrial espionage?" Unfortunately, quite often the answer remains the taunt, "When it is too late." If the barbarians are not at the gates, propelling management into action is challenging at best.

The second major paradox goes beyond business attitudes. It arises from the structure of the information commodity itself. Electronic information skirts about the Earth, extremely mobile, portable, and prone to subtle manipulation. The owner of proprietary data may have critical information stolen, but still retain physical possession of the original document or media. Copying isn't just easy; it is ridiculously easy. Treasure chests brimming with proprietary information zip out the door in a mundane briefcase. Or, the same documents dart across the globe via the Internet without a word of rancor or protest

from anyone, and management won't be any wiser.

Susceptible to interception and analysis, routine business transactions and electronic messages travel about highways of wire and fiber optics or through the air in satellite and cellular transmissions. Anyone can learn our "private" communications or secrets travelling in cyberspace. Much of this traffic remains in plain text. While encryption provides some help against this hidden danger, cryptography acts to safeguard only when users follow correct procedures. Murphy's Law creeps into the business use of ciphers. Users intersperse plain text emails between encrypted messages, supplying clues to monitor the traffic. Habits are difficult to control. Sending the same message frequently, or repeatedly transmitting the same type of document, provides a cryptographer a foothold to break a cipher. Not following encryption procedures stumbles into everyday business practice. Don't expect a business to operate with the stringent information handling guidelines of the CIA or the Defense Department.

Electronic information has inherent vulnerabilities. Unlike cash or valuable commodities, locking electrons in a safe usually is not a viable option. In order to be productive for a business, information needs to circulate on networks, PCs, Web sites, and on individual computers. Inert, noncirculating data creates little wealth. The paradox derives from the conflict between the desire for commerce and the need for security, and it will bedevil security professionals in the twenty-first century.

The third paradox arises from the personality of the modern corporation. Warriors against industrial espionage confront businesses that are not perpetual, static entities. A protective client in January may not be the same client in April. Fluid in employees, investors, management, and in business objectives, twenty-first century businesses embrace protean, mercurial transformations. Last year's security plan becomes obsolete faster than you anticipate. Will the pace of obsolescence continue to quicken? Are monthly revisions in security plans going to be the norm?

We face a new reality. Businesses will become more virtual. Composed of changing alliances, new methods of organization, ephemeral personnel, they will tax any static approach to security measures. In large organizations keeping user groups and access control lists current for network services wavers between a near impossibility to a "major challenge" for information technology (IT) security profession-

als. Constantly changing numbers of workers and revisions in mission objectives renders access privileges for databases and networks to slip "out of sync" with organizational reality. Who are we? What are we? These pithy questions become more than rhetorical devices; they reflect the angst of trying to protect an organization with ever evolving frontiers.

Understanding the drumbeat of the company's march in near time and space, that dilemma remains the greatest challenge for twenty-first century security. Viewing contemporary businesses as anything less than chameleon results in tunnel vision and in defending an illusion. Two adversaries exist for the security practitioner: the industrial spy and the ever-changing client. Thinking about what the client was last month may not address the threat of today. Considering what the enterprise could be tomorrow becomes a necessary survival skill. The fourth paradox compels the security specialist to act like the Roman god Janus, looking both to the past and to the future. Obviously, having current action plans will always be necessary, but constant reevaluation on their effectiveness for tomorrow may be the new mandate.

The security professional's battle against industrial espionage faces increasing technological assaults. Consider these trends:

1. Information technology has moved toward cellular devices with Internet access and applications ("apps") and other handheld computers. Proprietary data gets less centralized, harder to track and to protect behind a defensive perimeter.
2. The "office" wanes more virtual. Armed with a cellular telephone and a portable-computing device, the information worker has less of a need to conduct business at a central location on a regular basis. The line of defense becomes increasingly nebulous because a greater number of assets lie beyond physical security barriers or boundaries.
3. Self-sufficiency continues to grow among computer users. A plethora of information and software eases access to programming techniques and to database management. Users, even with the best intentions, may create information resources, which serve as a gold mine for the information predator. With little thought or concern, they carry these treasures on devices protected by less than ideal security.
4. Information channels diversify, becoming less controllable. Users, not bound by the company's email systems, networks, or