CRC Press
Taylor & Francis Group

Strategic Security

Forward Thinking for Successful Executives

Jean Perois

Strategic Security

Forward Thinking for Successful Executives

Jean Perois

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper

International Standard Book Number-13: 978-0-8153-5787-2 (Hardback)

Library of Congress Cataloging-in-Publication Data

Names: Perois, Jean, author.
Title: Strategic security : forward thinking for successful executives / Jean Perois.
Description: 1 Edition. | New York : Routledge, 2019.
Identifiers: LCCN 2018052811 (print) | LCCN 2019000041 (ebook) | ISBN 9781351123464 (Master) | ISBN 9781351123433 (Mobipocket) | ISBN 9781351123457 (Adobe) | ISBN 9781351123440 (ePub) | ISBN 9780815357872 (hardback) | ISBN 9781351123464 (e-book)
Subjects: LCSH: Leadership. | Executives. | Strategic planning. | Security systems.
Classification: LCC HD57.7 (ebook) | LCC HD57.7 .P4653 2019 (print) | DDC 658.4/7--dc23
LC record available at https://lccn.loc.gov/2018052811

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

CONTENTS

PREFACE

Security has moved at a tremendous pace since I became a security practitioner a few decades back. The evolution and the complexity of threats have positioned new security fields on the front stage. Yet although I acknowledge the importance of these new developments that contribute to the security of goods and persons, and make it a more multifaceted industry, the principles that have guided security practitioners for a long time remain valid. I believe in the value of classical security.

If you were to ask me why a book on security strategy, I would answer that this book is not exclusively about strategic security. It is more about applying a strategic perspective to the work of the security practitioner. I will not please everyone by saying that being the best at their job may not be enough to make a successful career. This is the stuff we were told when we were children but our experience of life has often proved otherwise. Yet the reverse is also not true. Being bad at your job will not promote you either. The recipe is probably a mixture of competence—that comes with hard work—and of self-confidence. In this book, I affirm that if they want to succeed, security practitioners should also promote themselves in ways that some old hands would probably call self-serving. Yet there is no reason security people should devote themselves entirely to their organization, selflessly and to their own detriment, and be forgotten on the way up to promotion. Yet it happens and it happens too often. Somehow, security is part of these jobs that chief executive officers (CEOs) perceive as not really capable of evolution. We will discuss in the book the probable reasons behind this prejudice, because observation and experience seem to show that competent security professionals are often maintained at the level at which they were recruited, avoiding the humiliation of being mocked as the latest victims of the Peter's Principle. The idea of promoting a security cadre to a position of general manager of a structure, a facility, a plant, or a headquarters never seems to cross the mind of a CEO, while I have seen human resources (HR) and finance people be picked for the job and become CEOs or general managers of facilities or offices, while nothing qualified them over their security counterpart. Knowing finance does not make you a good manager any more than being an HR specialist make you an expert on industrial production. Finding a rational explanation for this disaffection is a complicated issue of which our profession

is very much aware. Solutions are being sought in the academy, and the security profession is contributing to this much-needed effort at changing our image. Some say that by becoming more professional, security people will reach the C-suite and be chosen for more ambitious responsibilities at some stage. And they may be correct. However, the security professionals I have worked with were usually very professional, and no less competent in their field than HR, finance, or HSE managers. There seems to be a glass ceiling that security professionals fail to break through and I would like, in a modest way, to try to remedy to this situation. I hope that addressing self-help ideas and principles will help. For many years, I have read amazing books on self-development and often found them motivating and always exciting. Not everybody believes in their power. Which is normal since the power is not in the book, but should be found in oneself, and even so, I am not sure that this is what really matters. Self-development techniques bring a lot of benefits to the person who sets out to implement them with confidence, and I will discuss some of these principles, techniques, and processes in this book.

HOW THIS BOOK STARTED

This book stems from a course I wrote for the Security Institute UK titled *Strategic Security* for their security certificate quite some time ago. It was a short module that comprised eight chapters, complete with questions and small exercises.

It is only recently, after having left this course in the hard drive for a long time that I decided to have a look at it again and transform it into a book.

THE DISCOVERY OF SELF-DEVELOPMENT LITERATURE

The main difference between the syllabus and this book is that in the latter, I wanted to introduce the readers (or some of them, since the American readership is probably already familiar with the power of self-development techniques) to issues of self-help that have been the flavor of the day for a few decades, but really were pioneered in the first half of the twentieth century. How was my interest in these techniques aroused? It is an amusing story. I was the director of security for a major gas company in Qatar when I applied to go to a *rapid reading* course that was offered

in Dubai. I was then completing my master's degree and thought that reading more and faster would help me to perform better in the doctorate program I intended to begin as soon as possible and in my work since I was, by nature, the chief threat analyst of the organization, and as such had access to several of the remarkable Jane's security letters. I thought that being able to read faster would be an advantage. Not that I was so busy in my daily activities, but I liked the idea of being a rapid reader. The course was very interesting and strongly delivered, but the real personal discovery was the support book used to test our increasing reading skills. It was a book by Richard Dobbins and Barrie Pettman titled *What Self-Made Millionaires Really Think, Know and Do,* and it introduced me to concepts I had never heard about. Let us be clear, my purpose never was to become a millionaire, or I would have not served in the military in the first place, and even less in the security industry afterward. Even today, it is not one of my targets in life. Like everybody, I just feel the need to have enough savings to end up my life decently, but consider everything above that to be a bonus. I am not sure that the authors of this book really believed that becoming a millionaire is the supreme objective of their readers. Professional acknowledgement and personal achievement seem to drive most of us toward personal contentment. To become a millionaire, one needs to love money, and I was not brought up with money as the supreme life value. Success and social position were more what my parents had in mind for their children and values instilled during childhood tend to stick, no matter what we claim or pretend otherwise.

This book, by Dobbins and Pettman, was a book of revelations, of sorts, and I read it at night in my hotel room with growing marvel. I discovered in it what I have since called the mental laws of success, which are a mix of principles and techniques to help one reach goals for career achievement. Simply written and absolutely sound in their logic, these "guidelines" somehow changed my life, or rather the way I was managing my career, something I had never really thought about until then.

Sadly, it was a bit late in my professional career to apply all of them to my everyday working life, and I lacked faith in the ultimate goal that I would become a millionaire, but applying them definitely improved the way I perceived myself and did a lot of good for my self-confidence.

What makes this book unique, therefore, is that it provides a mix of strategic advice about the way you should run your security department as well as recommendations on the way to manage your personal career to

reap the benefits of your efforts. The security strategic thinking is nothing new. Several very good books have been written about strategy, and self-development books have sold by the millions, but this combined approach written specifically for the security professional makes it interesting. I am sure that many will find in it some recipes to set and achieve professional and personal accomplishments, and attain a fulfilling sense of satisfaction that makes life worth its while.

ABOUT THE AUTHOR

Jean Perois is a security practitioner working in the Middle East. He is a results-orientated security manager with a proven record of designing, developing, and implementing quality asset protection programs for major industrial projects in multicultural environments. His work experience includes expertise in strategic planning, business management, risk-assessment, security training, program development, physical security, force protection, security audits, and risk mitigation strategies. He is a security analyst with a passion for international affairs, an expert at monitoring security risks, and able to provide in-depth reporting on strategic issues and tools for decision making.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

1

Thinking Strategically in a Corporate Environment

In ancient Greece, *strategoi* were army generals cum politicians, whose task was to run the internal and external politics of the myriad of city-states dispersed in the Peloponnesian Sea. The famous Pericles (495–429 BC) and also the great historian Thucydides (460–395 BC) were among *strategoi* who marked the history of the Ancient Greek world. The word means "army leaders," and these army leaders played a major role in the political life of the Greek cities in times of peace and of war. Their role was military as well as political, and it should therefore come as no surprise that the word led to the word *strategy*, first defined as the art of planning and directing military operations and then in a business context as a plan of action or policy designed to achieve a major aim.

In the security industry, as in any other branch of business, strategic thinking can be defined as the ability "to plan long-term while maximizing performance for the short term" (Bruce 2000: 5).

In this chapter, I am going to discuss the basic components of strategic thinking when applied to security:

- Understanding what strategy is;
- Analyzing your position;
- Planning a strategy;
- Implementing a security program.

UNDERSTANDING STRATEGY

A strategy is a *declaration of intent*, a statement of where you want to be in the medium to long term (traditionally the 5-year horizon is the minimum target). A strategy is important because it enables you to make sure that "day-to-day activities fit in within the long-term program of your organization" (Bruce 2000: 6). A strategy encourages everyone to work together to achieve common aims. Most companies have a strategic plan, but they often fail to communicate it to the lower echelons, where you are now sitting as head of security or security manager. As a newly appointed security manager, your first task will be to become acquainted with the strategic plan of your company.

Defining a strategy is an important first step. It has been said time and again that a security strategy must be in line with the organization's corporate strategy. However, if you have been given the opportunity to see a corporate strategy document, you know that it is extremely difficult to develop a security strategy from a business program! Security is traditionally conspicuously absent from business strategy documents and you are therefore left on your own to devise something that should not antagonize the projects and growth anticipated by the finance people at corporate level.

Strategy concerns itself with what will happen in the medium to long term. Five years is traditionally considered as the minimum target of a strategy, but really this decision remains your call. Day-to-day activities tend to take precedence over long-term planning, and this is fine, provided the long-term strategy does not take a back seat. Strategy needs to be communicated to all who need to know, both internally (the security department) and externally (the rest of the organization).

THE STRATEGIC PROCESS

There are three distinct phases to developing a new strategy: analysis, planning, and implementation. The importance of the first two cannot be emphasized enough, as I have noticed in my career that security managers are not often given second chances: you must strike right the first time. In order to do this, you must get the first two stages absolutely right (Figures 1.1 and 1.2).

Let us begin with the analysis of the current situation.

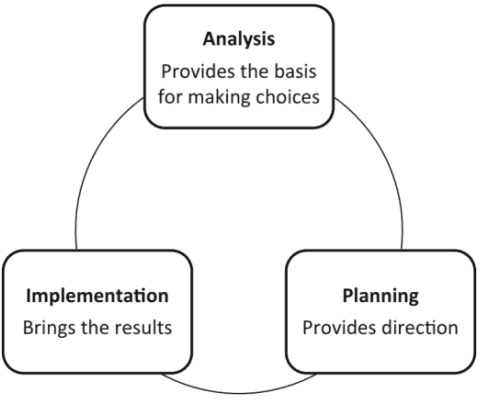

Figure 1.1 The strategy development process.

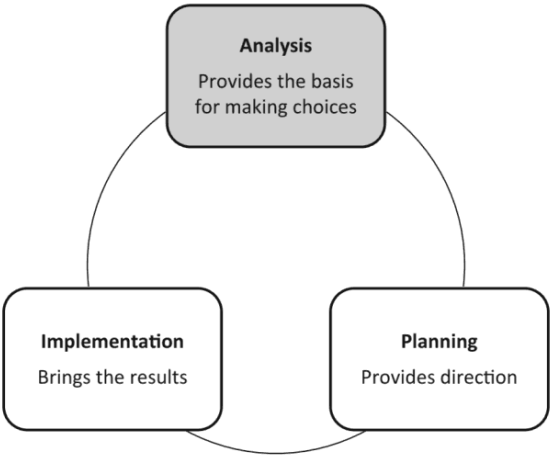

Figure 1.2 Stage 1: Analysis.

Stage 1. Analysis

Data Collection

To analyze data, you need to collect them first. It is important during this phase to collect as much information as possible regarding your organization and the current state of the security that is supposed to protect its assets (policies, plans, procedures, nature and number of tangible and

intangible assets, etc.). Before you change anything in the security master plan, you need to understand what role security plays in the protection of your organization's assets (*people, processes, assets, and information*) and to understand what management's expectations regarding your department's performance are. You may want to know:

- *What characterizes the existing security in your organization?* Think first about the impression it projects to employees and to external observers. Is it discreet, overwhelming, sophisticated, with a lot of technology involved, friendly? What does it look like? What corporate image do security officers project: robust, friendly, well groomed, or could do better? Does the security in general (personnel, procedures, and technology) provide reasonable deterrence? How does it compare with security departments you have observed elsewhere or worked for in the past?
- *How do employees perceive it?* This is of course linked to the previous questions. And you generally cannot perceive quickly what employees feel about security. After all, you are their chief, and they will not want to be the ones who told you how unloved security people are in the company. The *shoot-the-messenger* syndrome is very much present in many organizations. It will be your job to observe—particularly during the 30 minutes during which employees and cars arrive at the company and reach their offices in the morning—to get a feel for the relationship between employees and security personnel. You can also sit in the lobby and observe the morning arrivals. This is always very instructive. Are people trying to avoid using their badges, are they friendly with the guards and receptionists? Can you observe piggybacking[1] or tailgating, or if you have been spotted, embarrassed behaviors?[2] What happens to the offenders, if caught? How do the security guards react, if they do? How do the caught-in-the-act offenders react? These small incidents always tell you a lot about the perception of security and the discipline of both the workforce and your staff.
- *What do you think the management expects from security?* This is indeed a very important question. It often happens that the new security manager does not meet the top people who know what they want from security. Apart from a quick, informal

discussion with the chief executive officer (CEO) or the general manager (GM), the security manager is often entering her office on Monday morning with not much clue about what is expected of her. There are several possible situations. One, it could be that you are the first security manager hired by the management. Ask yourself: Why is that so? What may have triggered this sudden need for more than a few guards managed by the facilities department? There may have been incidents; a merger with a more security-conscious organization may have taken place, there may have been a change in hierarchy or in priorities, etc. You need to get an answer to that question. Speak with colleagues at human resources (HR), health safety and environment (HSE) to get answers. It is important to understand whether you are here to satisfy an administrative requirement, or because recent events have created some anxiety in the organization's leadership. This happened to me when I was hired as the first director of security of the then biggest gas project in the Middle East in 2004. The project phase had been ongoing for 2 years, the construction of the gas plant was well advanced, and the pipelines were already buried underground or laid at the bottom of the sea when I was appointed. It took me quite some time to understand the numerous and complex reasons that motivated my nomination. Some were political, a few were technical, and most had to do with the complex relationship between stakeholders in the project and the relative and always changing balance of their power. And, as you most likely have already guessed, these stakeholders pursued different security agendas. All converged toward an end result in which the assets composing the gas project were to be secured, but each stakeholder had a very specific idea about what constituted assets, and the way they should be protected. Anyway, if you are the first security director in a project, sit back, observe, think, and brace yourself for a complicated future. There must be some serious thinking from your side about who you are going to serve—one cannot serve several masters well—and what is expected of you. This does not mean that you will do different things as far as your asset protection plan is concerned, after all, industrial and corporate security is a simple art, but internal politics will definitely impact the way you will implement

company security policies, as well as how they will be prioritized and above all perceived. More importantly, you will have to think very seriously about the cultural aspects of security, and the perception of it by people coming from cultural backgrounds radically different from yours and those who often see security not as a bonus, but rather as a personal hindrance. You do not have too much time for this reflection. Do not forget that to establish yourself, you will have to implement some visible and tangible security measures quickly. Think that your appointment might have been a complicated issue, that some top managers may have had their own favorites, and that many people in your organization are far from convinced that a security department is a business necessity. To this end, I know that some of you will tell me that part of your brief, as security executive, is to educate management about what security entails, to help them differentiate between what is important and what is necessary, and I appreciate this commitment, but the reality is that management is usually very ignorant of what security is and that you will have to gain credibility before you have a chance to educate your hierarchy. And let's face it: Most of the time, they are not interested.

- *How do other competitors operate in comparable environments?* There are two ways to embrace this. (1) Your first possible approach is based on your experience. During the course of your career you may have worked in different environments and in different capacities. You have learned lessons and observed good setups and not so good ones. You have an intuitive feeling about what good security should look like and you can measure what you see according to what you saw elsewhere, that worked. (2) The second approach consists of measuring security by benchmarking what you see with what others do in the same industry. Doing this is sometimes easy, particularly when your facility is located in an industrial city, where neighbors operate very similar type of facilities in a shared environment. Chances are quite high that security meetings for security departments from the entire city are already organized to discuss threats, recent incidents, new trends and possible collegial solutions. Of course, it is a bit more difficult if you are new to the industry or if your

INDEX

Note: Page numbers in italic and bold refer to figures and tables, respectively. Page numbers followed by n refer to footnotes.