

P GRAÑÉN
ORRÚA

Grupo Editorial

CORPORATE SECURITY

A KEY PIECE ON THE CORPORATE CHESSBOARD



Lt. Col. Antonio Gaona Rosete

CORPORATE SECURITY

A KEY PIECE ON THE CORPORATE CHESSBOARD

CORPORATE SECURITY

A KEY PIECE ON THE CORPORATE CHESSBOARD

Lt. Col. Antonio Gaona Rosete



MÉXICO, 2023



Colima 35, Tizapán,
01080 Ciudad de México.

First edition, October 2023

© 2023 By typographic and editorial design characteristics
Lito-Grapo S.A. de C.V.

© 2023 Antonio Gaona Rosete

Special thanks: Dereck Bueno

Impreso en los talleres de LITO-GRAPO, S.A. de C.V.

All rights reserved under the law
ISBN 978-607-8758-82-1

The partial or total, direct or indirect reproduction of the content of this work is prohibited, without the prior express written authorization of the publishers, in terms of the provisions of the Federal Copyright Law and, where appropriate, by the applicable international treaties.

*To the extraordinary team that God gave me, my wife and my children.
You are my inspiration to love life.
Lilliana, Toño, Paulina.*

To my parents, for giving me the coins of life to withstand the storm.

*To all colleagues and teams with whom we play the corporate chess.
We changed the world when we had the chance.
We broke paradigms and created new ones.
There will always be a before and after our time.*

Corporate Security a key piece on the corporate chessboard

“...this book not only addresses a contemporary academic need but also provides a professional reference that I look forward to applying today and consulting regularly for its practical and real-world context as it confirms the value proposition of having security part of the corporate conversation.”

Scott D. Lindahl, CPP
Vice President Corporate Services & Chief Security Officer
Kellogg Company

“It’s a sincere and deeply insightful rendition of real-world security told with empathy and humility that reflects the caring and experienced leader that Antonio is. A must read for CSOs globally”.

Wayne Hendricks, Head of Global
Security Macquarie Group

En este libro, Antonio, en base a una dilatada experiencia en el ámbito de la seguridad, sienta las bases para explicarnos como “profesionalizar” la faceta de la seguridad corporativa dentro de la estructura empresarial. Con un lenguaje claro y sencilla, explica la importancia de que ésta esté perfectamente alineada con los objetivos del negocio y cómo formar parte de la cadena de toma de decisiones estratégicas. En resumen, una obra que se propone con una magnífica referencia para todos aquellos lectores interesados en esta materia.

José Miguel Gordillo Luque,
Director de Seguridad Global del Grupo Iberdrola

Contents

Foreword	9
Prologue	11
CHAPTER 1	
Background or the Beginning of the Journey	13
CHAPTER 2	
The Meaning of Corporate Security	17
ROLES	18
SECTION A. SECURITY AS A FUNCTION	
WITHIN THE CORPORATE STRUCTURE	19
<i>Service offer as an executive of the corporate security function:</i>	23
FUNCTIONAL PREMISES	24
CONTEXT OF FUNCTIONAL INTEGRATION	26
STRATEGIC AND OPERATIVE SECURITY	28
STRATEGIC APPROACH	30
<i>Strategic management</i>	31
COMMENTS	34
SECTION B. SECURITY AS A SPECIAL SKILLED TASK	36
DESCRIPTIONS	37
<i>Corporate security</i>	38
<i>Intelligence of corporate security</i>	38

<i>Security of individuals</i>	39
<i>Personnel management</i>	40
<i>Information security / Cyber security</i>	46
<i>Crisis management</i>	51
<i>Special investigations</i>	61
CHAPTER 3	
The Model and Process of Intelligence	64
SECTION A. BACKGROUND: THE CONSTANT DISRUPTION	65
SECTION B. INTELLIGENCE OF CORPORATE SECURITY	65
<i>A new corporate framework</i>	68
SECTION C. INTELLIGENCE MODEL FOR CORPORATE SECURITY	70
<i>Convergence of the intelligence model with the intelligence process</i>	71
DESCRIPTIONS	72
CHAPTER 4	
Structure of the intelligence model	73
SECTION A. PROCESS OF INTELLIGENCE FOR CORPORATE SECURITY	74
<i>Phase 1. Planning</i>	74
<i>Critical questions</i>	75
<i>Phase 2. Search and selection</i>	82
<i>Considerations for the search and selection phase</i>	85
<i>Phase 3. Analysis</i>	85
<i>Considerations for the analysis phase</i>	86
<i>Phase 4. Diffusion</i>	87
<i>Considerations for the diffusion phase</i>	88
<i>Phase 5. Exploitation</i>	89
<i>Considerations for the exploitation phase</i>	91
CHAPTER 5	
Integration of the corporate security model and process	93
EXPLANATION OF THE PHASES AND THEIR EFFICIENCY	94
CONSIDERATIONS ABOUT THE INTEGRATION	
OF THE INTELLIGENCE MODEL AND THE PROCESS	97

CHAPTER 6	
Rajectory, real life cases, and lessons learned	99
SECTION A. RECRUITING & HIRING, HEADHUNTERS, AND HUMAN RESOURCES	99
<i>Case 1. Construction Materials Company</i>	99
<i>Case 2. Tobacco Company</i>	100
<i>Case 3. Construction Materials Company</i>	101
<i>Case 4. Telecommunications Company</i>	101
<i>Case 5. Retail Company</i>	102
<i>Case 6. Construction Materials Company</i>	102
<i>Case 7. Banking Services Company</i>	103
<i>Case 8. Entertainment Company</i>	103
SECTION B. LESSONS LEARNED	104
<i>Considerations about the learning curve</i>	105
<i>Section C. Social unrest (violence)</i>	107
<i>Case: Indonesia – Social violence</i>	107
<i>Case: Algeria – Social unrest</i>	109
<i>Case: Thailand – Coup d'état</i>	110
SECTION D. KIDNAPPINGS AND LOST PERSONS	112
<i>Case: Port-Au-Prince, Haiti – Kidnapping</i>	112
<i>Case: Bogota, Colombia – Kidnapping</i>	113
<i>Case: Monterrey, Mexico – Kidnapping</i>	115
<i>Case: Jalisco, Mexico – Lost person</i>	115
<i>Case: Quintana Roo, Mexico – Lost person</i>	117
CHAPTER 7	
Final reflections	123
Track record	127
About the Author	131

Foreword

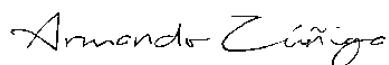
Leaving an exemplary trail through any journey requires perseverance and discipline. Accomplishing long-lasting hallmarks in a professional field would have meaningful outcomes; furthermore, success at this level in Corporate Security is simply unparalleled.

Security in general is constantly evolving, and its dynamic nature demands non-stop hard work, Corporate Security entails professional dedication; for this reason and after maintaining a successful performance over 28 years in the field, Lt. Colonel Antonio Gaona Rosete deserves full recognition.

In his book “Corporate Security, a key piece on the Corporate Chessboard”, the author provides testimony of the experiences acquired as an executive-ranking officer in both national and global organizations. The industries in which he performed the highest role of the Security function include: Construction, banking and financial services, retail, telecommunications, tobacco, and entertainment.

With almost three decades of professional acumen gathered in a fascinating sector not suited for the faint of heart, Lt. Colonel Gaona Rosete presents a successful managing model that permeates not only from the business field to the training venues, but also from the nook and cranny corporate hallways to the workshops and classrooms, and from the routine Security operations to the academic arena.

On behalf of every member in the Corporate Security, I would like to acknowledge the deep mark Antonio Gaona Rosete's work leaves on each one of us. Certainly, his work will be useful for all professionals in the field, as well as for the hundreds of students nourishing their learning; consequently, dedicating his life-long passion to cultivate and spread his expertise allowed him to reveal the road map of the Corporate Security role in our industry.

A handwritten signature in black ink, reading "Armando Zúñiga". The script is fluid and cursive, with the first letter of each word being capitalized and prominent.

ARMANDO ZÚÑIGA SALINAS

Prologue

The objective of writing this book is to share with the reader the concepts and experiences that allowed me to develop, over more than 47 years, as a security professional both in the public sector and in the corporate world, a successful model to perform the functional responsibilities of a *corporate security executive*. I developed the model and applied it successfully in Mexico as well as internationally on a global scale, working on executive positions as a manager first, and then as security director with companies in fields as diverse as construction materials, telecommunications, tobacco, retail, banking services, and entertainment. I defined such success according to the compliance standards international corporations expect from their high ranking officers; consequently, we would expect that kind of recognition when fulfilling the demands of a role that is, not only barely known, but also subject to many different interpretations, even by the security professionals themselves.

Adequately positioning the security function is achieved through certain level of interaction, as well as in the integrative role the security function must have in the development of critical business processes; these are bold indicators that determine the real position which translates as *the impact any security proposal has on the decisions made*, and that the company or employer recognizes as contributions of corporate security to the business. I have shared this experience

during conversations and lectures in diverse forums and universities with security professionals of any field, because I think it is necessary to fill an empty space in the general public knowledge about such an extraordinary profession of corporate security and their executive officers.

Likewise, I present four main realms from which the security profession is practiced: *national security*, *public security*, *private security*, and *corporate security*. The latter is where I look forward to contribute as I may by proposing some doctrinal points. Corporate security is the destination at which we, the security professionals, arrived to through different paths and with diverse motivations; this is the place where a new vocation was born to serve the corporations from within. I shall do my best to remain pragmatic, adding real life examples when available and applicable, since I have always thought that without practice, theory is not efficient. I truly hope this little big effort is useful and interesting; little due to its volume, but rather big thanks to the enthusiasm with which I lived every moment and I share them in these pages.

Background or the Beginning of the Journey

In September, 1994, after twenty years and sixteen days with the Mexican armed forces I received my honorable discharge and, by October of that same year, I was taking over my first assignment in the corporate world in the area of security. It took less than a month for all the years of experience to open the door for me to a new professional adventure. My arrival to that company occurred during a strategic moment because the organization had already started a global expansion process that would widely impact its objectives and, as a result, modify the organizational culture to a point where the company would become a *global player* in the industry. Such change, personally and professionally, put me through a complex transition due to diverse reasons.

First, the hiring company did not have a clear description of my position, not even the name of the post was defined; in the end, I was asked to do the job description and profile of the position I had already been hired to occupy, and then name it. The reason being that my position originated by the recommendation of the international consultant contracted by the company through its expansion process; the consultant recognized and stated the importance and vulnerability of their client's strategic information and, in turn, once the proposal was accepted, a new physical security area was missing in order to complete the setting of the information security framework. It is interesting however, that my opportunity with physical security

was triggered by the convergence with information security, a concept that is still being discussed currently in security forums.

Second, the authority and power criteria that ruled in government are not applicable in the private sector; I had to learn this immediately because the areas of executive protection and special investigations –which I thought to be among my strong assets, were the ones where I found the ruling criterion to be totally different.

Third, I found myself void of information and structured knowledge regarding corporate security, both within the company and with other security professionals of other corporations; as a matter of fact, this is a trend that prevails to date. I was facing a critical matter since, without a solid platform of what a corporate security function implies, how was I to chart a route to my career and professional development? How to build a career path in a corporation where nothing related is defined? I was astonished by the fact that I had been officially hired for a position that not even the employer knew the reason for its existence, except what the international consultant put in the proposal which did not provide the basic duties the required post would do which, as mentioned, became my first task upon arriving to my desk as the new area's manager. Throughout my career, I have seen similar cases in a number of companies. And the relevant learning is, after nine different positions, that even within top notch organizations one of two scenarios happen: *on the one hand*, it is either clearly described what your duties are, which is a very rigid criteria typical of companies that like to work “*by the book*”; or, *on the other hand*, management has no clue of the scope the function you are now in charge of, thus you find yourself joining the company to fulfill an immediate need, which is the reason why they hired you. Due to the above, I decided to:

Design a functional action model, considering the structure criteria and roles of other corporate functions, which facilitate setting the principles for a new function's performance on a fast-track approach and, later, elaborate on the detailed duties and the scope of the position.

Over time, I discovered that the professional development and economic growth you may achieve may be greater with companies that lack a clear delimitation of the area, because such situation lets you prepare and structure value proposals; additionally, the chances to grow shall open up as the security professional's abilities and knowledge allow. For this reason, I am eager to share my points of view about how extraordinary the profession of a corporate security executive officer may be; thus, I shall support my ideas on a 28-year trial-and-error process developing platforms and plans for various companies at national and international scale, all of which I regard were successful for two reasons. *First*, the value proposals I presented had relevant impacts on the business decisions made afterwards, since they transcended even after I left the organization. *Second*, the executive security function was effectively positioned as a critical service within the organization structure, making the position suitable for recognition and compensation according to the corporation's higher standards which, as a result, cascaded to the team members as well. I would summarize the above with the words the owner of an excellent organization once told me, he said that while I collaborated with them *"the work of security acquired dignity"*.

The Meaning of Corporate Security

What is corporate security? From experience gathered in the armed forces and in the private sector, I consider there are four professional fields within security, each field infused with specific tasks that demand particular profiles of the professionals to qualify for the job. Such fields are:

- *National security*—armed forces, National Guard, and the like.
- *Public security*—police forces of any scope: city, state.
- *Private security*—suppliers of security services and technology.
- *Corporate security*—employees and executives within a corporation.



ROLES

The distinction among the security fields is necessary in order to determine the conditions that regulate each one of them, as well as to segment the basic criterion, roles, scope, and specialties of corporate security; thus, avoiding the grave mistake of adopting models that work for national or public security to implement them in the private sector, or apply concepts that are successful in private security expecting them to function in public security too. I consider these options to be ineffective because we must strive to communicate within the corporation using the same language and concepts the organization uses. By switching my field of operation, my immediate objective became to “civilize” the knowledge and skills acquired while in the armed forces, where I carried out security roles to protect high profile dignitaries and, above all, conducted special investigations. Switching fields of operation requires an adaptation period, a learning phase. Being successful in one of the fields does not ensure that same outcome in another, and I know that for a fact. It is a mistake to insist on migrating predefined ideas or plans from one field to another, because they are all different from one another. Fields such as national or public security imply a vocation, while corporate security supposes “falling in love” with a profession to which we might arrive at through diverse paths. Once the distinctions among fields of action have been established, it is necessary to define what corporate security actually is. Hence, I propose a double description:

A. As a function within the corporate structure

- a) This description involves roles, processes, programs, key performance indicators (KPI), and the structure according to these.
- b) It also requires interaction in the agreement of the relationship among units or entities, according to their times, operating criterion, and organizational culture.
- c) And last but not least, business knowledge and corporate experience are a must.

B. As a specialty within the security field of operations

- a) Which only apply to the corporate sector.
- b) It entails the development and application in other specialties.
- c) And implies technical knowledge and skills, and operative experience.

SECTION A. SECURITY AS A FUNCTION WITHIN THE CORPORATE STRUCTURE

In order to define corporate security as a function, we must first identify the elements and roles that bestow corporate security with a profile that is relevant for the corporation, otherwise the outcome of our effort would be a line of operations that would keep corporate security as a secondary role. Traditionally, contributions from the security function translate to risks identified for which a series of solutions are suggested including processes, protocols, and technologies, all of which aim at security-related tasks to be assigned to other areas and hold them accountable by the company. At the same time, the security function strives to demonstrate the value of security through secret operations which, ironically, keep the value of security contributions secret; similarly, developing relationships with authorities and institutions portrays security matters as foreign to the company, alienating security from the company's culture. And this happens not only in Mexico but on a global scale, where the corporate security professional presents the proposals based on complying with a risks agenda (*risk driven*). From my experience with corporate security and in those instances with colleagues, who have also successfully positioned security as a relevant function in the corporate structure, the bulls' eye value is located on the businesses interests (*business driven*). This means aligning the security efforts to integrate them with the critical processes, understanding the timing and objectives of the company. That corporate directive implies greater business knowledge and operative skills, and focuses on how to make decisions. In order to establish a robust corporate security alignment which matches the

business interests, it is required to set forth the elements that sustain their guidance. These elements are:

- *Coexisting with risks.* The corporate security executive must identify the ways to support the company on taking risks and be prepared for loss management in the event an incident occurs. Business environment conditions may require making decisions that involve risks, what makes operations to be performed under resilience criteria. Therefore, plausible consequences must be analyzed, identifying the impact (loss) and how the company should assume the loss to, then, persuade the organization to anticipate such situations and make the necessary adjustments in the decision making process, so that risks are contained and avoid generating other risks not considered.

It is impossible to achieve absolute security. I consider that, in the new disruptive environments, the continuity approach has been replaced by the resilience approach.

- *Efficient communication.* As mentioned before, knowing the business language, the culture and times of the company to be able to communicate using a language that matches the corporation's language. An efficient communication allows us to know what an acceptable loss is for the company, and what is not. The efficient communication must be based on understanding the company's culture, that is, its nature. Understanding a language is not necessarily the same as being able to communicate using that language. Each company, and the people working there, have their particular ways which demand certain modes to actually connect with them.
- *Intelligence model and process.* The efficiency of the information you gather must generate the required knowledge for you to connect and effectively communicate with the company, and

demands a model supported by the actual knowledge of the company. But, in order to succeed in accessing the real information sources we should understand that access to those requires the security function to perform like any other function, for which your strengths are not based on your experience in security but rather on your interpersonal skills, on your managing ability, on your business experience, and on your ability to communicate. You must understand that even though you are in direct contact with the company's CEO and other top executives in the corporate offices, without networking through multiple levels and functions of the company you will not acquire actual knowledge of the organization. Furthermore, it will be through these networks that you may not only have access to the information, but you may also achieve the actual understanding of the loss criteria and, hence, be able to efficiently communicate within the corporation. All that said, states how critical it is to have a model to follow which allows the security function to actually understand the company before attempting to define the risks.

In my case, by consciously avoiding to impose the experience I brought from government security into the private sector, and searching for the knowledge on how to properly set my professional activity, I was able to create the model I needed to outline the two success paths for the executive corporate security function:

1. *Transcendence.* Through the impact that security proposals have on business decisions, becoming part of national and global processes and programs as well as being part of relevant and critical business process that transcend through time, e.g., *C-TPAT, Customs Trade Partnership Against Terrorism; SASI, Sistema de Administración de Seguridad en la Información; and others.
2. *Positioning.* Through recognition for all the security team achieved according to corporate standards, positioning the security function as an essential service for the business; therefore, improving

the level of interaction, salaries, training and development, and so forth.

These two paths totally modify the sense of the security value proposal for the company because, by aligning themselves with the business' interests, the security function sets out a change regarding the company's ability to become a secure organization. Therefore, instead of suggesting a security program for the company, the security professional shall persuade the organization about the critical role security performs within the company. Such persuasion shall gradually allow security to merge naturally into the culture, and this would be achieved without threats or sanctions. The above impacts not only on the profile of the security professional striving to arrive at an executive position, but also on the professional development that must be defined for the corporate security function. In other words, a much better fit for the function within the organization should consider that:

The traditional outline based on models transcribed from national or public security are not effective, because the model required must focus on the security professional having operative experience as well as a strong executive business profile.

Service offer as an executive of the corporate security function:

Up to this point and having as the goal creating confidence and trust for the corporate security function, I consider the following elements to be part of the service offer which would support the function:

- *Organizational culture* – Actual understanding of the business nature.
- *Internal alliances* – Knowledge of the areas and their critical processes.
- *Business strategy* – Identify the company's objectives and timings.
- *Internal and external* – Understand the company's loss criteria.

- *Corporate security justification* – Identify strengths and weaknesses of security in order to manage the previous points.

All the aforementioned clearly denote the need to identify the objectives the security function shall have and, as a result, the success criteria. Traditionally, hard facts and metrics are sought after, which might be valid, however there are other criteria that strengthen the functional positioning based on credibility and trust. These criteria include:

- *Impact* of the security proposals on the business decision-making process, e.g., policies, norms, processes, culture, etc.
- *Weight* of sponsorship and internal alliances, e.g., who believes in you, who trusts in you.
- *Role and stages* of the business critical processes in which you are included, e.g., advisor/operator.
- *Budget* approved for organizational structure and proposals, e.g., investment/cost.

FUNCTIONAL PREMISES

Once the security function is operating within the corporation, it becomes vital to discuss the characteristics that rule the security team's development; the premises that follow must anchor the function with content, form, and parameters that guide its performance throughout the on-going business operation.

- A company is secure when security is an intrinsic part of each and every activity performed by its executives, employees, and vendors. Consequently, resilience is a life concept that must apply constantly throughout our strategy; hence, the relevance of:

Persuading the organization's top management of making security a natural element of their culture to ensure its functional success.

- Strong internal networking and alliances *integrate the security function* to the organization. These are the elements that provide the credibility and trust to sustain corporate security. Regardless of how close the position is to the top executive levels, the alliances at all levels constitute the actual make or break for the function. There is no such thing as a small or unimportant position in any organization, all positions have their specific weight and timings. It may be hard to believe that an initiative from the first-level executive (CEO) could get stuck as it gets disseminated through the hierarchical levels or functions. In one occasion I witnessed a new executive, whose leadership was sponsored directly by the CEO, launch a program which simply did not fly due to this new executive lacking internal networks and alliances. Without a good relationship or internal alliance with all management levels in the company, support from top executive officers may not suffice for a successful implementation effort; organizational culture and its interwoven fibers also play a key role.
- Regarding taking risks, support from the organization becomes *the driving force behind security* which make developing strong internal alliances a must, as well as an efficient communication and a keen persuasive ability since the decision-making process requires calculating risks that help to identify the probable loss, as well as include new risks during the business operation and its decisions. Risk-taking does not imply making decisions blindly; rather, it is the security executive professional to outline the risk and its probable impact, which means weighing the loss against the benefits the business decision represents.
- *Efficient integration* to the business primary processes and controls requires developing knowledge and abilities regarding specialties that are usually other functions' responsibilities, such as business continuity, regulatory compliance, brand protection, or special investigations. These specialties, due to authorities regulations or internal normative, must be carried out by entities like audit, internal control, or the legal department. In order to

contribute, instead of being only a random support, it is necessary to train and develop the corporate security executive to have the proposal recognized and valid to exert control functions. We may be an important part to fulfill the compliance of norms and processes for these specialties, although to become an integral part of the executive team that plans, propose, and validates requires a higher degree of knowledge and skills which implies being acknowledged by the other functions. In summary, it is of utmost importance to possess business knowledge and operative skills.

CONTEXT OF FUNCTIONAL INTEGRATION

Identifying the level of integration of the corporate security function with the organization requires establishing the context for three integration levels. And the integration is supported by the following elements: First, *the function's interaction level*; second, *the topics proposed* in such interactions; third, *the approved budget*; and four, *the convergence with key areas*. The actual context is the precise measure of the positioning of the corporate security function; therefore, the aspects mentioned must be measurable. The three integration levels follow.

Operative level, e.g., risk driven:

- Security fulfills with the basic processes of surveillance, access control, CCTV, low-impact investigations, and supports other functions according to their requests.
- Security is in charge of very basic topics and is not considered to attend relevant business meetings.
- Security budget is defined by other areas.
- The security team reports to and interacts with a functional director.
- Security is a required function but, like other services, it does not have an impact on business decisions.
- Security is not included in important meetings.

Mid-level, e.g., hybrid:

- Security has internal clients who escalate their support requests.
- Security proposals begin to be included in relevant processes.
- Budget approval for security implies competing with other areas for resources.
- Reporting line and interaction with division directors and, sometimes, with top level management.
- Even though there is greater interaction, there are no proposals from security yet that impact the organization culture.
- Security is aware of important meetings and may be briefly required to attend.

Strategic level, e.g., business driven:

- Security has internal clients who request their collaboration in high-impact projects like business expansion, closings, fusions, due diligence, and post-merger integration.
- Security contributes with information that is regarded relevant for decision-making in impact-graded projects.
- Security proposals receive relevant budget approvals.
- Reporting line and interaction to top management levels.
- Security is included in important meetings.

As strict as this grading might seem, it is necessary to avoid attaining a false validation or a mistaken interpretation of the actual value the function has for the company. Decisions aimed to modify the development process of corporate security should be made only based on a strict assessment of the function. I have witnessed many cases of self-complacency which end up in the professional development of the security teams becoming stagnant. Reaching a strategic level demands an intense and well-planned development carried out successfully to achieve it. Each step climbed up through the hierarchy levels requires scaling up the projects, the type of interactions, and the ability to deal with internal policy situations.

Dignifying the security profession and positioning the corporate security role brings with it great rewards for both the employee and the employer.

STRATEGIC AND OPERATIVE SECURITY

In accordance with the outline so far, it is absolutely natural to have two proposals for security: the strategic one, and the operative one. The first one establishes *what, for what, and how much* of the value proposal; while the second one focuses on the implementation of *who and how*. On the one hand, strategic security is applied at corporate level, where the decision and control functions make the agreements, e.g., top management; on the other hand, it is at the operative level where those agreements are executed, where the business units follow the norms and guidelines to meet the KPI or key performance indicators and, in the field, no proposals are required.

It shall depend on how mature the security organization is to empower their operative units. Being the one responsible for developing the strategy and value proposals for a company is actually a rare opportunity, particularly on a global scale. In my case, and following the model of successful colleagues, I have always practiced allowing the business unit freedom to design their own proposals, as long as they observe the corporate KPIs. While having the global security director responsibility, I always fostered that each country business unit worked interdependently with the corporate office, which makes corporate security to have abilities and skills that complement the countries' units. I am a firm believer in that this approach yields healthy relationships and a steady development process. I have been hired by companies where the security requirement directive was to hire the best security profile available in each country, which shall operate according to very simple KPIs, providing them freedom to develop their own security solutions. In order for this to work, the corporate security director must operate in a strategic context.

For many companies, taking the corporate security function to the hybrid context is a challenge when they report to corporate offices that are rather rigid in their KPIs. One of my experiences was working for a global company in the tobacco industry where only three KPIs were enforced: zero lives lost, no more than one product unit loss, and keeping budget aligned with the company plan; therefore, I was allowed to develop the country-wide strategy and operation plan based on those three KPIs.

In another case, with a telecommunications company the orders were to follow the corporate guidelines to the letter, with a centrally negotiated budget and adhering to the forms they sent to the units. My profile is more aligned with the first example, while operating globally I worked with a small central team, very creative and versatile, that were knowledgeable about the business and had sufficient operative experience. This team, integrated by the best security profiles in each country, allowed me to steer quite versatile work groups where every team member grew and developed skills becoming able of preparing their value proposals which, to a point, challenged me to stay on top of my learning so that, as director, I could stay on top of my teams while keeping them improving their results by constantly learning. Implementing and operating that way taught me the elements to define my concept of strategic security.

Strategic security:

Strategic security is *the science and the art* necessary to develop a value proposal, all in a *convergence effort* with all the corporate functions, *aligned* with the top management strategy to achieve the business objectives set for the company.

- *As science:* it implies the knowledge and talent to understand the value criteria that define the company, its timings, its nature, and its objectives. The characteristics of science are business knowledge and executive talent.

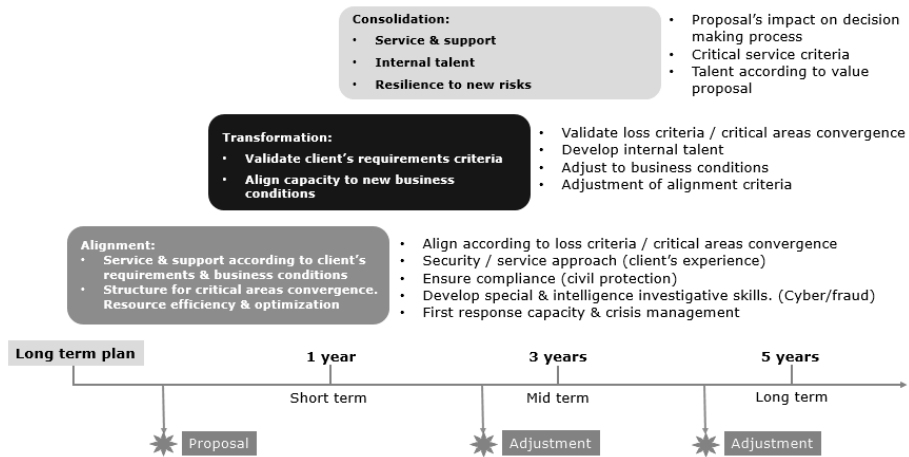
- *As art*: it assumes a set of people skills to understand the organizational culture in order to empathize and communicate efficiently within the company. It is truly an art to be able to persuade respecting the organizational values. The characteristics of art are skills and experience both personal and professional.
- *Convergence*: it means to recognize the value in the proposal, and have the latter included in the decision process of the company.
- *Aligned*: it means to have the same objective as the other functions, namely: understand the timings, the business environment, and support the scope of the company's objectives.

STRATEGIC APPROACH

Setting up a corporate security strategy according to the preceding concept implies a process that is key to security, since the function must lay out objectives for the short, middle, and long terms as shown in Figure 1; all of which must go through a planning process that would refine not only the value proposals but also the complete function's evolution.

In order to develop the strategy it is necessary that concepts like the roles and scope of the function, the proposal of plans and programs, the job descriptions and profiles and, obviously, the structure and budget have been validated by the organization including not only human resources, but also the other areas with which security converges and serves them; thus, the key resides in the company knowing well the function and acknowledging the area of security.

FIGURE 1. CORPORATE SECURITY STRATEGIC PROPOSAL.



Without such validation, the strategy proposal is a worthless paper, an ideal without support. Unfortunately, I have seen many organizations in which the security director focuses in defining a vision or a mission that, even though they make sense, they do not succeed in positioning the security function. These two concepts are value premises for the security team but, ultimately, the strategy value proposal is the one that sets the function's direction through the times to come.

Strategic management

Strategy management can be carried out via various methods or systems. Personally, I followed a process that allowed me to manage efficiently while I instilled a methodology in my teams that, over time, became a work and life discipline. Such a discipline helped them anticipate and be prepared to adjust to the changes and criteria that rule in any organization. I applied this methodology successfully in the diverse types of industries where I have operated and managed, as well as at different knowledge and experience levels of the teams.

The method is called *6G*, or the six lines of management. The *6G* methodology is based on six dynamic elements which cause constant movement around the security function in such a way that it adjusts to the organization's culture and operations, constantly looking for new proposals, reviewing what is done to improve it or adjust it. These are the *6G*:

- *Proactivity*: the proactivity line implies that the security executive achieves strategic and operative anticipation based on the knowledge of the organizational culture, the company timings, and their functions. By anticipating, the security executive would be ahead of potential new projects, changes in the company's objectives or in the organization structure, foreseeing what these might represent with regard to the current value proposals presented to the company. Obtaining that reading, the security director shall be able to anticipate and adjust the function's own timings and proposals. Proactivity is looking to anticipate changes that might present conditions like complex economic situations, a fusion, an acquisition or a refinancing maneuver, and even changes in the organizational structure at functional or top management levels. Failing to identify any of those signals would leave you without a chance to make timely adjustments, missing the opportunity to be efficiently prepared for any situation.
- *Control*: the control line means establishing the required mechanisms to maintain security's timings in synch with the company's timings. Control implies building the functional processes necessary to handle your management, communication, and implementation timings. Without control, you will miss the proactivity effect and will be running out of synch regarding your internal clients and their processes. Control helps you anticipate and plan your proposals accordingly. Control is not just a methodology to manage projects, it is a discipline that enables you to know when to schedule a meeting with the company director. Control requires you to efficiently manage communication, follow-up, and validation.

- *Communication*: the communication line consists in establishing an actual connection with the organization, which involves how and when to establish and stay in contact with each actor within the organization. Success in this regard demands a deep knowledge of the company, its culture, its organizational language, and its operational timings. The connection with the organization is build and maintained on a daily basis through the knowledge and skill to convey, from an executive presentation –business oriented, simple, brief, and efficient; a telephone call –clear, simple, and to the point; a contribution during a meeting –brief, sustained, and supported by your internal clients; and even mastering the body language or the personal image you project with and through your team –executive image. All of these are the basis that help you anchor that connection. Communication requires you to be proactive, be in control, and follow up.
- *Follow-up*: the follow-up line implies continuity of actions from start to finish. It is the drive with which the security team pursues each project, each proposal, and each contact. It is the need to carry every started effort to completion. Follow up is key because it requires keeping everything under control and linked up via efficient communication.
- *Validation*: the validation line consists in ensuring the proposal is valid regarding the service requested as well as the value of the proposal. This aspect is basic because frequently it happens that a value proposal that has been formally presented, accepted and, sometimes, implemented, is no longer relevant even for the person who requested or authorized it. Be that because their interests changed, or they decided to postpone it or, simply, because there is no budget available. Validation also implies quality control to ensure each internal client is satisfied, and this requires good communication and follow up as well.
- *Alternatives*: the alternatives line expects adjusting the proposals and actions according to validation so that every internal client and situation needs are met as required. A good practice is

to always have in mind ideas on how to adapt to changes, to new opportunities, and to adjustments in the requirements; doing so, you will always be ready for a change and adapt on time to look for alternatives. Developing new proposals not only implies innovation ability, it also requires actual knowledge about the company and their internal clients. Acting proactively involves communication and validation to anticipate possible changes.

COMMENTS

Developing the corporate security function as one more function within the organization structure is critical; and yet, providing the security function with value recognized by the high administration and other relevant functions is vital. The process requires business knowledge as well as interpersonal skills that are acquired through training and corporate experience. You might perform the security responsibilities within a corporation during a number of years; nonetheless, this does not mean the function has been positioned according to the company's recognition standards. Interaction levels, business process criticality, training and professional development, salaries and structure, are some of the elements that describe the function's positioning; however, the utmost important element of all is the impact your proposals have in the corporation's decision-making process.

Nowadays, the most relevant global security associations like the International Security Management Association, ISMA, and the American Society for Industrial Security, ASIS, have established that the security proposal demands new knowledge and skills to be at par with what any corporation should receive from the security function. For this reason, they have formed bonds with prestigious universities in the U.S. –Kellogg, Wharton, and in Europe –IE Business School, Technische Hochschule Ingolstadt, to open up training spaces for security professionals who work with corporations; thus, the executive development curriculum include, among other subjects, proposals that:

- Empower the security leaders to interact with top management executives.
- Develop their business knowledge and sharpen their abilities to face risk management.
- Allow them to understand the critical business concepts to widen their strategic perspectives.
- Foster value creation.

This scenario represents quite a different offer for the corporate security executive and it implies, not only to possess the knowledge baggage as described, but also that the company's expectations with regard to the security executive and their responsibilities –the security team as a whole, are perceived at a higher level thus, the company is willing to invest in their training and development.

- Furthermore, there is still a consideration of great importance. Security usually deals with situations and problems that differ from what is considered business-as-usual by the rest of the functions, consequently, most executives prefer not to learn about them unless the issue's impact transcends and affects them directly. Hence, an expression I heard once from a colleague, who was a director in a global company, is: “My boss always says: ... *do not bring me trouble, if there is trouble, fix it!*” This explains the nature that is commonly found among executives and the companies' culture; so, providing security with a business-like approach requires creating relationships with top management levels and all areas alike; while doing so, the contact with security should be brief and to the point, the situations shared are already solved, the proposals mentioned with clear impacts, and the solutions implemented with the affected areas. This executive interaction should facilitate making any decision that might still be required.

SECTION B. SECURITY AS A SPECIAL SKILLED TASK

Once corporate security has been described as a function within the business structure, it is now the turn for the special skill task to be discussed. This topic peaked my interest because I believe there are plenty empty conceptual spaces in the security profession, which we fill up according to trends we see around or, otherwise, we simply try not to explain or worry at all. From my standpoint, corporate security is not recognized as a specialty and it is barely identified as another operating mode on the security list, which is why it is not seen as a corporate function. When I describe corporate security as a specialty, I must explain about what I regard as a confusion between the concept of specialty and the concept of special nature. And my explanation goes like this: I have worked in diverse environments and types of businesses which include construction materials, tobacco, telecommunications, retail, banking services, and entertaining; then of course, there are all the other industries such as pharmaceutical, logistics, energy, airports, and etcetera. Each one of them has a special nature, and each one of them requires an in depth knowledge of their nature as well, which is acquired only by operating in their fields and ranks and, with time, their nature shall be mastered. Based on that, I can state that I am a specialist in the construction industry (11 years), in retail (5 years), in banking (4 years), and for all of which I transit through a learning curve to acquire those specialties. As an example, before joining the retail industry I was in the construction materials business as their global corporate security executive and, as I took over the security director role in my new endeavor, I was told by the welcoming colleagues that it should take me no less than five years to consider myself knowledgeable in the retail business, which happened to be true; therefore, something similar happens for every industry and type of business. This leads to the need of experiencing an immersion process in each company and the corresponding learning curve, which I will comment further in the chapter dedicated to the intelligence model.

Now, I have suggested that each company's nature is special and that they require the respective business knowledge and skills for one to be able to understand and coexist efficiently within each organization; however, regardless of their nature, it might be possible to implement in any type of industry and company, in one way or another, the diverse security specialties that we find out there. In order to cite those I consider to be the most relevant, the following list is further described below from the corporate perspective:

- a) Corporate security
- b) Intelligence of corporate security
- c) Security of individuals
- d) Personnel management
 - Guards
 - Consultants
- e) Information security
 - Comments on convergence
 - Considerations about convergence
- f) Crisis management
 - Critical infrastructure: crisis management and business continuity
 - Considerations about crisis management
- g) Special investigations
- h) Information security / Cybersecurity

DESCRIPTIONS

I prepared this material having as a starting point the manner in which these specialties apply in corporate security, without aiming for a thorough research on every specialty. Some of them are not exclusive of corporate security; such is the case of investigations and crisis management, on which security may converge with other functions and have a shared responsibility in accordance with the actual security capabilities, and with the type of situation and the company

culture. I share my point of view from the successful lines of action I have witnessed, and from one or several of the specialties; thus, following are the descriptions on which I sustained my proposals as security director, both nation-wide and at a global scale.

Corporate security

This is the basic specialty, because it implies how the security area is perceived by the rest of the areas from both the corporate and the operative perspectives, and particularly regarding human resources. Many colleagues name the area differently, although I consider the right term to be corporate security. This specialty entails the application of other specialties and, as a result, requires knowledge, business skills and, above all, operative experience. It is extremely hard to apply any of the specialties without experience. For clarity, an analogy with the medical profession should help, consider that the equivalent to the corporate security leader is the internist physician, who would analyze the patient first and would write the first diagnostics that, subsequently, would lead the patient to the required specialists. The internist will be as good as good are their diagnostics. Similarly, the specialty in corporate security implies knowing the other specialties although not necessarily dominate them, in order to be able to later define the security proposal. This also requires seniority in the function to generate trust and credibility organization wide. The corporate security specialty is not available in a standard format; which makes it interesting because, as a specialty, corporate security would be as relevant to the company as efficient has been the effort to position the function. You might be managing the operation of corporate security without applying corporate security.

Intelligence of corporate security

The specialty of intelligence of corporate security is little known, even though we all say we are experts in it. *First of all*, because the concept of corporate security is also unpopular and seldom utilized

even by colleagues within corporations; *secondly*, because the information on how to develop corporate security is scarce; *thirdly*, because I consider the approach with which the intelligence of security focuses solely on identifying risks, taking the positioning of the function for granted instead of developing trust and credibility based on the approach the function has towards the business; and *lastly*, because the criteria of intelligence of corporate security demands actual knowledge about the company that facilitates identifying the loss criteria recognized by the business, and consequently requires action. My experience confirms that only companies' validated losses (impacts) drive the companies to make real decisions, which also demonstrates that the actions to prevent losses frequently result from compliance instead of emanating from the companies' culture. I devote the next chapter to explain in detail the concept of the model and process of intelligence of corporate security. It is important to highlight, though, that every outcome from the intelligence of corporate security shall be as valuable as the magnitude of influence it has on the company's decisions.

Security of individuals

This is one of the specialties that impact the most on corporate security, although usually its relevance is based on protecting executives as the main security program disregarding the effects on corporate security; bear in mind that, what is done while protecting executives would serve certain level of the organization, leaving a valuable gap in safeguarding other individuals down the hierarchy lines. The security of individuals centers on the utmost precious element in the list of probable losses: life or any damage to physical or moral integrity of persons. Hence, in addition to the human life, the impact must consider the value an individual represents for the organization translated as the hypothetical loss from perspectives of their business knowledge, legal investiture, and leadership role. An efficient model and process of intelligence defines the categories for the individuals according to their job, exposure, role, nationality, operations status,

etc. Once the categorization is done, the risk elements likely to create what is called a “life threatening situation” or LTS must be identified. These elements facilitate the creation of various risk groups depending on the type of company, which generates an offering of programs or solutions quite diverse. As a result, there is the *VIP* group which is normally defined by the business owners, the top management, or the stockholders; and the owner might be part of this category, as well as any member of the top executive levels (C-Suite) or a stockholder, and this is where the executive protection category comes in although it may not apply to all the individuals that might be in this group. Next is the group of “potential risk persons” or *PRP*, which includes those employees who, inherently to their exposure, are subject to environment or context-related risks or to risks directly created by the activity they perform; within this group we find business travelers and executives responsible of closing business negotiations or terminating work relationships, e.g., human resources executives firing employees or employees dealing with clients that, eventually, might turn aggressive against them as could happen to a bank teller. Another group includes the high impact persons or *PAI* (in Spanish, “Personas de Alto Impacto”), which refer to employees that due to their business knowledge and job position the company regards them as indispensable because their loss would be critical for the organization; thus, this category encompasses the business continuity teams. Lastly, there is the *PAC* group (in Spanish, “Personas de Alta Consideración”) which includes all the employees, clients, and vendors whose integrity falls under the criteria for safeguarding life and integrity of the company. I consider that the mentioned above represents a solid foundation for the security of individuals as part of the security proposal, and it opens up a space where programs and related actions can be adequately presented.

Personnel management

During my personal experience, there has not been a single security experience, either on a national or global scale, in which I have not

operated without external or internal personnel in order to satisfy the multiple security physical requirements. On such occasions I have hired services from hundreds of external providers and I have managed around seven thousand internal elements, all under my command –which is a larger number than an entire division in the military. The external component of these personnel is referred to as *guards and consultants*.

1. Guards

It may seem a basic topic; however, the image of the security area totally depends from them because it is a security guard whom the employees meet daily upon arriving at the facilities, and it is also a security guard who greets clients and vendors when they come to the business units. This is actually a delicate matter because the guards are frequently regarded as secondary to the security services, and it is in fact a permanent discussions with areas such as operations, procurement, or human resources, since they question why these personnel are necessary. Managing personnel implies preparing a value proposal to demonstrate the benefit for the company, and thus the external personnel is considered as the important support that is necessary in addition to the security service the function provides to the company.

Moreover, when the need of external security personnel (guards) is brought to the table, the areas taking part in the discussion to decide their cost usually question the amount without considering the actual value of the service; this discussion might start due to corporate security lacking the effort in advance to describe the real necessity of the external support. This work requires identifying the areas that need the service which is called the “service structure”. Each service post entails as many processes as they are required to take part of, for instance, human resources might ask for a control of external personnel –which includes all contractors besides the external security personnel, to comply with certain authority regulations; internal control might ask for the incoming and outgoing of product and

materials; logistics might require the control of entrance and departure of transportation services; audit may ask for counting merchandise entering and leaving the warehouses; and information technology might need that all computer equipment brought in or taken out of the facilities be checked.

While describing this process, the value proposal for the service of external personnel might be defined as well, and determine how the entirety of their service is conformed; then, assigning the corresponding percentage of time and abilities that each process requires from the external security personnel, the areas would be able to visualize the actual value of the service in accordance to their requirements. It is interesting to realize that, in the end, the resulting percentage assigned for security-related processes and activities is always less than the sum of the other percentages. I noticed that, in the construction materials industry, we determined a ratio of 80/20 after identifying that the external guard used 80% of their time to security-non-related processes. A similar outcome was found in the retail industry where the ratio reported that 25% was dedicated to product loss, 25% to civil protection, 25% to customer service, and 25% to security-related tasks. This was the case that represents my experience with around seven thousand internal elements –required due to the spread of the retail operation, and thus the company recognized the value of maintaining that structure operating based on the knowledge and skills the personnel had to have according to the value of the elements being protected –people, materials, and facilities; as well as the actions that could be required to take. Efficiently managing external personnel brings along a new way of interacting with the other areas, which facilitates making them aware of the value the security area provides for them. This is particularly important when explaining to them the need for the external personnel to have the training and skills according to what we expect from the security guards regarding their functional areas; and even in circumstances where the external personnel substitutes the internal personnel who should be performing such tasks, which might bring the discussion back to the cost of the external service. As you might notice, this

aspect is critical because the functional role of security demands high impact and low cost proposals from us, and we have to find alternatives that satisfy the company's requirements. Such work is not done by the external vendor, and part of our challenge is to develop the process and promote it internally; another part of the challenge is to train personnel to efficiently execute their processes, making sure the service provider is able to comply with the level of service they were hired to perform.

In order to maintain a healthy relationship with a vendor it is necessary to know their cost structure and understand their relationship, as well as ours, with their employee who shall perform duties within the service structure previously established. This specialty involves more than buying a service from a vendor; it requires to reason out their service; and entails interactions with several functions, build the service structure and proposal, internally sell the proposal, and cultivate the relationship with the vendor according to what we expect to accomplish, understanding their cost structure and quality proposal. These are all topics that require knowledge and business skills, in addition to management of external resources.

2. Consultants

Managing a consulting service —also as external support, is a relevant matter because it is a topic with multiple interpretations as well and, in some instances, feared by corporate security professionals due to either lacking understanding of how to work with them or as a consequence of how the consultants arrived at the company. I must point out that, in my opinion, not many consultants are well versed in the corporate environment thus their proposals do not have that specific knowledge. Thus, as I joined the private sector, I came across external consultants hired by the organization as a result of the company not having their own security executives. During my career, I worked jointly with external consultants on kidnapping cases as well as in the personnel evacuation process under political unrest situations. There was once when consultants were assigned to my

area to examine the actions being carried out by my function. Each particular case had their own repercussions in my executive management performance, and I learned that good management of external personnel might be very valuable for positioning corporate security; however, any misunderstanding, any proposal out of focus, or any slightly vicious selling initiative from the vendor shall turn out totally negative. Professionalism from the consultant and their knowledge of specifically related topics are crucial to achieve a positive and constructive relationship; particularly, when teaming up with the security executive in order to be able to detect from the consultant any piece of information they might not perceive in the short term like the organizational culture, the business timings, the loss criteria, and the positioning of the security function. In summary, I consider the most relevant aspect is to clearly identify the roles the consultant is required to perform. Personally and having worked with external consultants, I consider the following roles:

- a) *Knowledge*: there are situations that require knowledge about specific subjects, or that a specialist contributes with new models and methods that allow the setting of new guidelines or improve the existing ones. Security is dynamic, hence the importance of staying up to date. There might be occasions where listening would be enough to improve our proposal allowing us to enrich what we have developed, as well as to measure our position and knowledge. If we ever feel that our proposal has become stagnant or that we are not being able to position our initiative better, asking for external help is a totally valid move; therefore, resorting to consultants that have operated in the corporate realm might bring in new ideas and lines of action. My case in this regard is a crisis management experience in which I worked next to an international consultant in a kidnap situation; their knowledge on dealing with the problem was very interesting and useful, the experience gave me the basis for handling kidnap situations in Mexico, Colombia, and Haiti under totally different conditions in ev-

ery scenario, and it also provided the common ground rules to manage each instance. The consultant's contribution was mostly on the operative side of the procedure than on the critical portion, which refers to communication and coordination with corporate and top management during highly complex situations, a segment of experience and knowledge I acquire only through being the operator myself.

- b) *Validation*: an external point of view may give value to the internal proposals, identify weak spots, and contribute with knowledge to enhance our function and our proposals. Achieving this requires to identify the consultant who will add this value, without fear of having an expert validating our work. We may rarely see security executives looking for consultants to obtain support in this regard. Another situation is when the company is the one calling an outside expert for an additional opinion, which is valid, especially under high-impact circumstances although, in such a case, it is critical that the consultant really possess the knowledge, the professionalism and, particularly, the corporate experience to present their assessment. There was once a bad experience, in which the hired consultant turned out not to be an expert regarding the consulting business in general, the consultant job was solely to fill out a format and, next, to offer himself for the proposal implementation.
- c) *Operation*: there are situations where the implementation times require expert hands to speed up the process. Facing an evacuation process for personnel in Algeria, I looked for support from consultants and, similarly, I had consultants in the operation when we had to protect executives in Bangladesh. Both cases were successful. On the other hand, however, I had to manage a kidnap situation in Colombia, teamed up with a consultant that did not know the country, the *modus operandi* of the perpetrator, not even the language, obviously it turned out to be a terrible service. In conclusion, it is critical to identify security providers with real capacity; it is not wise for that com-

pany to hire an expensive consultant to justify what was overlooked due to negligence or misunderstood savings.

Information security / Cyber security

In 1994, certain international consultants advised the CEO of a cement company about the criticality of safeguarding the organization's information and, since the company was carrying out expansion plans and was about to enter the global market, the subject of corporate information risks was starting to gain attention. Topics like industrial espionage, information theft, hackers, or internal threats had started to be popular concepts in the security arena. This context gave origin to the information security management office within the security direction of the cement company. The most relevant aspect of this situation was that the consultants recommended the creation of a physical security management office as an instrumental piece for the information security process. And that is how the position originated, a post I took as my first experience in corporate security. The keys of this process were:

- Information security was placed outside of the information technology area (avoid to become judge and jury).
- Physical security acted supporting information security (convergence).
- Relevant topics: corporate security, through the information security management office carried out programs regarding ethical hacking, network vulnerability assessments, and social engineering, the latter jointly with physical security (independently from information technology).
- We progressed during a number of years, although we never converged on the same objectives or in taking the physical risks as a relevant subject for information security. In the end, the information security area was absorbed by the technology area, which I regard as not healthy for the company since they become judge and jury. Many companies, however, have already achieved the separation I suggest.

- During my years of corporate experience, the concept of convergence has always been on the table for discussion although with a variety of outcomes, being just a handful of companies with a mature corporate security vision the ones that have reached this stage, breaking the functional turfs and egos to give way to a truly secure company since convergence must include the other critical areas like internal control, audit and compliance, and even human resources. In my case, I succeeded in achieving this convergence while I was the executive security and intelligence director of a financial institution, where I included investigations and cyber investigators who developed investigation and support programs jointly with the technology function. We worked hand in hand with cyber security on prevention and investigation processes. Nowadays, we are still performing the same process, which includes the technological knowledge and ability in the security direction of my current organization according to the new institutional timings and projects.

1. Comments on convergence

To converge means integrating objectives and resources towards a specific mission. When physical security converges with information security (cyber security) their efforts should be aligned towards a common objective, which would be to make the company a more secure organization. This requires a coherent collaboration between two functions that normally work in diachronic manner. Convergence does not imply that both entities would get rid of the essence of their individual missions, it requires both parties to help each other in defining a mission with clear goals that supports communication and collaboration. Today, the development of the Internet of Things (IOT) or the Industrial Internet of Things (IIOT) are conducting every online session to scenarios where attack threats are hybrid; therefore, the cyber physic systems (CPS) make the development of a coherent convergence program mandatory. This becomes evident when servicing the security of essential systems such as fi-

nance-related, energy-related, or transport-related, where lacking the support from a critical vendor would impact the operation of technology-based systems; or, on the other hand, a natural disaster that would translate into the loss of essential operators or critical facilities. Be that as a preventative measure or as part of the business continuity plan, both areas should collaborate in a coordinated manner. The benefits of convergence include, among others:

- An integral vision of threats for the company, which facilitates defining the position and criteria of corporate security within the organization.
- The development of a holistic strategy that aligns risks management and threats.
- The increase in the efficiency of required efforts, which improves productivity and resources optimization.
- The development of the knowledge base through mixed training (physic & cyber).
- An efficient communication and collaboration process during contingencies management.
- A value proposal for the company that permeates the organizational security culture.

This approach leads to a convergence that not only aligns the security areas, because it also attracts other control and support functions to participate in topics of compliance, business continuity, and risks management.

2. Considerations about convergence

As mentioned, I have always strived to escalate the value proposal of the corporate security area under my responsibility, *taking into consideration that convergence brings tangible benefits to the organization by explaining how an integral vision facilitates efficiency, optimizes resources, and achieves a clear loss management.* Consequently, I have always aimed to position security services and support with the critical areas of the

organization based on this concept. While performing my security role both, on a nation-wide operation as well as internationally, I have gone through the following situations:

- Cyber security operates in an independent fashion, leaving the human component out of the equation and, when they encounter this component they call physical security –although that means joining an ongoing investigation somewhat out of step, increasing the complexity of the case and causing the task to be inefficient.
- There are times when incidents labeled as cyber-attacks from the beginning, are actually physical and are connected with aspects that, having the case's context, make sense; however, the search for solutions would be misled which would require more time, make the process inefficient, and brutally increase in the loss magnitude.
- Continuity plans for critical situations are developed without including the standpoint of physical security, which would be the operating area in such cases.
- The technology function absorbs cyber security, becoming judge and jury, and isolating themselves from the other areas particularly when an investigation is in progress.
- Cyber security focuses on external threats, not paying attention to the internal threats while, frequently, their vulnerable points are within their own resources which turns them into the internal threat.
- Internal threats are not weighed appropriately, because they are not considered a feasible threat by the human resources area or the control functions, all of them stating that fraud and abuse of trust are the only risks to worry about.
- Cyber security personnel are among those who comply the least with basic physical security criteria required to ensure the efficiency of the management system of information security.

Experiences like those above caused inefficiencies when working on incidents and, more frequently than not, represented important

losses because, having a coordinated plan or a convergence program might have avoided the negative outcomes, or could have mitigated the monetary losses. These situations must take into consideration the impact on the corporate image and the repercussions on compliance with rules and regulations, as well as the internal exhaustion especially when the perpetrator is found within the organization. As of today, several studies on the matter demonstrate that, in spite of the outlined benefits, the concept of convergence remains as a wishful thinking theory in which the *Chief Security Officer* (CSO) and the *Chief Information Security Officer* (CISO) move in parallel paths. The lack of leadership, the turfs of power, and the functional ego are still the main obstacles. I personally consider that, in addition to the noted above, the following happens:

- I acknowledge that physical security has a limited scope in their corporate roles and, as a result, in their capacities and services; which limits the function to basic topics of physical control for information security. Frequently, physical security does not have a robust area of investigations, where including professionals with knowledge and skills for forensic cyber investigations would guide the security proposal to converge with cyber security. The situation becomes even more relevant because, who would investigate the technology personnel then?
- The internal dispute, in which the technology area wants to control cyber security and where also the struggle for resources put the professional ego in a crossfire, keep cyber security operating in parallel paths with technology and physical security.

A different perspective for corporate security is required, one in which physical security and information security, jointly and with cyber security promote the consolidated value proposal that outlines common objectives with a strategic vision and a culture focused on a secure, resilient, and successful company. Convergence does not provide a specific model, which demands a specific design from the organization in which physical security must make the first move

towards cyber security, and that is considering that physical security has developed the necessary skills to be heard. I truly believe that convergence constitutes a real solution, it is the correct path, even though it may take a while for the concept to become familiar within the corporate security.

Crisis management

Crisis management is one of the most interesting specialties for any type of company and for any field of security. There is abundant information available on the subject, which translates into diverse interpretations creating its own crisis. Taking into account that organizations may go through a variety of crises, it is necessary to define the concept of crisis in a manner that facilitates understanding and managing it. I have always thought that the simpler the explanation of concepts, the easier it will be to take them in and create processes for them. Thus, here I provide a simple description for the word: *Crisis is everything that exceeds our capacity to respond.*

Such definition makes the preparation phase to be extremely relevant because the definition is based on the capacity to respond. I have managed kidnaps, extortions, coup d'états, civil unrest, and natural disasters; so, regardless of how well prepared a company is, *every situation will be different thus making the case to easily surpass the company's capacity to respond*; frequently, it might result that way due to their plans not matching the situation, or because the decision-makers decided to respond according to their better understanding. Hence, the efficiency of crisis management is based on having the personnel or contacts that would facilitate the required answers according to the circumstances the crisis generates. Lacking response capacity would imply a loss of control, a critical point not only to tend the crisis but also to avoid further creating situations with larger repercussions or collateral effects. Let's think for a moment on the impact the loss of the CEO would have on the company, mainly if the organization is going through rough times; in cases like that, if the company is not prepared for the event the answers to avoid a crisis will not

be there. A bad or wrong response might trigger multiple negative situations; therefore, the faster the company is able to obtain solutions, the quicker the company will regain control over the situation. During a kidnap situation in Haiti where, even though it was a high impact situation, we were in control because we knew the conditions the kidnapped person was, negotiations to free the person were progressing correctly, and the communication with corporate helped us to keep top management calm. Two things happened, however, that turned the table around. First, the spouse of the kidnapped person contacted the CEO directly and demanded the process to speed up; and second, when we paid the ransom the perpetrators did not free the kidnapped person. From that moment on, the situation turned into a dual case which demanded immediate actions; this forced me to make a decision in response to the CEO's pressure who asked the top management team if we were doing enough. Such questionings have the characteristic of creating a whirlpool of doubts and suggestions about, and interference in the negotiation process. On the negotiation side, I had to accelerate the process asking the consultant to step aside because they could not handle the process on a fast track. Having the ability to define solutions I did not have before helped me avoid a double crises. It happens in many cases where a contingency is dealt with and all the answers run out, the crisis is approaching and new answers need to be generated; nonetheless, it might be the case that, even with the right options their inadequate application or a change in the original conditions may cause the process to run into collateral crises. Being this a high impact subject for most companies, it is clear that crisis management would be handled by several areas, depending on the situation and type of impact. I had an experience in a global organization where the area of institutional communications was in charge of multifunctional coordination, such setting privileged the company's image and brand to be top priority in face of any loss. On a different case, in the banking industry this leadership and coordination was, by policy and regulations, controllership's competence. Regardless of what the particular case might be, the relevant matter for corporate security is:

To become an integral part of the corporate teams to tend the different crisis phases and manage any new feasible crisis.

And, in situations that are security's direct responsibility, work with the other functions related to the subject in turn. From the crisis management perspective, these are the aspects I regard relevant for corporate security:

Loss criterion

This is the key point that will determine what the company will do on every one of the stages of crisis management. And it becomes more evident during the preparation phase because it requires investment and demands answers from the diverse functions involved, be that due to the crisis impacting on them directly, or because their participation is critical to avoid collateral crises. Likewise, the preparation phase needs the functions to develop a process that identifies the conditions that might lead to a crisis, and expects them to outline the actions necessary to avoid it and, when required, generate adequate answers (consultants).

Here is an example to illustrate the loss criteria. At a company where I worked as security director, the training programs regarding civil protection were of utmost importance because of the high risk of a fire in their business units; given the magnitude of the potential impact, which would include the loss of lives, sanctions from authorities, and sales lost, live fire control training was vital. During one of the exercises, several employees were hurt and it was necessary to take actions not only to tend the wounded, but also to look after their recovery and wellbeing. Oddly enough, the situation was handled well and it did not turn into a crisis; however, after the incident, a media problem arose as a consequence of human resources mismanaging the situation of one of the wounded employees to whom the company had promised compensation, but human resources said there was no compensation. The situation turned into a crisis due to

the unexpected outcome. This case was extraordinary and uncommon; the crisis management team looked for the answers quickly and efficiently. The underlying importance is that the company invested in the preparation phase to actually care for the real value of potential losses (human lives and operations) and, as a result, there never was a loss of lives during high impact situations (store fires). It is also common that companies decide not to invest in the preparation phase, postponing the creation of a solid prevention culture until a crisis arrives. This modality must be identified by corporate security because it becomes a much complex process and, usually, exhausting due to the counter culture flow effort it requires.

Actual importance

Regardless of the corporate structure, the nature of the crisis will determine the role of corporate security; hence, corporate security's importance will depend on the function's capacities and, at some point, external support might be necessary even with a robust security structure in place. The nature of the situation will also influence on the degree to which the crisis management plan is observed because, as the situation unfolds, top management is informed and the timings are fulfilled, there might be adjustments on searching for the answers or solutions accordingly. The number of training courses is irrelevant, what matters is the actual practice and expertise gained through the sessions. Indonesia and Algeria had me managing personnel evacuations during civil unrest situations; Mexico, Colombia, and Haiti required me to negotiate in kidnapping cases; The Philippines and Mexico got me managing natural disasters that caused contingencies and crises; I have controlled extortion cases in Colombia and Mexico; and served when there were fatalities involving employees in Egypt and Colombia. Many times the work was performed in person and other times, remotely. Similarly, I have participated in financial and operative crises supporting diverse functional areas while managing security in a bank; the same is applicable to logistic operations in the retail industry; as well as for trading operations in

the construction materials industry. In summary, there is no course or workshop that prepares you for the actual experience. Each situation, environment, and *modus operandi* are different and these make the difference on what information you would have to analyze to respond, not only to manage the event, but also to the way you would have to conduct the communication with top management and those involved in tending to the crisis. I have witnessed different reactions for each situation in which I have operated; additionally, I have worked with external consultants who dominate one type of crisis although they do not master all of them. Ultimately, as corporate security director, it is your responsibility to manage such diversity of situations.

As I mentioned from the beginning, there is a lot of information about crisis management but, the truth is, in any corporation this topic is not an exclusive subject for the security function. There are many entities with interests involved in managing situations that may take things beyond the company's response capacity and, in order for corporate security to play a relevant role, the function must establish itself with credibility and trust and aim to integrate the security function to this critical process. I have witnessed organizations that, even in situations related with the security function, hire external consultants to coordinate the search for responses. Many companies deal with the preparation phase frugally, and then when the crisis arrives they react not limiting the availability of resources which, in my opinion, is a negative culture for the company because in their employees' minds the idea will linger of the incident being avoided if dealt with it on time. At present times, the programs about crisis management and business continuity are overtaken by current situations and the companies are forced to escalate towards programs focused on the organization's resilience, where uncertainty demands complex answers and, sometimes, hard to obtain. The positioning of the corporate security director depends on the ability to integrate the function to these programs, all of which call for business proposals supported by strong experience in handling difficult situations (business driven).

1. Critical infrastructure: crisis management and business continuity

In order to make more sense of the above, next I will describe how is it possible that, while protecting critical infrastructure, all the detailed plans may change when facing a contingency or a crisis. There are multiple reasons that can cause a business continuity plan that has been validated and agreed upon, to fail and turn into a crisis:

- *Actual capability versus planned capability for critical programs*

The framework for critical infrastructure considers all physical or logic operations, service or process that, if interrupted or terminated, generates a severe impact on the continuity of daily life in a given community, affecting their economical, physical, and social welfare, as well as the capability of function and viability of their government. Essential services include, among others, health, transport, water, energy, public security, and banking services. Critical infrastructure compromise their social viability upon a grave impact; however, it must be stressed that critical infrastructure does not operate independently. You may have an excellent business continuity plan but what happens if logistic support to move yourself or if the food supply is lost? Or, simply, what if the business continuity staff prefers to reunite with their families instead of resuming operations? It is only when the business continuity plans or crisis management programs are executed in a real contingency or crisis, that their effectiveness can be confirmed. With the definition of crisis we stated above, being effective in a crisis situation requires that we succeed in not having our capacity to respond, surpassed; or, in other words, how fast can we respond efficiently. There might be a significant difference between the real capacities in comparison with the institutional or theoretical capacities the company considers it has regarding safeguarding.

I have developed and operated contingency plans and crisis management programs for over twenty years in diverse industries –cons-

truction materials, retail, banking, telecommunications, and tobacco and, recently, entertaining— and I can attest that the reality exceeds the scenarios projected in the plans and programs companies outline during their training workshops. By referring to scenarios, I not only speak about the time and space of the incident, I also include the roles performed by the many actors there are in those scenarios. Nature is the most extraordinary source of threats today. The Covid-19 pandemic turned out to be such a disruptive factor that the capacity to respond of the continuity plans of all kind of businesses was surpassed, as well as the capacity of authorities to react and support, and also the understanding capacity of society. The pandemic triggered other risk scenarios whose impacts are still being identified and measured. A sanitary crisis easily generates a political crisis, an economic crisis, and a social crisis. The qualitative losses caused by the pandemic will reflect on the human factor of all social structures. The aforementioned breaks paradigms and forces thorough revisions of basic criterion of planning; thus, the proposal to develop response capabilities will not only support the business continuity, but also strengthen the resilience of institutions and organizations. With regard to critical infrastructures, the questioning and breaking of old models should come not only from companies, but also from authorities in charge of the plan of national security, mapping scopes and resources these should provide under the most disruptive situations.

- *Real capability or virtual capability*

Perhaps you have heard the term “black swan” (Taleb, 2007), which is defined as “high impact events that are hard to predict”; or the term “gray rhino” (Wucker, 2016), that refers to “events that everybody sees approaching but no one wants to confront”. Such terms although accepted as valid, are actually poorly considered, which misleads the reasoning and criteria to sustain the intelligence to outline the risks and threats scenario; then, potential impacts are not correctly defined and measured. We prefer to rationalize every event or condition, searching for the most convenient solution, which

results in the creation of comfortable programs and platforms that allow us to comply with the organization's requirement. Actually, this is worse than having nothing implemented because responses based on a false sense of security may be fatal, both for the people involved and for the corporate resilience and credibility. Frequently, compliance with rules and regulations seems to be the goal, although it is achieved without real commitment or company culture behind it. There is a difference between making and believing, even if complying with the norms sets a true commitment that permeates through the organization culture. There are instances where compliance is observed, because legal costs associated to an incident are regarded more important than actually ensuring the capability to respond to a crisis. It is even worse when the whole plan is devised including guidelines that are easy to understand but do not considered its actual execution. I can refer to real life cases of institutional plans that were defined and approved, which were not put to action as planned; furthermore, the actions taken were implemented according to "the perception and reaction of the moment", where the information sources for answers and solutions were selected through an inefficient process instead of the thought-out predefined process. It is outstanding that during the pandemic, the sanitary crisis captured all the attention, while other risk elements that represented collateral crises were preferably left aside. I have evidence that many programs were there merely as part of a plan to comply with norms and regulations, and their premise was: "spend as little as possible in prevention and, if anything happens, then use all the required resources to solve it." Unfortunately, the intelligence process is contaminated when the corporate area leading the contingency and resilience plans, frequently with external consultants support, focuses on the descriptive part because it makes it obvious and easily understood so the rest of the organization buys-into the plans.

I believe that, because of costs and a true company culture or secure organization, in most instances any catastrophic event is considered as improbable; then, when defining the risks, we avoid analyzing sources of threats and focus only on risks we are able to solve

thus leaving other potential causes without consideration. We tend to identify those things with which we feel more comfortable, and for which the answers are readily available. For instance, the specter of the cybernetic menace becomes relevant given the technology platform supporting not only the essential services but the whole company. However, it is key to understand that not all risks in this regard are cybernetic. Focusing only on cybernetic risks as the main threats might easily get us trapped in a tunnel vision, which would lead us to ignore or minimize physical risks that might as well be catastrophic.

There are other threat factors that could have a greater and graver impacts of disastrous proportions, such are the risks generated by the human factor. I regard that as the main source of all threats for any organization, which makes the subject deserving a thorough process and multifunctional analysis; additionally, a self-examination company-wide program would identify causal links, trends, and modalities related to the human factor. The human ingredient is the threat factor that is uncomfortable to recognize. An example might provide a better picture, let's consider a continuity plan that includes evacuating personnel in case of a natural disaster –e.g., an earthquake, and we take for granted that, after evacuating the essential services staff, they would cheerfully proceed to another site where their help is needed to resume operations. However, we cannot rule out two possible circumstances: that there may not be means to transport them, or that the essential services staff are not willing to go due to the emotional impact of risking their lives and their families'. Oddly enough, the human resources area is the least willing to participate on analyzing the human factor as a threat source.

As mentioned, nature is another source of threats and their unpredictability confers them probable catastrophic magnitudes, even with the possibility of anticipating their occurrence and location. Floods, earthquakes, fires, storms, and hurricanes may all have different impact levels and categories, and even pose indirect impacts. As of today, pandemics and epidemics are part of present and future scenarios. We already had information about the possibility of a pandemic, and we maintained the response formats unchanged.

Sadly, the actual response capability to mitigate the impacts caused by the actual risks, were easily surpassed by the diverse threat sources that triggered them. Even with specific structures in place to support business continuity or manage the crises, these structures and plans are overtaken by reality. The “black swans” will be the trend, and the “gray rhinos” already wander around the office hallways of risks management areas and the other functional areas.

2. Considerations on crisis management

The structures of business continuity, nowadays, are based on identifying probable contingencies; nonetheless, the structures must be scaled-up to correspond to visions of impact and response that reach beyond resuming operations fast at the lowest feasible cost. It is necessary for the company to accept impact scenarios which contemplate the unthinkable, and aim towards resilience to make operations feasible in spite of the losses. Bear in mind that our business continuity plan may be surpassed and, as a consequence, a crisis might be triggered. We must be aware of the “black swan” because, current threat sources bring with them risks and impacts we do not want to acknowledge. Similarly, we must identify those in the organization who accept the “gray rhino”, because such acceptance promotes the denial of what we considered the company’s efficient response capacity –institutional capacity, which is usually documented in thick three-ring binders we display on training workshops and annual audits. This new vision brings critical structure security into existence as a result of thinking not only on obvious security, the one we control, but also on reviewing every stream that converges with our operation; moreover, we should not take for granted that all answers will be applied to the letter of the security manual. The true impact that results from a critical infrastructure failure is not currently measured and, consequently, will not be properly attended with the response capability in place today. As corporate security directors, it is vital to position the function within the organization so that the area is included in those critical processes. Business continuity programs

not always fall in the security realm, but they usually require security to take part in them; thus, we should participate to contribute with an integral vision that makes the plan complete and ensures the necessary actions are performed to resume operations. An executive business-like presentation must help us explain the significance of a bad business decision derived from a critical incident or crisis, a situation that could be better managed having corporate security collaborating in the business continuity team.

Special investigations

The control and investigation processes within a company are normally performed by areas like audit, internal control, and the legal department. In some organizations, the difference between audit and internal control is defined based on the amount of the possible loss; the reason for this being the report line of each area, usually the audit area reports to the CEO while internal control reports to comptrollership. These areas work in coordination with the legal department –either to manage the investigation efforts or to use legal resources, and protect the company in the likelihood of a crime or law violation, although it may not always be possible. Corporate security is normally not included in this type of investigations. In order for corporate security to participate in high-impact investigations, the company shall establish –as a norm or via a formal requirement, the specific scope of security’s involvement. Also, the company shall support the development of investigative capability hiring security professionals with appropriate criminalistics profiles. By saying that, we are not requiring the formation of a police department within the organization, but rather an area with investigative training and forensic vision whose contributions complement those from audit, internal control, and the legal department via special investigations. It is necessary to differentiate the high-impact investigations, such as frauds and trust abuse, from the operative investigations like theft of merchandise, products, and employees’ belongings; additionally, there are internal investigations about minor incidents as well. I have seen multi-func-

tional task forces that include security, but they do so only as a physical control area, a check point, without including them in the investigation process.

I have conducted hundreds of operative investigations, and it was as security executive director with a bank that I carried out high-impact investigations as responsible of special investigations; there, my investigation team included lawyers and criminologists. During this experience, we developed the ability to perform cyber-forensic investigations by bringing into the team elements with knowledge in technology and information systems; as a result, we gained access to information sources and financial processes turning corporate security investigations into a key element for the bank's investigations team, especially concerning money laundering and high-profile frauds. I regard operative investigations as relevant as well; although, high-impact investigations demand technical skills and abilities in addition to the company recognizing that corporate security has a higher ranking role. Corporate security frequently participates in business ethics committees, or takes part in receiving internal complaint calls; however, the scope of investigation efforts, whether operative or high-impact, shall be outlined by what has been described above. As corporate security director, you must define the width and breadth of the scope your function is able and appropriate to have within corporate investigation processes. Personally, I found it very useful to have the attorney at law studies in my academic background, as well as the public prosecutor's office experience to set the bases for credibility and trust in the investigations department.

The Model and Process of Intelligence

SECTION A. BACKGROUND: THE CONSTANT DISRUPTION

Probably, Covid-19 has been the most important and disruptive phenomenon for humankind during the present century. The pandemic has put to the test every single concept that had guided the strategies and plans of corporations, the national policies and strategies, the global economy, and the human nature. We have not yet begun to realize the true pandemic's impact, and what its direct and indirect effects will be on the world's future; so, the fact that prevails today and tomorrow worldwide is uncertainty. Today, companies of every size are been forced to test their leadership models, their internal control processes, their human capital and, above all, their resilience to modify their projections and approaches to the future.

The current premises under which corporate security has developed and outlined the risk scenarios, as well as the value proposals displayed on the board meetings, should include the ability to adjust to scenarios subject to constant uncertainty. These premises are based on maintaining an ongoing learning about the nature of the companies we work with, understanding their policies, norms, and procedures, their strategies and operations, as well as understanding how they assume and manage their losses and, most importantly, on

learning about their human factor and organizational culture. Premises vary and their changes mean new learning and, what we thought we already knew, must be learnt again; and doing so, we come to know the company's new nature, their people, their sense of leadership, the strength of their values, and their capability to adapt to change and uncertainty. These elements rule their strategies and operations; consequently, they are also the elements that generate their new vulnerabilities.

SECTION B. INTELLIGENCE OF CORPORATE SECURITY

The main objective of the intelligence process is to facilitate information that generates the necessary knowledge for decision making. However, when referring to intelligence of corporate security, we must consider the supporting platform on which the function develops and enables their value proposal for the corporation. This platform requires knowing and mastering the corporation's context in which their policies, norms, processes, and culture are developed. The intelligence procedural model may not vary, in an effort to build the risks agenda, the impact analysis, the value proposal, and the implementation plan of the chosen model. The breaking point, however, the backbone of the intelligence of corporate security, resides in understanding the inner change and the way the company holds and redefines their essential elements. And, by doing so, the organization generates resilience, determines their loss context, and sets their strategy and projections again as their business timings evolve. Among the critical elements is the human factor, since it definitively impacts on the organizational culture.

Given the current context, I consider there is hardly a business continuity model that has not been tested hard and, in many instances, vastly surpassed because the evolution we have seen on the disruptive trend has gone beyond the limits of any scenario; hence, the sanitary crisis has extended to the political context as well as to the economic and social contexts globally creating multiple disruptions. If we add

the conflict in Europe (Russia-Ukraine war, 2022) we obtain a continuous disruption and, as a consequence, a world of uncertainty. Corporate security models today demand a more assertive and executive vision, a vision that includes new tools to read, understand, and learn from the organization. These models require dynamism to maintain themselves aligned with the critical functions of the company, and to discern business scenarios and developing value proposals to anticipate and be ready to cope with ongoing changes. The intelligence of corporate security must focus on integrating their proposals to those of other functions, converging with them to achieve resilience and ensure processes that support operative aspects which evidently will require action; even though this may not be the most critical contribution from security, it may foster the function as a valuable team player. Operative intelligence must be separated from strategic intelligence, because the latter takes the function's conversation with top management executives to a higher level; and once there, the essential topics, stages, and security executive positioning should be discussed. In order to permeate security into the critical processes of the organization, the security executive profile should include skills and business knowledge. The intelligence model for corporate security must contribute to redefine the company's risks agenda; therefore, through analyzing the impact (loss), the value proposals might be prepared aiming to ensure critical processes and contribute to an efficient loss management. The risks approach and the actions taken to coexist with them require a change in the organization's culture; as a result, the concept of security must be a critical service for top management, for the other functions, and for each and every person in the company. In summary, security must be centered in handling uncertainty. The concept of a secure company entails a multi-functional effort which converges in a resilient organizational culture with re-learning abilities.

A new corporate framework

New environment

With a generalized uncertainty in the global business scenario, every corporation's top management team should review their objectives aiming at short-term and, probably, mid-term goals to re-assess their criticality elements, their risks agenda, and contemplate changes in strategic as well as operative topics such as:

- *Government*: trends, norms and regulations, politics, scope, capability, and gaps.
- *Society*: values, criterion, social extremes, generational breaches, and polarization.
- *Criminality*: scope, *modus operandi*, capabilities, and reality.
- *Media*: veracity, political trends, assertiveness, and networks.
- *Economy*: availability, cost, and trust.

The new environment we face today, enters in a cycle of changes surrounded by constant uncertainty which compels us to review each threat source, since the risks these may generate also change and so does their respective impact. In turn, the impact forces us to review the sense of loss in every organization to determine how to handle the loss and cope with it. The risks agenda of each company used to be created for scenarios with a certain degree of certainty. The aforementioned aspects, however, do not deplete the elements to consider when analyzing a risks agenda, and it is only through a multi-functional effort that a platform to support the decision making process can be obtained. Corporate security, sustained by its intelligence platform, must have the executive capability to maintain the internal communication that positions the function to be part of the organization's effort towards resilience. The intelligence platform must include a vision that complements or adds value to other functions' visions, while the corporation's risks agenda must be the governing piece of the joint corporate effort.

The Covid-19 pandemic has impacted all aspects of life, and human beings have been affected in our most basic elements of survivorship: the senses of being and doing. Other global disruptions like the yellow fever or the world wars have impacted the whole humanity in one way or another, and over a delayed span of time due to the world not being globalized yet; however, this pandemic has caused a brutal disruption on a global scale and, due to digital technology and communications, with immediate reach world-wide. The sense of loss has been global as well. Perhaps the loss of human lives has not been of the same nature and magnitude as the other disasters, but the impact of uncertainty with regard to one self's security has been devastating. Months of changes, of over information, of fear, and the new modalities of work are the evidence of each society and individual being affected differently; as a result, the human resilience capability is being tested. Hence, the human element of every country, society, organization, or corporation becomes decisive for each corresponding structure to regain a sense of security. Corporations, companies, and businesses must validate their key elements with regard to:

- Culture and internal governance
- Crime and offense criterion
- Loss management criteria
- Norms and policies
- Company timings
- Strategy and operations

One of the most relevant sources of threats for the organization, as we have stated, is the internal menace the human factor represents because –intentionally or by neglect, it may cause severe damages of high impact. Thus, at the time of re-assessing each source of threats, corporate security assessment should include the potential impacts of human factor on the organization, and do so in convergence with the other functions; furthermore, the assessment exercise should also

consider the changes the human factor might experience through time. This process implies the use of technology, e.g., behavior & data analytic tools, in order to understand and project those changes. Corporate security should focus in understanding and tending to the causes of any likely illicit or negligent act, for which joint proposals shall be prepared in conjunction with other functional areas aiming to prevent such events.

SECTION C. INTELLIGENCE MODEL FOR CORPORATE SECURITY

Several aspects need to be established in preparation for the model: *First*, corporate security must define its functional purpose, which is a description of the efforts the area would perform while serving the organization. *Second*, once the purpose is defined, a model would be necessary to structure their information platform with which to manage and coordinate efforts and actions. *Third*, the model should have the capability to adjust, to re-learn from the ongoing changes organizations encounter; in turn, forcing the integration of security with the company-wide effort directed to tend to the business critical elements. On top of that, those critical elements are likely to be affected by the wave of changes that might impact the corporation. Adjusting the model takes us to reassess the sources of threats, project new risks validating old ones; and, jointly with other functions, the assessment of probable impacts allows the pitching of new value proposals. This process conceives uncertainty as the core factor on which the short-term actions must be based, which then shall be measured to review the ones needed for the mid-term and, subsequently, the long-term. The value of corporate security's contribution lies in the efficiency of the model, which must support fundamental aspects: the assertiveness of the value proposal and its positioning regarding key functions, and the function's capability to participate in critical stages of the organization's operation and evolution. The contribution's value resides on maintaining a high-executive performance level that draws the organization's trust and credibility to the security function. Never before the efficiency and effectiveness of the corporations' capabilities had gone through

such a hard and long testing period, which requires a sustained multi-functional effort, convergent, and founded on solid organizational culture tending to the human factor supported by technology as the essential element to reinforce the company's resilience. Corporate security and their executive staff have the enormous challenge of being at par with the company's effort. We do the obvious, and provide the relevant.

Convergence of the intelligence model with the intelligence process

The foundation for efficient decision making consists of gathering, timely and accurately, information to generate assertive knowledge; in a corporation, all functions perform processes in search of information. The strength of corporate security not only resides in identifying the sources of threat and the risks that might impact operations, the strength is also in the director's capability to identify, understand, and master the internal elements that rule the organization's dynamics; as a result, the intelligence model should enable the corporate security director to successfully navigate through the organization's channels. There are many techniques and tools available in the intelligence world, nonetheless, corporate security requires an *ad hoc* model that serves the specific conditions and circumstances. The model must support the function to operate both as a function and as a specialty; ideally, a model that can be explained and operated following the hardest to find of all senses: the common sense.

The model of intelligence I have developed and implemented successfully over the last 30 years can be defined as:

A process for gathering information that develops knowledge, facilitating the outline of a value proposal validated by the company; the process' outcomes, besides positioning the function within the corporation, shall be measured according to the proposal's impact on decision-making processes followed when attending to threats or opportunities.

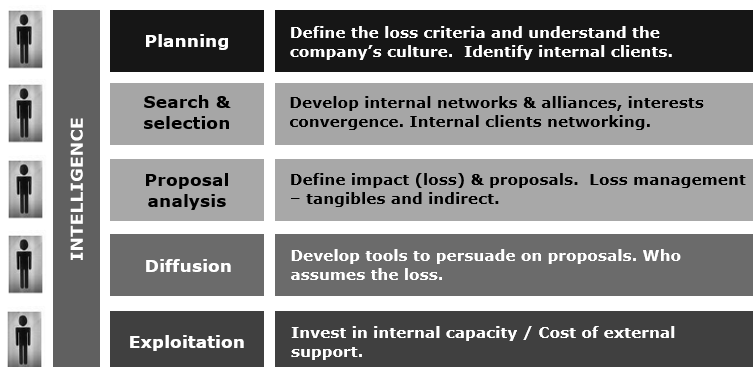
DESCRIPTIONS

- *Information and knowledge*: as commented, information is critical for decision making; however, to be successful the information must translate into knowledge allowing the communication process to adequately tend to and connect with the company's culture.
- *Value proposal*: is the integration of service and support validated by the company as the contribution from security and, according to this validation, confers the conversation with a corporate level. The higher the validation, the higher the conversation level (interaction/topics/timings).
- *Measurable success*: it is derived from the integration of the value proposal to the company's culture, processes, and policies, depending on the validation obtained. A successful outcome projects the function towards a more strategic objective: a secure company.

Structure of the intelligence model

The intelligence model for corporate security uses the same phases structure as the traditional intelligence process: planning, search and selection, analysis, diffusion, and exploitation (see Figure 1); such alignment provides for a logical order and facilitates the application of the 6G system presented in chapter 3 which includes: proactivity, control, communication, follow-up, validation, and alternatives; thus, maintaining the model's dynamic.

FIGURE 1. DIAGRAM AND PHASES OF THE INTELLIGENCE MODEL FOR CORPORATE SECURITY.



Each phase requires specific talents
(Knowledge and skills)

SECTION A. PROCESS OF INTELLIGENCE FOR CORPORATE SECURITY

The starting point of the model includes a series of critical questions—discussed below for each phase, and their answers should provide information and knowledge to the security executive with which to develop and present value proposals to serve the company's requirements; the success of the value proposals would leverage the positioning of the function. Each phase, as noted in Figure 1, requires specific talents where skills and business knowledge are fundamental, which makes operative experience at a strategic level no less important. The model's objective is to understand the company first, and then build communication bridges with the different actors within the organization; also, identify and understand the power and influence relationships that exist according to the nature and culture of the company and, above all else, understand the loss criteria and the manner in which it is managed in the organization. Comprehending this last element allowed me to efficiently align the value proposals, the communication mode within the organization, and provided the capability to position corporate security as a critical service and support in all the companies where I have managed and operated.

Phase 1. Planning

The planning phase guides us to respond some key questions presented further below that, in turn, shall help us understand the following aspects:

- The basic criterion for positioning the security function.
- The timings on which the company operates.
- The nature of the company.
- The culture of the company, which is key to connect with it.
- And, that the organizational culture guides the human factor behavior.

Why are these questions important? First of all, their value lies in allowing you to be proactive and establish the first controls your function needs. Secondly, they open up a communication process that builds bridges to connect your function with the other areas; consequently, an orderly follow-up would start with which, as the information flows and is verified, would generate additional alternatives. Such proactivity was explained in the 6G model in chapter 2. Moreover, this communication process and the assertive answers keep you and the security function aligned with the company's variables; so, the model that results from the questions and answers interaction would let you take on internal and external changes and, regardless of the company you are working with at the time, the responses you get would guide you through the new challenges you might encounter. In summary, the answers you obtain must define the direction your value proposal shall be aimed to.

Critical questions

- Foundations of the security function
 - Basic question: What was I hired for?

Particularly, to occupy an executive position. This answer might seem trivial, although it determines the first steps to take. I can assure that the reasons for my hiring by every company I have worked for, are different; consequently, the conditions and the initial positioning were different. The reasons may vary: to fill a new position that was created, to substitute an employee leaving the company, or because some special situation requires so, or even because some norm or regulation requires the position to exist. This question is vital and must be addressed during the job interview. Why are they interested in you and what do they expect from the function? This shall be your starting point.

- Basic question: To what functional area does security report to and what is the hierarchical level of that post with regard to the general director?

This questioning is foundational because there might be functions in any organization that are not friendly regarding security's good performance. For instance, it might be too complicated reporting to operations or human resources because security recommendations usually are either focused on vulnerabilities related to operative processes, or are situated within a cause-consequence process that is linked to human resources investigations about disobedience or any other human-related violation; both alternatives would have your direct supervisor to become judge and jury. In my opinion, it would be better to have security reporting to the legal area or the entity that enforces compliance with norms and regulations. The answers you gather should provide the scenario where your relationship with the new company begins, it will help you avoid false expectations, and will prepare you for a daily relationship that may result too complicated if the function is misplaced on the organizational structure.

- Loss criteria
 - Basic question: How does the company manage their losses?

To properly address this question requires an in-depth understanding of the company's culture. It is crucial to understand what the company regards and acknowledges as a loss, and how each function assumes their corresponding piece with regard to identifying and taking actions to manage the loss; as a result, you should also know how they define and activate the necessary elements to manage such loss. In every company, the functions tend to identify the probable causes of trouble (loss) which would make it mandatory to report the issue to top management and, justifying an omission or negligence would be critical. Such a situation might occur due to the operative results not meeting the expectations, or because the operation cost was negatively affected, or because a strategic asset loss occurred, or because operations in general were affected, or because a legal

problem arose due to negligence. There might even be a situation that affects the company's image; in which case, the economic loss might be manageable although the image loss would be hard to mitigate.

In some situations, I took for granted that the risks that could affect an asset or an operation were covered by an insurance policy; it turned out, the finance department did not manage that kind of policy due to the low probability of the incident to occur. Another case was the operations area that did not authorize the implementation of controls so that they could meet their quota, even by not complying with the norms and regulations; then, the legal department warned them about sanctions that might apply to the company. In another instance, human resources followed the advice of the legal department and, although there were no risks, they assigned special security to top executives; in this case, human resources acted to avoid the likelihood of any executive suing the company in case an incident happened. Understanding these criterion is fundamental for identifying what the actual impact is when developing the risks agenda and, also, the moment when the company should trigger or escalate the solutions to manage the loss. It is necessary to have a clear picture of the criterion each organization follows in order to know how each of their functions operate, and how they manage their risks and losses. Frequently, as it occurs in banking, security solutions are part of the norms and regulations thus making it easier for them to assume certain losses; hence, when investing in controls or in security, the question might be: Is it because there is a loss that forces the company to take actions? Similarly, in other industries with norms and regulations that require the implementation of civil protection-related actions, it is necessary to know when does the company actually acknowledges the losses they cannot assume. And also, how is the value assigned to those losses in order to adjust the necessary expense or investment? How much does the company spend or invest in security to manage a supposedly recognized risk? In retail, the loss is assumed as product wastage or shrinkage and, as long as the amount of wastage or shrinkage is within the projected parameters, the loss is accepted as something inherent to the business operation, they coexist with the loss; however, such practice might foster the hiding of the theft as if

it was wastage or shrinkage, instead of considering the incident as a fraud, violation, or malpractice. How should it be interpreted if, after a bank robbery, proper actions are not taken against the negligence of the executive responsible for the branch operation? In that case, should the loss be assumed as shrinkage? The format of the previous questions differs from the traditional context of loss prevention. I followed the traditional questions and setting during a number of years, although as I tried to better understand how the company works and what its culture is, I switched to the loss management criteria. The experience showed me it is the loss criteria what determines how the company defines the levels of control and, in turn, develops its security judgement. The company, then, might solve the incident and manage the loss, although not necessarily take actions to prevent the issue from happening again. Having norms and regulations that force the company to comply with security solutions does not imply the organization would go beyond the regulatory compliance. This is precisely what the security director must understand to prepare the proposals and develop diverse courses of action to illustrate potential losses and, consequently, have the company investing in security.

- Nature of operation
 - Basic question: How does the company actually operates?

This is a question that requires us to understand the company from within, comprehending its dynamics and the criticality of each of the processes and operations. You might know several things about the company, but really knowing the organization requires spending time with it as well as access to actual information about the real operation of the business. When you join a company, it is necessary to look for the appropriate information to focus your first interactions, especially if the job description, roles, and scope differ from how your area is perceived by others; thus, their perception would be reflected on the relationship they and their areas expect to have with you and your staff. I have come across situations where the areas that, even though they seem familiar with security, do not know

the roles and scope of this function. For instance, it might be obvious that the retail operation –and the inherent security, should be centered on their stores; however, once we identified that the logistic process was essential for the stores’ operation both, at the distribution centers and for the product transportation, we knew we had to deal with two area directors. Obviously, each director privileged their own operation so each functional area had their own idea about what to expect from security. Another example regards to the construction materials industry, there might be a variety of operation areas which include business units that include productive units, operative units, logistic units, and even exportation units; additionally, if the operation is global, then the company displays a particular nature within each country’s operation. The nationality of the organization –as per the country’s operation, and the directive team, entails a different character to each operative component of a global corporation and yet, they are the same. Once you understand the nature of the operation you may assess the weight of each function, which would be relevant when preparing and presenting your proposals. As you come to comprehend the diverse operations that conform the company, you will identify the internal clients with which you should connect and build basic alliances, such alliances would provide strength to the security function. By grasping the real nature of their operations, and through interactions with different executive levels within each operation, you would get answers to the question of what the company regards as a loss, and how it is managed.

- Business timings
 - Basic question: What is the current business situation for the company?

This essential question would provide you with information about the moment the company is when you join their ranks, and it is actually intended to be an ongoing question; that way, you would be aware of the circumstances prevailing in the business from the instant you arrive until the time of your departure. Every company is immersed in its own dynamic environment which changes con-

stantly; therefore, it is important to identify and understand what those changes bring along. There might be fusions, acquisitions, re-engineering processes, efficiency exercises, take-overs, operation closures, and change of owners and stockholders, among others; all of these situations have an impact on the organization's immediate future and, usually, it is not minor. So, if the security area is not prepared to cope with such changes, the impact might represent grave consequences like losing the long-sought function's positioning you have achieved. These operative and economic stages are "the timings the company lives", and all are key moments during which it is necessary to identify and anticipate, if possible, the consequences and implications they will present for the organization. For instance, changes in the stockholders might cause organizational rearrangements, modifying the company's culture, or a different approach to approved budgets usually to reduce expenses and costs. An acquisition might mean a headcount reduction, selling assets and even closure of operations. A fusion might not work and result in staff reduction or in organizational structure break-up. A re-engineering process or efficiency exercise would have similar outcomes which could reach the extreme of partial or complete operation closure and assets liquidation. A problematic financial situation, on the one hand, might have implications ranging from headcount reduction, to the operation termination and liquidation of assets, to organizational culture changes, to the company going out of business; on the other hand, a new general director might bring in a new business strategy, a new organizational culture, or new loss criterion. All of these critical business timings require understanding of the organization, possible consequences, as well as having the security function prepared and able to adapt. All the above highlight the importance of having business knowledge, good communication with the other functional areas, and operative experience to be able to read the company timings correctly; as a result, your value proposals would be in synch with the business timings. In summary, in order to *be* with the company, you must *know* the company.

- Organizational culture
 - Basic question: Who moves the company?

This question comprises all the previous questions, and that is so because the internal behavior –organizational culture, is what holds and strengthens the emotional intelligence (EQ) of the organization. From the moment you join the company, you must be exposed to processes and programs that set the human capital stability, which should make the workspace a great space to work at as well as a safe space. This is key because the main focus of security is centered on the human factor, since it is on this factor where the causality resides and also where the consequences are fed back. Company culture determines causality because it rules congruence by holding the company values, by walking the talking, by making transparent deals, and by being honest when applying consequences. An organization becomes secure through their executives and employees alike; that is why, internal and external security depend on a vision of a secure organization. After years of developing security solutions, putting plans and programs in action for different kinds of businesses, operations, and countries, it has been the organizational culture the compass that guided my understanding about those business decisions that ended up as security issues. It is mandatory to understand the reasons that cause the employees to generate vulnerabilities to controls and processes, and why, at times, a loss is tolerated as long as the profit justify it. These subjects are hard to acknowledge, although it is the company's nature which actually rules personnel's behavior and, as corporate security executive, you must understand and handle those criterion to find an efficient way to communicate with the organization, thus successfully pitch in your value proposal.

Considerations for the planning phase

Before identifying the sources of threats and pointing out the risks' impacts, it is crucial to really know and understand the company. Having a thorough insight about the company we should be able to

comprehend the criterion that guide the daily actions; while doing that, we should have established internal contacts, gathered basic information, and familiarized ourselves with the culture and loss criterion. I have seen that, working on the answers for the basic questions above not only helps the intelligence process to be more efficient, it also builds critical communication channels through which your value proposals would be positively validated. Asking the questions and obtaining appropriate answers to all of them, will build on the business knowledge and foster interpersonal capabilities, while developing relevant conversations with other functional areas.

Phase 2. Search and selection

Internal sources

The planning phase set a guiding path which shall entail identifying and creating information sources. Internal information sources are critical because they define the intention underlying in the information requirement; additionally, these sources might provide the most relevant details needed in the analysis phase. Consequently, a careful approach should be followed in order to learn and understand their means for communication; bear in mind that each function has its own voice, identity, and perception of its role and scope within the organization. Security is an area that, by definition, cares for all the other functions; therefore, here is an implicit symbiosis cycle that exists in positioning the security function: first, it depends on your ability to effectively connect with internal sources; then, they become your clients; and, finally, your fundamental allies. You must be aware that a big mistake is taking for granted that the other functions are, by default, willingly available and welcome security. The perception other areas have regarding security's role, scope, capabilities, and knowledge determines their openness as source, client, and ally. It is among the security executive challenges to achieve this communication flow so that, when performing the search and selection, valuable and necessary information is available.

Basic criteria of internal sources

Each functional area is like a mini-universe within the organization—which would be the big universe in this analogy; and, at the same time, the nature of the company defines the specific weight each function, or mini-universe, would have as a component within the big universe. The strength of security would depend of the relationships developed according to the critical factors that move each mini-universe and, ultimately, those that move the big universe as well. The intelligence network of choice is the one developed through internal sources and internal resources. The people in charge of daily operations in every functional area, at any hierarchical level, are the ones who actually know what impacts the company.

External sources

The information requirements determine the scope of the external sources we should aim to develop. Also, the threat sources and the risks impact would be fundamental to define the network; similarly, we must ensure the capability of the network to provide us with information that is both useful and reliable. There might be sources that not only supply information but also offer some support, mainly because information has a cost that needs to be justified for the company. The bottom line is: External information must add value to internal information.

Vendors

The creation of a network of external sources must apply a criteria that allows the search of external information to complement the internal information. Since most sources imply a cost, our network should be developed under a cost-benefit criteria. The cost might be direct when the information itself is offered as the product being purchased; or, as a result of the relationship with our company, the vendor provides us with information related to their service. Often-

times, we shall need to train our vendors so they become an information source according to what we need; we must be cautious, however, with those vendors that have intelligence products among their offerings, checking their search scope and analysis with which they operate and, above all, verifying their intelligence criteria and their information sources. Take into account that, whenever environment information is going to be presented, the sources must be documented so that the content proves to be supported and reliable; failing to do so, might be interpreted as an attempt to influence through uncertainty and fear.

Authorities

When connecting with authorities on behalf of the organization, there is always the possibility of over extending our reach and look for sources and contacts that are beyond the actual needs; in other words, we might tend to think that evidently those contacts are justified, nonetheless, we should be observant of an unspoken criteria about authority contacts –required intelligence. More frequently than not, we might focus on creating an authority contact base that cannot actually help us from the legal context where they operate. The information that comes from these sources, due to their timings and scope, might be useful for a broad and general overview; nonetheless, each organization requires detailed information to compete with executives of other companies that might possess more useful information. There might be specific situations that demand having such connections, for instance, solving a kidnap case, or an extortion, or any catastrophic situation; also, considering that many times, unknowingly, we might be the information source for the authorities.

Operators

Security executives of other organizations are essential elements in a search network, in which the industry, the operations' geographical zone, or links with interest groups are prime contributors of actual and

relevant information for the intelligence process. The experience in global operations demonstrated that affiliation to associations like the International Security Management Association (ISMA), provided access to security executives in companies that operate in zones from where I required information; the incident might be regarding a Due Diligence (DD), a Post-Merger Integration (PMI), or perhaps during extreme conditions like a coup d'état or terrorism. Likewise, but on a local scale, groups or business associations related to security might represent relevant information sources. It would be up to each security executive to develop these information sources to connect with the search options that best solve the need.

Considerations for the search and selection phase

The planning phase is mandatory to set the search and selection phase on track, because this is the phase where the internal networks are created which establish the need for information and, in turn, are the primary information sources. External sources are necessary to complement the internal information needs, because we must consider that all functional areas in the organization perform their own intelligence process and, our contribution should add value to their repository. We live in an information world with complex dynamics; which is why, defining information sources requires business knowledge and operative experience that helps identify, build, and maintain these networks.

Phase 3. Analysis

- Once the information is gathered through the search and selection phase, we are ready to perform the analysis; here, again, business knowledge and operative experience become valuable to analyze internal and external information, keeping in mind the answers from the basic questions presented at the beginning of the planning phase. A permanent reference to the function positioning must be present in the mind of the security execu-

tive, because the analysis should seek new opportunities to improve it. The analysis shall determine the next four elements:

- *Impact*: Based on the loss management criterion (impact), the analysis shall determine where the impact might be generated, how it can be generated, and which function(s) might be impacted. Other functions that might be active working on the loss simultaneously shall be identified as well.
- *Nature*: The analysis shall also identify the key elements that are considered by the organization for loss-related (impact) decision making. The larger the impact and incident exposure, the higher the hierarchical level involved in knowing about and acting to solve the issue. We must be prepared to answer, if asked, about which areas might intervene even if they were not impacted and, by doing so, we promote their interest in collaborating with the process.
- *Timings*: The timings become vital if the company is going through difficult financial stages, either legal or strategic, because knowing about the incident and probable loss might affect the company negatively on any of its strategic processes.
- *Culture*: We must identify how the company behaves when facing similar situations, and how does the company manages the loss; knowing that, therefore, would allow us to prepare a security value proposal and even define how the value proposal may coexist with the company culture, which would also contribute to integrate the role of security to the culture.

Considerations for the analysis phase

When performing analysis, comparing and referring to diverse contexts and benchmarks are crucial; that is why familiarity with the business environment as well as with the operations of the company is required. In any company, there are elements that must be known in order to be successful when analyzing the information; among such elements are the company culture and its timings, as well as the power ingredients that influence the decision making process.

The phase of analysis considers the scenarios where the company might be actually affected, and prompt the organization to validate in transparent and tangible ways the probable loss the company does not want to experience.

Phase 4. Diffusion

The importance of the diffusion phase resides in it being a communication resource supported by a tool or process; moreover, this phase shall convince the internal clients that the value proposal is focused on aspects that concern them. The persuasion process involved requires skills to use or manage the tool, and also business knowledge to achieve a successful validation of the value proposal. If the process has gone through the phases of planning, search and selection, and analysis accomplishing the expected results by answering the basic questions, building internal networks, and aligning the probable losses with the company's loss management criteria, you shall have the necessary arguments to support the proposal.

Developing an executive presentation requires abilities to structure and consolidate information, in ways that ensure the contents make sense according to the level of interaction expected with that particular audience; hence:

It is mandatory to develop executive presentations that support the what and the what for of the proposal; these are, precisely, the two points where the decision making process has an impact.

It is clear that the *how*, *when*, *who* and *how much* are also important; however, my experience had shown me that in the end the *what* and the *what for* (loss) will be the decisive pieces. Then, the products to develop in this phase might include:

- *Presentation and authorization*: the presentation must be prepared according to executive standards, outlining the conditions that

would provoke a loss; the approach should have the answers to the planning questions guiding the audience to welcome the value proposal when facing a potential loss. The executive presentation must adhere to the organization's interaction level in form and content, and be in total alignment with top management communication formats. Putting an executive presentation together requires communication skills and business knowledge; at the same time, the person conducting the presentation must generate credibility and trust in the audience. It is of utmost importance to stress that, at this point, we do not require a presentation about security topics, but rather an executive business presentation in which security's contributions add value to the business strategies, policies, processes, and operation.

- *Presentation and control*: while presenting the information, there are documents that convey the sense of control security holds with regard to what is being presented. These documents include maps or similar diagrams that display the risks agenda, the points where the loss might occur, the criterion for the risks levels, as well as the execution level of actions required to contain the validated loss. These diagrams facilitate keeping the functional actions under control, and monitor the current conditions that support the value proposal. These are dynamic intelligence documents that present the status of actions versus the risk levels, with regard to the loss being managed. The loss must have been previously validated, and the actions approved as well through the corresponding presentation and authorization document.

Considerations for the diffusion phase

The risk conditions, the loss impact, and the value proposals are presented in the diffusion phase, which is the phase where the decisions about the value proposals are made. This is also the phase where the decision maker must be persuaded to support the proposal; furthermore, the phase aims to consolidate information and interests of

functional areas that had already validated the document in the initial stages; and, by doing so, they endorsed the credibility and trust they developed on the service and support the security proposal would provide for them. The two security objectives that should be met in this phase are:

- *First:* Obtain the validation and approval of a value proposal that would also be considered as part of the relevant decision-making for the company.
- *Second:* Position the security function as a critical service for the organization.

The specific weight of this phase lies in getting the organization in action through the persuasion process started in the planning phase, where the objective of becoming a more secure company was stated. One of the biggest obstacles for corporate security is connecting internally using efficient formats and language; therefore, you must establish communication bridges to communicate effectively throughout the organization. Each and every phase of the intelligence model is important because the answers to the planning basic questions, together with an efficient search and selection process—in which security connects with the company actors, would help you build the necessary bridges to the other functional areas of the organization. And, while you construct those bridges through interactions with functional areas, you will develop the credibility and trust necessary to support the bridges.

Phase 5. Exploitation

This is the last phase of the intelligence model, the phase in which what is executed, as well as the form in which that is done, would derive from the successes achieved in structuring the preceding phases, being the diffusion phase the instance where the decision is made with regard to the value proposal. The exploitation level or execution of the authorized plan would be reflected on the execution of each

of the phases of the intelligence model. The complete utilization of the intelligence model comprises from the proposition of the strategy for the corporate security function, and the plans and processes this entails, all the way through the subsequent proposals resulting from the convergence and from the service to diverse actors.

When speaking about execution we refer to three scope levels, where each one of them represents a different aspect for corporate security. Next, I explain these levels according to the person that carries out the exploitation which, in turn, triggers the respective decision:

- *Internal employee:* As mentioned previously, the culture of a company is based on the fact that security emanates from the way its personnel behaves; as a result, when the employees operate and execute secure procedures and actions, the organization turns into a more secure company. Achieving this requires top management validation, so that becoming a more secure company has value for the business and, consequently, is endorsed by the CEO or the general director. Similarly, security proposals should have a business approach to which the corporate functions integrate their critical processes, as well as the diverse controls their personnel executes. There would be security solutions validated by each function which would include the security value proposal that was agreed upon previously. This is what high-impact exploitation looks like; hence, corporate security has reached a high capability to place value proposals supported with the positioning of credibility and trust. Everything that influences the company's culture or the company's high-impact processes shall scaffold security transcendence.
- *External support:* We discussed about external support when referring to personnel management in section B of chapter 2; thus, we should remember that in this regard there are three lines of action to choose from depending on what must be achieved:

- *Expert*: When the expert knowledge or skills required are not available within the company. This need must be detected in the analysis phase and the expert resource would be incorporated in the diffusion phase. Usually, this kind of support would be considered in high-impact situations for which the consulting firms offer specialized support, and that implies experience and capabilities of information and logistics.
- *Ratify*: When the subjects are too technical it might be necessary that top management, as well as corporate security, require the ratification of a specific highly specialized knowledge or procedure, thus someone with that niche expertise might be called to ensure the correct action is implemented.
- *Support*: There might be occasions when the execution times demand certain agility from the participating elements; hence, external specialists might collaborate with the security team in order to achieve the required timing.
- *Corporate security*: When the organization validates that corporate security personnel is able to influence other functions' processes, we are in a situation of relevant execution. This instance is valuable because it implies that security personnel is trained and capable in dealing with business-related events, which is a positive indicator. The more the organization requires that corporate security develops business knowledge and skills, the better positioning the function achieves. There are punctual matters, however, that clearly pertain to security and, aside from those, relevant issues related to the company culture and processes contribute to project security as a business function.

Considerations for the exploitation phase

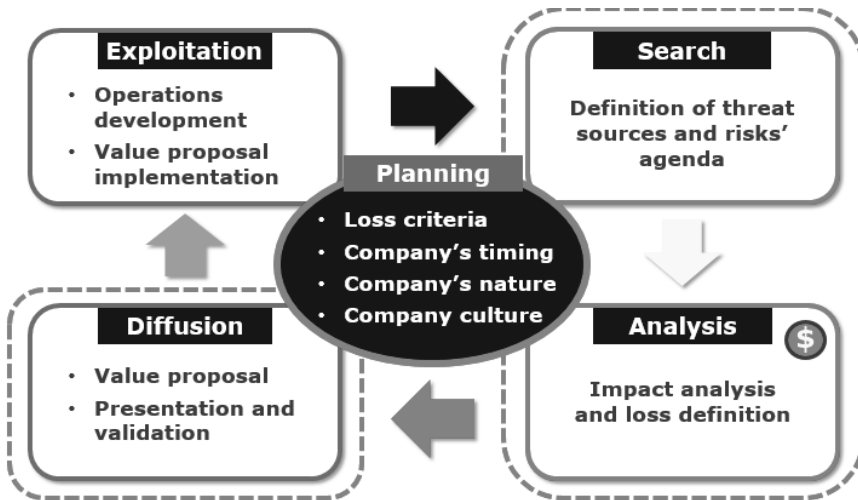
The exploitation phase highlights the scope of the value proposal presented in the diffusion phase, because the decision making might

require the use of some budget. Even though corporate security focuses on searching and proposing low-cost high-impact measures, the monetary aspect is still relevant especially when the company timings are complicated. For this reason, it is vital for security solutions to be multi-functional, whenever possible, thus having more than one functional area integrated to support the value proposal. We must be careful not to confuse norms and regulations that infer a budget and are considered security solutions when, in reality, they are part of the operative cost. For instance, the monitoring system in the bank's branches are regarded as mandatory and sanctioned by banking regulations, even though they are operated by security personnel. Exploitation derives from diffusion, where the company validates the potential loss and authorizes the proposed solutions. Corporate security must clearly mark where the proposals would be implemented, and where security would manage and operate the norms and regulations-related aspects the company must comply with.

Integration of the corporate security model and process

Once the model of intelligence for corporate security has been formulated, we may see now that the model integrates automatically with the security traditional process. The diagram in Figure 3 illustrates their flow and integration.

FIGURE 3. INTEGRATED MODEL AND PROCESS OF INTELLIGENCE.



EXPLANATION OF THE PHASES AND THEIR EFFICIENCY

Planning is the phase where the company's critical information elements are determined and, with those identified, required knowledge is available so that the intelligence process allows:

- To develop the basis upon which to establish internal clients and alliances to consolidate a secure company criteria.
- To identify and develop key contacts and sources of information.
- To identify the company's loss criteria, and how the criteria is managed by each functional area.
- To identify the business timings, and align the security function with them.
- To understand the company's nature and its timings to accelerate the learning curve.
- To connect with the company's culture to get security aligned with the corporate EQ.

The efficiency of the planning phase resides on building strategic communication bridges within the company; such bridges would facilitate acquiring the knowledge needed by the security function to create value proposals for the business.

Search and selection is the phase that marks the moment to identify the key sources of information both, internal and external, and establishes links with them so that real knowledge about critical elements becomes available; this phase of the intelligence process, then, allows:

- To ensure the information platform with internal and external actors.
- To determine the threat sources.
- To identify internal and external risks.

- To determine the impact, regarding which the assertive information comes from the actual knowledge obtained through the planning phase.
- To develop the corporate risks agenda.

The efficiency of the search and selection phase resides in developing the risks agenda, which should also include as key element the definition of the loss validated by internal sources.

Analysis is the phase during which actual information is obtained about key actors, timings, and nature and culture of the company. Based on that information and knowing the company's loss criteria, this phase of the intelligence process allows:

- To consolidate the risks agenda, aligning threat sources and risks with a streamlined loss criteria according to the impact the loss represents to the different actors.
- To identify interrelationships among critical elements according to the loss criteria.
- To structure all the elements considered in the analysis phase to develop the value proposal.

The efficiency of the analysis phase is based in procuring critical information that have an impact on the internal actors' spirit, and this information would constitute the knowledge base for the company's decision making process with regard to security issues.

Diffusion is the phase where the company's communication and culture criterion are identified; subsequently, the required bridges are built to reach those actors who have key roles in the functional decision making processes of the business. Hence, the intelligence process allows:

- To define the appropriate tool to persuade the decision-making targets.
- To develop the executive presentation according to the type and level of audience.
- To develop the follow-up process with other key actors in the decision making process, starting from the main executive presentation and customizing the content according to subsequent audiences.

The efficiency of the diffusion phase is the capability to persuade the audience to validate the value proposal, and the success would be in the impact the proposal has on the decision making process; therefore, the more strategic the content of the proposal, the greater its relevance. The diffusion phase consolidates the credibility and trust built throughout the phases of the model and process of intelligence.

Exploitation is the phase where the capabilities and vulnerabilities of internal and external resources are identified and validated; thus, knowing what resources are available for the company to implement and operate the proposals. Based on a successful proposal, the intelligence process allows:

- To develop and implement the necessary process to integrate the proposed elements in policies, norms and regulations, controls, and processes where the proposal is aimed and in alignment with key actors.
- To develop the process of selection, hiring, and administration of external support.
- To develop, jointly with key actors, the training process for the executive corporate security personnel.
- To develop the follow-up and validation process to monitor and assess the implementation effectiveness, ensuring the intelligence cycle continues as described in Figure 3.

The efficiency of the exploitation phase resides on the implementation of the proposal serving the capabilities and vulnerabilities pertaining the available resources; consequently, through these resources, the efficiency of actions would be validated, new alternatives would be proposed, and the dynamic of the intelligence process would be maintained sourcing information needed to feedback the planning phase and restart the cycle.

CONSIDERATIONS ABOUT THE INTEGRATION OF THE INTELLIGENCE MODEL AND THE PROCESS

Integrating the model and the process of intelligence consolidates all the elements, knowledge, and experiences gathered and put into action for the corporate security structure to comply the objective: *safeguard lives, maintain business operations, and protect company's assets*. This integration, however, also comprises *developing the security function* just like any other function in the organization, aiming to be recognized with dignity based on credibility, trust, and respect being positioned as a critical service within the corporation. As discussed throughout the book, each element contained in the model and in the process requires vast business knowledge and professional experience; therefore, these two goals constitute the tools and the guide for the corporate security executive to develop a high-level professional profile, which would enable the security professional to escalate the organizational ladder of the corporate security structure.

Rajectory, real life cases, and lessons learned

SECTION A. RECRUITING & HIRING, HEADHUNTERS, AND HUMAN RESOURCES

Usually, the manner in which we were hired by a company for a security executive post is not shared. Nonetheless, this might be interesting if we pay attention to the reasons and procedures each company uses; especially when the career path takes you from a managerial position to an executive level. That is why, with eight hiring counts on my back –three of them with the same organization, I would like to share some of the lessons learned. Following are the eight cases in chronological order.

Case 1. Construction Materials Company

I referred to this case earlier and now I will give more details about the experience. I joined the company as the security manager during the time when they had started a global expansion plan. An international consulting firm was supporting them in the expansion project, and they recommended the creation of an information security area that would converge with the physical security area –my new area, which happened to be new for the company as well. So, my post resulted from a consultant’s recommendation which explains why

the company did not have identified the need for the position; thus, there was no job description nor profile, no roles and no scope, not even a name for the job. That said, I was welcomed to be the first security manager for global operations; in fact, my boss, who was the security director, had no experience in security because all his previous responsibilities had been in administrative areas. The learning process resembled embarking in uncharted waters; the immersion included the creation of strategy, structure, plans, and programs for a company –which was already operating successfully at the time, in the process of becoming a global player and all was completed in three stages. There was no headhunter or human resources employee involved in my recruiting. While I was still in the Mexican armed forces, I sent out my resume to several employers, and this opportunity came up through a good friend of mine who, at the time, held an executive position with the organization.

Case 2. Tobacco Company

I was still employed with the former company, when a tobacco company that was in the middle of the process of being acquired by a global organization contacted me. The acquiring party had stipulated that they required a security professional according to a certain profile, and who was able to fulfill a post description that corresponded to their global criteria; the selected candidate would be the first security manager for the new company. The leader of the search effort was my new boss and, since I matched the position's requirements, they hired me. Once among their ranks my boss, being honest, told me that actually they did not need me because he and his team could handle their security needs; although, being that a corporate requisite, they had to comply. My access to the company was simpler due to an efficient corporate security area already in place, which gave me enough flexibility to operate; all I was required to observe, though, was a set of clear and simple key performance indicators (KPI). The learning process was as smooth as swimming in the pool. However, companies evolve and the scenario under

which they hired me radically changed because, six months after later, the operating units shrank dramatically; as a result, the organization got rid of most of the units and only one factory remained which, obviously, did not justify the profile of my position. Similarly, the security manager of the company, operating in another country, had to leave because the profile of the function exceeded the new requirements. This time, there was no headhunter either but I was contacted by the talent manager from the human resources of another company.

Case 3. Construction Materials Company

While at the tobacco company, I received a phone call from the construction materials company where I had worked before. As I said, I went through three different stages with this organization, and this was going to be the second. They contacted me because the former security director left the company and the new director—who developed the plans and programs for the global operation, required someone to fill the position I had left. I was gone from the company only for a year and, when I got back, I returned to the same office where I worked before and found my file and some souvenirs still in place. This was the beginning of one of the most interesting stages of my career, I was rejoining a company I already knew that continued its frank expansion, and it was becoming globally recognized. Previous positive outcomes, efficient networking, and a little bit of luck helped me land this opportunity. No human resources this time nor headhunter either.

Case 4. Telecommunications Company

During a due diligence in Europe with the construction materials company, a director of security operations in London, UK, contacted me. Their telecommunications company was in a fusion process with another company and the companies involved were one German and one Finnish. The companies were joining their operations and

required a security director for Latin America. The opportunity got my attention because the business would be a new experience, besides being my first role as a security director. I took the job and was able to create everything from scratch, just like the other two companies before this one. Although, again, organizations go through tough adjustments and, this time was not the exception, the operative and administrative conditions became very complicated. Shortly after, the fusion did not work and one of the companies bought the other one out. No intervention from human resources or headhunter this time either.

Case 5. Retail Company

Before I joined the telecommunications company, I had an interview with one of the largest retail companies in Mexico, whose operations director got in contact with me after my cycle with the first organization finished (Case 1). They hired me to be the first security and loss prevention director and, even though it felt like plunging in the ocean without knowing how to swim, this has been one of the best experiences in my professional life. Retail operation is extremely complex, and this company was going through a process of being acquired by a much larger player. I had to experience, in contrast with former cases, a different learning curve; the difference being, according to my new colleagues of other areas, that in order for me to familiarize myself with the retail business, I would have to spend at least five years to consider that I know the business. For my next challenge, no headhunter and no human resources either.

Case 6. Construction Materials Company

And here I go again back to the construction materials company, this time it was due to the retirement of the security director, my former boss, and they invited me to take over the position of global security director. I was really interested because, even though I was in charge of

the global operation before, I was so as a manager and now it would be as director. It was spectacular! I managed the security operation using the same programs I had developed and implemented throughout my previous stages with the corporation and, their time was up when the next company looked for me. There was no human resources but, this time, a headhunter did intervene.

Case 7. Banking Services Company

The headhunter and I had several conversations during an extended period of time. It was my first experience with a headhunter and it was interesting, you do not get the sense of interest the hiring company might have in your candidacy. It is a complicated and uncertain relationship. The process took long enough that, it was during these interactions, when I developed the set of basic questions you should ask yourself when a company is about to hire you –see chapter 4, section A. Then, at last, after several interviews I was hired as executive security and special investigations director, beginning a sensational professional experience.

Case 8. Entertainment Company

Another headhunter contacted me while I was still working with the banking company and, again, I went through conversations for a long period of time until I finally joined the company where I work while I write this book. The content for this paragraph is keeping me busy and is still work in progress.

Each one of us would have our own history and anecdotes; however, I truly believe that only the corporate security area might have as many variables as the corporations decide to furnish on the organizational structure. As I said at the beginning, it depends on every professional to develop a career, striving to achieve the best positioning with dignity being recognized through value proposals and, along the way, create a space for the teams with whom we work.

SECTION B. LESSONS LEARNED

- When a company hires you, it is critical to understand the company's criterion upon which they decided to have or create a corporate security function. The initial need might vary and, it would be supported by those criterion, that you would start developing your value proposal. Refer to the basic questions in chapter 4, section A.
- The security executive position is a highly specialized position, mainly for top management posts; for this reason, human resources and headhunters alike have a hard time figuring out the value proposal of such executive for the company. The value offering in the labor market for corporate security is diverse, and there is actually no clarity about the true profile for the security professional. Hiring a security professional with former experience in the public security sector, would make it necessary for the newly hired to adjust the available capabilities to the corporate environment, and acquire business knowledge fast; while, for the candidate that comes from the corporate world, the challenge in the learning curve would be to understand the new company. It is of utmost importance that you, once hired, work with human resources in structuring the real profile of your position and the elements for assessment; otherwise, it is very likely that you end up being evaluated according to a different post.
- Personally, I consider changing companies to be beneficial for the security professional because, with every organization, you would be exposed to new conditions and variables. This will force you to develop the executive-kind of profile and gain experience in assimilating the corporate criterion of every company; besides, you should become a business-savvy executive according to the nature of the company in turn, so that you devise how to apply the security specialties —e.g., crisis management, security of individuals, special investigations, etc., to the specific business context. I understand and respect the per-

son who decides to build a career in one company, as long as they follow a sustained evolving path for the executive and their security team. It is imperative to avoid being trapped in a comfort zone that blocks the growth of the security team and their leader.

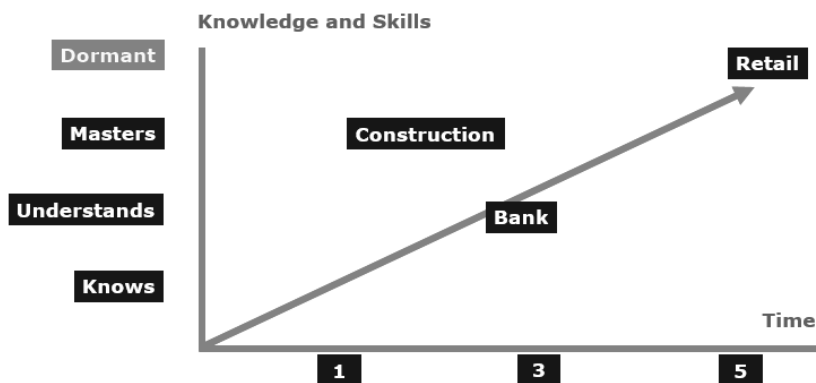
- Even the most reliable corporations go through strong changes according to the conditions prevailing in the business environment. During 28 years of corporate working life, I have journeyed through most of the existing corporate processes: fusions, efficiency exercises, re-engineering processes, acquisitions, etc., so you should also be prepared to face such changes. If you understand how the company moves while navigating the waters, you shall be able to get ready and adjust your plans to achieve resilience with your team.
- Every switch of employer requires a learning process and that takes time. Regardless of how much operative experience you have, it is always necessary to go through a learning curve; that said, this process helps you identify the knowledge and abilities you must acquire. And, once you obtain those, you shall become a business specialist in the organization where you currently work. Knowing the right questions to ask might make the learning process shorter, or might enable you to start making valuable contributions to the company sooner, or both. The intelligence model for corporate security has been the platform with which I achieved positive results regarding company changes, accelerated the learning curve, and adjusted the value proposal; therefore, together with my teams, we have always reached the goal of positioning the corporate security successfully.

Considerations about the learning curve

With regards to the learning curve illustrated in Figure 4, after three years with the construction materials company –remember it was expanding, we reached the most developed stage because corporate

security was successfully included in the executive teams participating in the global expansion process. Retail required five years to reach the mastering level of knowledge for the corporate security specialty in that industry. The model of intelligence –see chapter 3, allows you to shorten the time necessary to familiarize yourself with new surroundings and conditions, so that you may begin to pitch in your value proposals at operative level sooner than expected. According to popular wisdom, the executive “honey moon” period lasts only three months; so, if you are able to come up with value proposals during that part of the journey, that is a good omen for the future of that marriage.

FIGURE 4. PHASES OF KNOWLEDGE AND SKILLS ON A LEARNING CURVE.



On the vertical axis of the learning curve, we have the *knowledge and skills* levels starting with *knowing* the basics, then *understanding* how the basic things and also how the not-so-basic things work; after that, you continue learning to *master* the knowledge and you should be aware of not reaching the dangerous zone of the *dormant* knowledge, where you stop learning. And, on the horizontal axis, regarding *time* I resort to the time references the companies use: *short-term* (1), *mid-term* (3), and *long-term* (5).

SECTION C. SOCIAL UNREST (VIOLENCE)

Case: Indonesia – Social violence

During a due diligence process in Indonesia with two executive work teams deployed to two different locations, difficulties arose in several parts of the country which triggered civil unrest. The incident caused a generalized exodus of thousands of foreign visitors and residents, while the armed forces struggled to bring things back under control. Before the violent incidents started to occur, 48 hours earlier, I was attending a social gathering when I received a report from a team member in Jakarta who was assigned to a group of executives. The report indicated that the situation in Jakarta and the rest of the country was getting worse, and that barricades were being set at the main international hotels to protect the access to those venues; also, military vehicles started to patrol the streets.

Immediately, I got in contact with colleagues in other companies that had operations in Indonesia and with the embassies, which recommended to evacuate the non-essential personnel because they considered the situation to be compromising, and about to get out of control. Taking their advice into good consideration and with the field report from the security team, we contacted one of the executive directors in the team to inform them that the recommended action was to evacuate. The director replied that they will not evacuate, and he stated his decision was that the whole team would remain in Indonesia. During the call he said that the importance of showing commitment to the potential business partner and to the country supported his decision; furthermore, he elaborated adding he had the situation under control because he made arrangements to have an aircraft available in case they needed it. The violence was evident to all population. Phone calls came in from colleagues in the work teams in Indonesia, asking me to evacuate them leaving the valiant director behind. They had to be moved out of Indonesia.

Things were getting more complicated by the hour, there were tanks and armored units on the main streets. I was informed about the

death of two British tourists which occurred en route to the airport. My main concern was that the martial law would come into effect, which would cause the airport to be blocked, and there would be no more flights allowed to evacuate the country. In that case, I asked my security executive on site to speak with the other director, and explain them the situation since two embassies and some companies were already evacuating; if the executive director declined, my security element would summon all the security work team in the hotel to take shelter there, and wait until what had to happen actually happen. The second executive director immediately accepted our recommendation and asked us to get their departure protocol ready. Then, I contacted the first executive director and told him about the other director's decision; I also asked him for the pilot contact information and the aircraft data, that is when I found out that the pilot –worried about his life and his crew's, had already left the country. After three phone calls, I got seats on a flight with an international consulting firm whose plane would be flying into Jakarta from Australia. While the plane was in transit, we moved the group to the airport with the help of experts who protected them during transportation. Evacuation was complete on the same day, 24 hours before violence got to the extreme that the incident was referred to by some as “the Chinese hunt”, due to the violence that was used against people of that citizenship. Past midnight in Mexico, I received a call from Singapore; it was the second executive director thanking me for the evacuation maneuver, on behalf of all the executive members of the due diligence team.

Lessons learned

- It is necessary to consider that in high-risk situations there will be diverse kind of reactions from the different actors involved. Authorities, companies, and society in general, all operate differently when they are in complete control; thus, those who could have helped might be restricting and sanctioning your actions. Operative experience is of utmost importance to

manage complex situations like the ones described above; above all, it is vital to have an intelligence platform with reliable information sources and contacts that allow you to manage the case, particularly when there is no infrastructure at hand on the emergency site.

- It is important to know that, during security contingency situations, there will always be a reckless element who knows about everything, who knows an expert and feels wise enough to question your proposals or formulate their own, not only at the emergency site but also at corporate headquarters; which is why, only gathering evidence and framing the responsibilities on the consequences of decisions made, you shall be able to limit their influence.
- An efficient intelligence platform, including contacts for high-risk situations, should have at least three connections or supports. It is a fact that when a situation detonates, you may lose all the support you thought would be available. I witnessed evacuations in which the support provider was carrying out personnel according to the size of the client. Another example for real is that your contact with the authorities, the one you trusted the most, on the moment of the crisis got assigned to a different operation; thus, you had to resort to the second or even third level of contact and support and manage the implications of it.

Case: Algeria – Social unrest

While working with the construction materials company, one of the most important business operations was international trading; hence, the company had trading executives all over the world operating independently. One night, I got a phone call from the trading director asking for support because one of their executives was stuck in Algiers, capital city of Algeria, where social conditions were heating up and the executive could not leave the country. I contacted the executive immediately who was alright in his hotel; however, there

was too much violence on the streets, so obviously he was too afraid of getting out of the hotel to go to the airport. I asked him to remain in the hotel while I searched for support to get him out of the country.

The conditions were already difficult and, due to not having that kind of situation in the radar for the intelligence team. I started searching for support immediately contacting international security consulting companies; however, it was too complicated because they had their resources already assigned. In the end, even though it was very difficult, we were able to obtain protection for the executive during the transportation to the airport, they also escorted him to board the plane, and made sure the flight departed from Algiers. The operation was successfully carried out, and the executive flew to Morocco since that was the only available flight we were able to book for him.

Lessons learned:

- There will always be unplanned situations; nonetheless, the response capability will appear based on the efficiency of an intelligence platform equipped with the necessary contacts and support resources.
- Also, there would be situations in which, in spite of having the contacts and the support, the priority to obtain their response would be affected by colliding demands of the vendors' clients who are all facing the same emergency incident.
- During this kind of situations, the credibility and trust of the corporate security area is put to the test. Perhaps there may not be many instances of this sort but failing in just one of them would be catastrophic.

Case: Thailand – Coup d'état

- After one year of political violence, the Thailand army staged a coup d'état and took control of the country. Our operation in Thailand was small but there were executives and employees

to protect. The key question was making the decision of executing or not the evacuation closing operations temporarily while the situation calm down. We contacted the intelligence base in Thailand and set as a reference indicator the actions taken by the embassies and foreign companies; monitoring them, especially the embassies, provided us with reliable feedback because they are always the first ones to set the evacuation in motion. The director of the company's operation was calm, and agreed to follow the recommendation from the security team. Fortunately, the coup was executed without violence and our recommendation was to remain in the country, maintaining the business in operation.

Lessons learned:

- It is important to identify the different criterion the embassies of other countries might have in the country where your operation is; nonetheless, there may be relevant discrepancies among them. Some embassies prefer to protect their nationals from certain level of insecurity on, while other embassies prefer to wait for later moments of clarity to make their decision.
- When your operation in the foreign country is already established, it might be easier to decide what actions to implement because you and your team know the country and the intelligence base is mature. Furthermore, a relationship with the operation's directors that is based on trust is fundamental to act with assertiveness; usually, top executives possess an in-depth knowledge of the environment where they operate.
- Developing relationships with the country's government officials becomes very useful in these situations, depending on what might be possible to ask from them –information, support, etc.; however, when the situation is too critical these contacts might turn elusive.

SECTION D. KIDNAPPINGS AND LOST PERSONS

Case: Port-Au-Prince, Haiti – Kidnapping

During a business trip I received a call notifying me about the probable kidnap of an international consultant in Haiti; as a result, I changed my itinerary on the fly, literally, and reroute towards Port-au-Prince to attend the negotiations with the support of a consultant from a highly recognized international company. Even though our organization had an excellent security program for expatriates; as a result, the operation's manager had an armored car and driver assigned for his protection. On the day of the kidnap, the consultant was about to leave the country and asked the manager to lend him the armored car with the driver. For some reason, the operation's manager refused the consultant the car which made the consultant follow different security measures and, on his way to the plant, he was randomly kidnapped by a group of criminals.

The abducted consultant was the husband of an assistant in our company who had contact with the CEO; thus, upon learning about the incident she contacted the general director. Consequently, the pressure came not just from corporate but was received directly from the top; and, it was not only the CEO asking about the case progress, but also other executives who report to the CEO, and wanted to show concern and appear proactive. They surely provided us with some brilliant advices. Security conditions in Port-au-Prince, especially in Cité Soleil, were terrible to the extent that only the UNO forces were allowed to enter the zone.

Negotiation process

The language was a key barrier (Haitian Creole), thus a prestigious security consulting company was contracted, which in turn relied upon the services of a local consultant. The conversations began and the local consultant started with an aggressive tone –constantly insulting the kidnappers, arguing that it was the way negotiations were

handled in Haiti. It felt like I was somewhat kidnapped in my hotel for a week, awaiting daily for the criminals to call since five in the morning –they said they would call at that hour although they did not. Finally, the call came in and the deal was done. The ransom was prepared and delivered according to their instructions. The night passed, and the victim was not freed; the criminals said they found out about our company, and they increased the ransom amount. During the negotiation process we received a call from the victim, he informed us that he was alone in a house, calling from a cellphone they left there. The door was unlocked but he was afraid of running away, so he preferred to wait for the negotiation to finish; however, he also told us he was very upset because we did not pay the ransom. These were the conditions we were facing, and the consultant's wife became more insistent in her calls to the CEO who, in turn, asked a director to urge me to progress on the rescue. Then, it happened that the plant manager contacted me and said he could help us free the kidnapped person. He explained that he knew the perpetrators, they were his nephews and he could talk to them; although –repeating the criminals' last phrase, the cost would be higher because now they had identified the company. I reported the news to my boss who told me the negotiation was my responsibility; up to that point, I decided to pay the additional sum and the kidnapped person was returned to us the next day.

Case: Bogota, Colombia – Kidnapping

The company had started operations in Colombia recently, hence our security intelligence at the time was still a little blurred. We had gathered information from several embassies, including the Mexican embassy, and each one of them provided us with a different version about how to handle the diverse risks that might have an impact on the company, and kidnapping was among them. We still had uncertainty to solve when an abduction incident occurred; nonetheless, the victim was not an executive or a foreign person but an employee of the sales division. We had no experience on handling a situation like

that, so we contracted an international security consulting company to support us on the negotiation process.

Negotiation process

The negotiation process was complicated due to several reasons; the first one being that the consultant assigned to the case did not speak Spanish, which required me to translate back and forth between the consultant and the team. The second reason was that the consultant did not know the country nor the *modus operandi* of kidnapping in Colombia. The third reason was that, due to their inadequate handling of previous abductions, the consulting firm was legally banned to operate in the country. All that said obstructed the attention the case required on a daily basis; thus, we ended up contracting an independent negotiator who –having gone through the experience of been kidnapped, was really good and with his help, the ransom was finally determined. Next, we had to deal with the payment procedure which resulted extremely complex. The law in Colombia prohibits paying ransoms, especially in the case of a foreign company. As things evolved, a priest offered his help to deliver the payment and we went ahead with this option; although, we made him aware that he would have to climb uphill to arrive at the location to make the payment. While the priest was waiting for the public transport, some soldiers saw the priest and offered him a ride telling him they were bound in the same direction. The priest could not refuse and climbed onto the military vehicle carrying with him a briefcase full of money. Minutes later, he continued his journey on foot and completed the mission. The victim was freed two days later, unharmed. The company was never exposed during the negotiation, and the consultant charged more than the ransom amount the company had paid to rescue him. After enjoying good food and being nicely treated, the consultant concluded there was not much he could do to help; so, he gave us his cellphone number for us to contact him ... in case we had any doubts!

Case: Monterrey, Mexico – Kidnapping

There was a time during which the state of Nuevo Leon, particularly Monterrey, experienced an outbreak of express kidnappings. These crimes occurred as follows: the perpetrators would abduct a person randomly, usually on a Friday evening, and contacted the family that night; they took a couple of days to finalize a quick negotiation which normally included several thousands of Mexican pesos, and the title of property of a car –pink slip in the U.S. I worked on two different cases involving relatives of employees, in two separate dates.

Negotiation process

On both instances we took control of the situation, and established contact with the family, the company and, fortunately, with the specialized authorities considering the dates when the incidents occurred. The negotiation was rather simple; however, gathering the money and getting the car according to the kidnappers' demands after negotiating was not that easy. Other than that, the overall conditions were positive, the process went according to what our procedure recommended to manage abductions. Both victims were successfully liberated.

Case: Jalisco, Mexico – Lost person

During the opening process of a retail store in a small town in the state of Jalisco, Mexico, the day before the inauguration event they informed that the operations manager in charge of the process was not answering his cellphone; hence, I was asked to have my team locate him so that he could take the call. The request was impossible to fulfill because nobody knew his whereabouts. We informed the general director that we were trying to locate the manager, but no one seemed to know the hotel he was going to stay or the flight he

could have taken; normally, this manager used to travel alone and always prepared his schedule on his own. His wife did not have any information, they were separated, and he usually made his trips without assistants and without informing anyone of the details. There was no clue about him in a complex urban area.

Search process

When there is no specific starting point from where to begin building a plan, the situation is very difficult to approach. The available intelligence presented a mid-risk zone with regard to organized crime or common crime; hence, we could not rule out an illicit act but, as time went by, no news came up about the lost person. We had to get into action, so we interviewed people close to the missing manager, we looked up information in social networks to identify his hobbies and interests, and determined a search area that we could cover with our resources and support from authorities. This support was difficult to obtain because, legally, not enough time had passed since he went missing. We searched in tens of businesses of all kinds, we searched in the country surrounding the small town; we called hospitals and the forensic offices but there was no trace of him. 24 hours had passed without obtaining a single lead about where he might be. It turned out that—even though the search team worked intensely non-stop all this time, one hour before the opening hour of the new store the missing manager was located. Their staff informed me that the manager's car was parked next to the store, and the manager was sitting inside. We went there immediately and, as he responded to our questions, he told us he decided to take some time off so he spent several hours meditating alone in an open field. The experience, which in the end was solved by itself, resulted in a complex situation that exposed all personnel who took part in the search effort, besides alerting the company.

Case: Quintana Roo, Mexico – Lost person

A corporate human resources event was planned to be held in Cancun, located in the state of Quintana Roo, Mexico, and corporate security was providing them service. We were notified that the weather outlook was not good and the forecast was worst, so the immediate recommendation was to cancel the event and fly all personnel to Mexico City. The recommended plan was authorized and the departure process began. We relocated over 300 employees in record time. After 24 hours of the transportation hard work, I got a phone call from the corporate office in Europe letting me know that, a similar event for the legal division –although smaller in magnitude, was scheduled also in Cancun and they, too, had departed from Cancun but there was one top level executive they could not locate: our missing person.

Search process

The hardship of the situation was posed by the weather, Cancun was getting heavy rain and winds with hurricane force. Only military planes were allowed to land, and transit in the city was more than difficult. We contacted an external security consultant, and they said they would need 24 hours to actually respond. They required a convoy that would allow them to mobilize resources to the zone to begin the search, and that was too much time. So, I sent an element of my team and, with support from federal authorities, we got him onboard an official flight –on a military aircraft. Once the plane landed, he was able to obtain a vehicle capable to endure the harsh conditions, and started searching for the missing executive in hospitals and hotels. It is important to note that, by the time this was happening, communications were difficult and the Mexican government had deployed the DN-3 plan –level 3 of National Defense, which applies to catastrophic situations. With the search operation engaged to this level, and with my security element immersed in the zone under dangerous conditions, I received another call from the European

corporate. This time to report that their missing executive had been found. He decided to take a break and stayed in Miami, and he did not call his wife or his office to inform about his change of plans; however, what he saw in the news about the situation in Cancun made him call home. A very complex and dangerous situation that tested the whole team hard and which, finally, got solved on its own; nonetheless, a security element truly risked his life going on a field search.

Lessons learned

- The intelligence process is critical to understand the conditions and *modus operandi* that may prevail during diverse situations facing different risks. In spite of the three last cases being abductions or lost persons, the conditions to manage the process differed on each instance; and, even when there are always variables that cannot be controlled, having as much information as possible, operative experience, and an excellent communication with top management will always assure you and your team a better response capability.
- In situations like these, it is vital that the security direction attains as much control of the situation as possible, keeping top management up to date about the status and the actions that need to be implemented immediately. This shall provide the necessary leeway to the security director with which to get the first directives into action; nonetheless, as time goes by, the pressure from different actors might increase and among these are: members of top management, family of the affected person, and their immediate superiors. There would also be the self-called experts who take their opportunity to give advice on how to solve the incident. It is the security director's role to manage the contingency, to maintain the corporate team at ease, and to avoid a collateral crisis due to overlooking the multiple elements in the process.

- As *described* throughout the book, each situation brings along its own elements which make them different and unique; there are some, however, that always come into play and these are:
 - Family: Tending to the family is critical, and that is not only during the incident but also once the situation is solved. Selecting the liaison person is fundamental to maintain the family informed and tranquil. Regularly, *this task is emotionally* exhausting, and must fall on human resources; therefore, security must not tend to this needs because the emotional side of any incident is very hard to manage.
 - Top management: The first level executive team will react to the situation according to their concern about the persons involved, their relationship with the affected employee, the legal implications, and also according to the recommendations they receive while the incident is in progress which, unfortunately, also include occasional advisors. Once the security director has been able to *establish a good relationship* with top management, supported by credibility and trust, the security area shall have the necessary room for maneuver to operate without their intervention.
 - Security director's role: Being the security director puts you right in the middle between the incident and top management, you are the intermediary (buffer) in charge of the negotiation; consequently, you shall coordinate the negotiator, and interact with the authorities while keeping the CEO informed. The other areas involved shall also be coordinated by you, and these are usually human resources, legal, public relations (communication), and the area to which the employee reports.
- While there are excellent security consulting companies, I recommend being very careful when working with an external

security consultant. Both instances in which we had an external consultant, the support we received was inadequate and, at times, it even generated risk situations. This happens, especially, when the external support is selected by an area different from security; as a result, a virtual report line is created between the support provider and the area that hired them.

- About contacts and networking, it is important to establish contacts with the authorities when they have professional and reliable structures. Likewise, corporate security should be the function who defines the contacts network, especially when adding external consultants, to verify that their support is real. I happened to have external consultants and support by geographic region where, as a consequence of their nationality and their physical presence, they provided better support than external consultants who –coming in from a different region, are unable to “behave locally.” This is key when you have your team operating without a local security structure, or when you need to reinforce what you have in place.
- You shall expect that, even though the process has been performed successfully, the actions and timings are questioned; particularly, regarding abduction cases in which the victim or their family might consider that “not enough” was done to free them sooner.
- In my experience, the situations of missing persons are far more complicated than the abductions. The variables in these cases are many because you cannot discard an abduction. To begin with, it is hard enough to stay calm and reason out feasible actions –some of which might be urgent. Additionally, it is necessary to maintain a clear communication channel with top management and family, when all parameters are open to possibilities. Then, if the missing person had the intention of disappearing temporarily –which did not seem like that to the subject, that might increase the difficulty of the case. The process required to solve abductions and locating missing individuals, more often than not puts the lives of those performing

the actions at risk; that is so, because even with support from authorities and a good security team, there is always something that may alter the balance demanding you to be ready to act upon new responses.

- Your responsibility as security director for the life of the kidnapped or missing person, the operating team, and the tranquility of affected families is crucial; therefore, you should always carry on with that responsibility, there is no margin for error.

Final reflections

- Corporate security is a professional field that has been barely explained and vaguely understood; consequently, there is little literature on the subject written by executives who have performed this responsibility. In fact, the very concept of corporate security is often misplaced with private security; a common example happens among security professionals because we all have interpretations as diverse as our experiences in the field. I share concepts in this book that I have developed during the last decades, and which have helped me adequate my knowledge and military experience to the corporate platform. The outcome has guided my career path and that of my work teams; hence, the intelligence model has worked so efficiently, that it allowed me to move through different companies, navigating difficult times, and learning to cope with diverse natures, cultures, and loss criterion. Additionally, reducing the learning curve, accelerating the knowledge process, and contributing strategic value sooner has proven to always be beneficial. In summary, all said has facilitated the successful positioning of the corporate security function in all the organizations where I have collaborated.
- With regard to working in different companies, the opinions vary on the subject; I respect every one's decision since conditions and situations are, like decisions, a personal matter. In my case,

the reasons that made me switch companies were: *First*, the lack of professional development and personal growth, being these through studies and training, roles, scope, and corporate positioning. *Second*, because the company did not fulfill what they offered with the position, which is what happens when the small print in a contract includes the most relevant parts. *Third*, when the relationship with the boss turns toxic. *Fourth*, when the offer from another company fulfills my expectations about professional challenges and development. Each of the changes I write about obeyed to one of these reasons, and the outcome has always been positive. I would like to add that my experience in the military entails a professional trajectory where changes are a natural ingredient of growth. Culture in the military is made of constant development, of always aspiring to the next hierarchy, and this is something I brought with me to the corporate world by not being afraid of change, and always preparing for change and even foster change. Corporate life seldom has a career path along with it, or an end goal as reaching the top in the corporate security function. It is hard to decide about changing jobs when you are afraid of managing change, and there is no method or proven process at hand that helps you charting the way; this might be the reason why many capable professionals get stagnant in their comfort zone. Just like becoming an excellent professional is a respectable goal, I believe we should also aim to develop a great professional profile and a brand of our own because, at the end of the day, the best product you have for sale is yourself.

- The concept of positioning has been mentioned many times throughout the book, I regard this as a key element to measure the company's real perception about the corporate security function. Positioning results from two lines: *The first line* denotes the level of interaction the function has with top management, functional directors, and the scope of the conversations with them; as well as the stage, role, and importance of the projects in which security is included. And, above all, the

impact the security value proposal has on the company's relevant decisions in these projects. The requisites to reach this line are: vast business knowledge, operative experience, interpersonal skills, and excellent multi-functional relationship, where internal clients and alliances are the foundations for functional positioning. *The second line* is achieved according to the recognition obtained in the first line. Success in the first line means the organization regards security as a critical service, and their executives as possessing high-level talent which is necessary for the company. Positioning is reached when the executives become part of the company's recognition chart like personnel retention plans, training and development programs for high-level executives, compensation packages and benefits, as well as the profile, roles, and scope in the organizational structure. All of these aspects of corporate assessment and compensation are managed by human resources, which implies that an excellent relationship with the area is in order. When the company acknowledges the value of an employee's contribution to the business objectives, they are regarding the employee as a high performance resource who is worth for the company to invest in their development, and fight for keeping that talent within the organization. So, as the function is included in these parameters, the second line would be achieved. Both lines of corporate positioning require work at structural level which entails the holistic development of the function, not only for the executive level but also for the whole corporate security team; the bottom line here is that the leader would be just as good as the team. The benefits must reach all members in the security team. I firmly believe this vision allows the corporate security director to transcend through the team's development and the impact of the value proposal. Without my team works I would have never succeeded in every organization where I have developed.

- As the final conclusion, I reiterate that all the content shared herein is based on my own professional experience, and totally

motivated by my personal style of leadership and development. I broke the traditional scheme of the armed forces and the private sector, because I never refrain myself from speaking with authorities and lines of command to ask for opportunities to assume new challenges and command posts. I always act supported by solid results, both complying with high impact objectives, and building a relationship with the company based on credibility and trust, from the offering as key service to the critical support during contingencies and crises. As I have mentioned, the experience in the armed forces and the private sector have been an extraordinary adventure; throughout this journey I have provided executive protection to the Pope John Paul II, as well as to presidential families; also, I have been part of the military public prosecutor's office, university professor, international lecturer, security manager and director in Mexico, Latin America and, lastly, global director. And, about what shall be next in my personal and professional life well, I still hold a lot to write about. Here I share the premise that has always guided my path: "Sow efforts and you shall reap opportunities."

Carpe diem...

Track record

MARCH, 1979. AS A MEMBER OF THE SECURITY TEAM ASSIGNED
TO POPE JOHN PAUL II.



SEPTEMBER, 2016. RECOGNIZED AMONG THE MOST INFLUENTIAL
PEOPLE IN SECURITY.

Corporate Security Executives

Antonio Gaona

Head of Global Security, CEMEX



THE
**Most
Influential
People** in Security
2016

MARCH, 2022. RECOGNIZED AMONG THE 100 MOST
INFLUENTIAL SECURITY EXECUTIVES IN MEXICO.



About the Author

Antonio Gaona Rosete is a Lieutenant Colonel, retired from the Mexican Army, who graduated from the Heroico Colegio Militar. Moreover, Antonio also holds a law degree from the Universidad Nacional Autónoma de México (UNAM), and a master's degree in business administration from the Universidad Autónoma de Nuevo León (UANL). Antonio has completed courses for senior executive leadership in the following business schools: IPADE, IESE, Kellogg, Georgetown University, and the University of Pennsylvania (Wharton); he obtained certification in studies on terrorism by the St. Andrews University of Scotland, and on business continuity by the CBIC of London, UK.

Antonio Gaona Rosete served in the Mexican Army for 20 years; in his experience, he performed with the Presidential General Staff, and as Military Prosecutor. Lt.Col. Gaona also has 29 years of experience on top management positions both, in operative and executive roles, with corporations nationally and globally in industries as diverse as: construction materials, retail, telecommunications, tobacco, banking, and entertainment. He has implemented due diligence and post merger integrations processes for operations in Turkey, Russia, India, Algeria, and Brazil, as well operated in high-risk zones in Southeast Asia, Middle East, Africa, and Latin America, where business operations were affected by terrorist groups, guerrilla, and

organized crime. Antonio has performed crisis management processes during violent upheavals in Indonesia, Thailand, and The Philippines; under terrorism in Egypt and Israel; and kidnap and ransom cases in Colombia, Mexico, and Haiti.

Ltc.Col. Gaona has been recognized, in the United States of America, as one of the most influential corporate security executive officers in the security industry in 2016, on a global scale; and also, as one of the top 100 most influential corporate security executive officers in Mexico in 2017 and 2022. Furthermore, Antonio has been a member of the International Security Management Association (ISMA) for more than 20 years.



Corporate Security Executives

Antonio Gaona

Head of Global Security, CEMEX

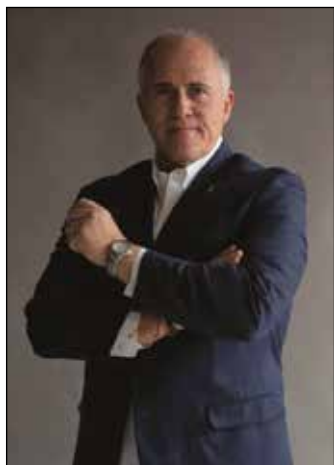


THE
**Most
Influential
People** in Security
2016



Corporate Security. A Key Piece on the Corporate Chessboard
was completed in Mexico City during the month
of October 2023. The edition was in the care of the
lithotypographic office of the publishing house.





This book deals with the criteria that govern business organizations in terms of loss management and how the Corporate Security executive must apply an Intelligence model to understand the times that the company lives, its nature and, in the end, what determines its performance and its organizational culture. Once you understand the above, you can structure a value proposition such that it is included in critical decision making.

Corporate Security becomes a critical function when it addresses the human nature of corporations in their identification and assimilation of risks, and in how they decide to manage their actions to manage loss. This differentiates mandatory compliance from compliance as a culture. We are not talking about the security of the company, but about a safe company.

The author shares in this work more than 28 years as a senior manager of Corporate Security, operating globally for construction, tobacco, retail, telecommunications, banking and entertainment companies, in environments of terrorism, guerrilla, social violence, organized crime and natural disasters, where the times and nature of each company determine the actions to be taken to manage these conditions. It also narrates how he achieves a successful 20 year transition from the field of security in the armed forces to the corporate world.

This book is a reference document not only for Corporate Security specialists, but for anyone whose responsibility is to see for safer and more resilient companies

