



# WHITE PAPER

**2022**

**ON THE SECURITY FUNCTION IN CORPORATE BUSINESSES**



# INTRO > DUCTION



## STÉPHANE VOLANT

PRESIDENT, CDSE

As early as 2011, the Club of Chief Security Officers (Club des directeurs de sécurité des entreprises - CDSE) laid down the fundamentals of the Security Function in corporate businesses with its first White Paper, thus accompanying an ongoing revolution in organizations. These fundamentals can be found in this new opus, with a perspective that is fresh but strengthened by more than ten years of crisis management practice and daily experience of the hazards of corporate security. For the Security Directors who are members of the CDSE, these “good practices” constitute the bases, the “invariants”, guarantees of a **security strategy that is integrated into the governance of the company because it is efficient and transverse, and at the service of the business.**

These fundamentals of security, however, will most certainly have to be revisited in the third White Paper of the CDSE and probably even in the fourth because, despite a revolution, other evolutions have yet to happen. Several businesses, among the flagships of the French economy, have yet to grasp the significance of these topics and have not set up a security department yet. Others believe that they are taking these issues into account, but should, however, be allocating even more resources to them. Thus, reading through the CDSE 2022 White Paper is as much about measuring how far we have come as it is about seeing the efforts that still need to be made. It is demonstrated, at the end of the document, by **the 18 structuring recommendations for a strategic Security Function in Corporate Businesses, fully integrated with the security continuum.**

In line with the progress made, this White Paper is the result of the fusion of ideas from **the 14 commissions and working groups. They promote experience sharing and the emergence of solutions for all topics that corporate security departments deal with.**

Protecting people and tangible and intangible assets, business intelligence, international security, crisis management and business continuity, but also fraud and compliance, supply chain... The diversity of issues discussed year-round at the CDSE and dealt with by security departments in their daily activities illustrates the growing role of this function, at the heart of a business's global security policy.

Some of these themes were absent from the 2011 White Paper but now appear to be essential. The management of **radicalization**, for example, is of considerable importance in organizations. Security departments are now taking their full part in raising awareness of this phenomenon and are proposing tools or procedures to deal with deviant behaviour and therefore protect the business. That is why the CDSE closely works with the Secretary-General of the Inter-ministerial Committee for the Prevention of Delinquency and Radicalization (SG-CIPDR).

In 2011, there was no talk of **cybersecurity**. In 2022, the issue of technology and cyber is omnipresent, both in our businesses and personal life. Security Directors have never been so involved in these issues. Cyber-attacks are a proven threat and Security Directors know that the protection of the business first of all requires controlled digital security. They are now working intelligently with their fellow CIOs (Chief Information Officers) and CISOs (Chief Information Security Officers). These crisis professionals are working daily to better raise awareness among all employees and constantly prepare the business for worst-case scenarios, **to think and imagine the unthinkable, to manage uncertainty**. Hence why the ANSSI (French National Agency for the Security of Information Systems) wanted to work with the CDSE to recently publish its guide *"Cyber-related crisis: the keys to operational management"*. Here too, it is good proof of the path the Security function and the CDSE have taken over the past eleven years.

In 2022, the Security Director is no longer working alone. Security is an active subject and the job description of the person in charge of it will always evolve. Resources allocated to the security department are not fixed and vary along with each business according to its history and its sector of activity. However, **the Security Director can now rely on a real professional sector made from people with different backgrounds and multiple skills**. A study led by the CDSE since 2017 now gives us a more accurate picture of the general physiognomy of these departments, as well as the progress to be made in terms of professionalization and attractiveness. The feminization of the sector, for example, is underway, although there is still a lot to be done in this area. Nevertheless, seven female Security Directors, CDSE commission chairs or experts, contributed to this White Paper. There were only two of them in 2011. There will be even more of them in 2032.

And then in 2022, security expenditure is no longer simply considered as a cost by Businesses, but more as an "avoided cost", an investment with certain profitability, value and a competitive advantage, in the same way as the requirements related to corporate social responsibility (CSR). Thus, by protecting their rights-of-way, their employees and their clients, Security Directors contribute to national security. The presence of successive Interior ministers [eq. Homeland Security] at each edition of the CDSE annual conference attests to this. And Gérald Darmanin was not mistaken, during the 2021 edition, when he described Businesses and the private security firms they employ as *"the third security force of our country"*. That is why, as in 2011, the CDSE recommends in this White Paper **the creation of a "circle of trust" establishing the Security Directors as privileged interlocutors of law enforcement and State in businesses and allowing information sharing based on professional secrecy**. Such a measure would definitively give substance to the security *continuum*, for an increasingly optimal homeland security.

As you understood, our recognition is legitimately due to the “great elders” of the CDSE, pioneers of the role of Security Directors within businesses. And the current members of the Club, co-authors of this White Paper, are proud to present to you, in the following pages, the fruits of their work and their reflections...



**WHITE PAPER**  
on the Security Function in Corporate  
Businesses. CDSE Paris. May 2022

**Publishing director**  
Marc-Antoine Bindler

**Contributors**  
Gabrielle Berthelot, Jean-Paul Bonnet,  
Serge Collignon, Christian Crémel, Antoine Creux,  
Edmond d'Arvieu, Clémentine de Lambilly,  
Bernard Galéa, Jean Garcin, Christophe Gomart,  
Arnaud Kalika, Jean-Louis Kibort, Aurélien Lambert,  
Fabien Laurençon, Fabienne Louvet,  
Pierre-Arthur Mazeau, Jean Maurin, Claire Niclause,  
Jean-Yves Oger, Émile Perez, Anne Picot-Periac,  
Michel Pozzo di Borgo, Rudolphe Proust,  
Joëlle Rietjens, Annick Rimlinger, Pierre Tramier

**Traduction**  
Charlotte Coombe, Florent Janssen & Margot Barbe

**Graphic design**  
Aurélie Alder. San Emeterio  
[reflexiongraphique.fr](http://reflexiongraphique.fr)

SUMMARY

**I. DEFINING  
THE SECURITY FUNCTION  
IN SECURITY BUSINESSES**

**P. 11**

POSITIONING OF THE SECURITY FUNCTION

**SAFETY IN BUSINESS STRATEGY: REALITY OR FICTION?**

**Bernard GALÉA** . Danone . CDSE Administrator

**P. 12**

THE SAFETY & SECURITY SECTOR

**THE SECURITY DIRECTOR: A STRATEGIC ROLE  
WITHIN A LARGE ECOSYSTEM OF STAKEHOLDERS & SKILLS**

**Fabienne LOUVET** . Renault . Chair of the CDSE's "CCEF" commission

**P. 18**

LEADERSHIP & MANAGEMENT

**WHAT ARE THE MANAGERIAL QUALITIES THAT MAKE  
A GOOD BUSINESS SECURITY DIRECTOR?**

**Christophe GOMART** . Unibail-Rodamco-Westfield

**P. 30**

BUILDING A SAFETY & SECURITY DEPARTMENT

**THE CREATION OF A SECURITY DEPARTMENT IN 2022:  
THE RECENT EXAMPLE OF PERNOD RICARD**

**Serge COLLIGNON** . Pernod Ricard

**P. 35**

BUSINESS-STATE RELATIONS

**THE NECESSARY CO-PRODUCTION OF SECURITY**

**Émile PEREZ** . EDF . Vice-President of the CDSE in charge of International

**P. 40**

**II. FONDAMENTAUX & MISSIONS  
OF THE SECURITY FUNCTION**

**P. 51**

INTERNATIONAL SECURITY

**THE SECURITY DIRECTOR FACING INTERNATIONAL CHALLENGES:  
ARNAUD KALIKA'S PERSPECTIVE (MERIDIAM)**

**Arnaud KALIKA** . Meridiam . Chair of the CDSE's "International" commission and CDSE Administrator

**P. 52**

CRISIS MANAGEMENT & BUSINESS CONTINUITY

**CRISIS MANAGEMENT CANNOT WAIT ANY LONGER**

The "Crisis management & Business continuity" commission of the CDSE: **Gabrielle BERTHELOT** . Kering  
**Anne PICOT-PERCIAC** . Atos . **Joelle RIETJENS** . EDF  
Under the direction of **Jean-Yves OGER** . Renault . Chair of the commission

**P. 58**

CONTRACTORS & PRIVATE SECURITY PROVIDERS

**ESSENTIAL PLAYERS IN THE SECURITY CONTINUUM  
FOR A RESPONSIBLE PURCHASER & A QUALITY PRIVATE SECURITY**

The "Private security" commission of the CDSE: **Claire NICLAUSE** . RATP  
and **Christian CREMEL** . Bouygues . Chair of the commission

**P. 64**

CYBERSECURITY & INFORMATION SECURITY

**THE SECURITY DIRECTOR & CORPORATE CYBERSECURITY ISSUES**

**Jean-Paul BONNET** . Safran  
Chair of the CDSE's "Cybersecurity & information security" commission and CDSE Administrator

**P. 72**

STRATEGIC & COMPETITIVE INTELLIGENCE

**STRATEGIC AND COMPETITIVE INTELLIGENCE,  
A VECTOR OF ASSET ENHANCEMENT**

The CDSE's "Strategic and competitive Intelligence" commission: **Fabien LAURENÇON** . IRSEM  
Under the direction of **Jean-Louis KIBORT** . L'Oréal . Chair of the commission and CDSE Administrator

**P. 77**

FRAUD & COMPLIANCE

**COMPLIANCE & FIGHT AGAINST FRAUD:  
TWO GROWTH LEVERS FOR THE BUSINESS SECURITY DIRECTOR**

**Rudolphe PROUST** . Altarea . Chair of the CDSE's "Fraud & Compliance" commission

**P. 84**

PRODUCT LIFE CYCLE & SUPPLY CHAIN

**PRODUCT SAFETY, TRAFFIC & SUPPLY CHAIN:  
FOR A GLOBAL FIGHT AGAINST TRAFFICKING**

**Edmond d'ARVIEU** . Sanofi . Chair of the "Supply chain" working group of the CDSE

**P. 89**

CRITICAL INFRASTRUCTURE

**PROTECTING CRITICAL INFRASTRUCTURES:  
A COMPONENT OF GLOBAL STRATEGIC REFLECTION FOR BUSINESSES**

**Michel POZZO DI BORGO** . Bank of France  
Chair of the CDSE's "OIV & protection of installations" commission

**P. 103**

SÉCURITÉ GLOBALE

**DEFINING A GLOBAL SECURITY POLICY WITHIN THE COMPANY**

**Antoine CREUX** . Société Générale . CDSE Administrator and Treasurer

**P. 109**

### III. NEW CHALLENGES & PERSPECTIVES IN SECURITY

**P. 115**

RADICALIZATION

**THE RADICALIZATION PHENOMENON:  
A RISK FOR THE COMPANY**

**Pierre TRAMIER** . Danone . Chair of the CDSE's "Radicalizations" commission

**P. 116**

DIGITALIZATION & TECHNOLOGIES

**DIGITALIZATION OF THE SECURITY DEPARTMENT:  
OPPORTUNITIES & RISKS**

CDSE Lab: **Clémentine DE LAMBILLY** . Orange and **Pierre-Arthur MAZEAU** . Thales  
Under the direction of **Jean GARCIN** . Manpower . Co-chair of the CDSE Lab

**P. 121**

ANTICIPATING CRISES

**THINK & IMAGINING THE UNTHINKABLE, MANAGING UNCERTAINTY**

The "Crisis management and Business Continuity" commission of the CDSE:  
**Gabrielle BERTHELOT** . Kering . **Anne PICOT-PERCIAC** . Atos

**P. 127**

SECURITY CONTINUUM

**CORPORATE SECURITY DIRECTORS  
WITHIN THE SECURITY CONTINUUM: A DESIRE YET TO BE REALIZED**

**Annick RIMLINGER** . Aéma

**P. 134**

PERSPECTIVES OF THE SECURITY DIRECTOR

**WHAT SKILLS ARE NEEDED FOR TOMORROW'S SECURITY DIRECTOR?**

**Aurélien LAMBERT** . EGIS

**P. 144**

**18**

## STRUCTURAL RECOMMENDATIONS

**P. 153**

FOR A BUSINESS SECURITY FUNCTION THAT IS STRATEGIC  
AND FULLY INTEGRATED INTO THE SECURITY CONTINUUM



# **I. DEFINING**

THE SECURITY

FUNCTION

IN CORPORATE



BUSINESSES

## SAFETY<sup>1</sup> IN BUSINESS STRATEGY: REALITY OR FICTION?

### Bernard GALÉA

*Vice-President Security and Economic Intelligence of the DANONE Group, and CDSE Administrator*

If the Company has a modicum of control over its endogenous risks, i.e., those generated by its own activity (accidents at work, process...), it is increasingly confronted with diffuse exogenous risks.

In a world in total upheaval where uncertainty is growing, organizations are facing new and multi-faceted challenges. We are almost simultaneously experiencing persistent conflicts in Syria, the Sahel, Afghanistan, Ukraine, a significant growth in radicalization movements and sectarian deviances, unprecedented health crises, natural disasters, exacerbated trade tensions between countries, and so on.

These various crises have had, have, and will continue to have geopolitical and geo-economic consequences which force companies to rethink their strategy and modify their approach to safety.

Nowadays, the security function's goal is to protect the Company, its people, its assets, against all forms of malicious threats, whether of human, logical or economic origin: it is now a concept of a global approach.

In the aftermath of 09/11 attacks, physical security suddenly became the priority. All leaders feared that terrorist attacks would impact their staff or facilities. More than twenty years later, in 2022, in the "new normal" era, skyrocketing digitalization, Artificial Intelligence, financial fraud, the advent of remote working, cyber-attacks combined with political instabilities and the still uncertain consequences of the COVID-19 crisis are forcing Security Directors and their teams to be more agile. The latter must cover an ever-wider spectrum. And, in the same way, they are required to promote at least convergence with other functions such as those of the directors of Information Systems Security, HSE risks (health, safety and environment), Risk Management, Crises and Business Continuity.

### RISK MANAGEMENT: A BUSINESS UNDERTAKING MEANS TAKING RISKS

The company's strategy mainly consists of three pillars: the business model, competition, and the area in which it can deploy its market.

Through comprehensive risk and crisis management, the Security function helps building the foundations of the three pillars and contributes to developing and implementing the strategic plan by protecting the organization.

Upstream of any decision-making process, it partakes in risk analysis (geopolitical, security, competitive, reputation, predation, destabilization, counterfeiting, incidents in the "supply chain", etc.) to be able to anticipate them. The ability to collect, sort and analyse information to understand the environment, discern threats and think of adequate means of protection becomes an expertise that is critical to protect organizations in a relevant way.

<sup>1</sup>Security: for the purposes of this article, a generic term covering Safety and Security.

In its deployment phase, it must prevent risks and, in the event of their occurrence, participate in crisis management and business continuity measures to enable the company to pursue its strategic objectives by adapting to its new environment.

**More than ever, security is the necessary support for the decision-maker's risk-taking. The Security Director has become a business partner aiming to secure the thoughts and decisions of board members and executive committees by reducing uncertainties.**

### **TRUST: A BUSINESS UNDERTAKING SHOULD BE SOCIALLY RESPONSIBLE**

**Corporate Social Responsibility (CSR)** is defined by the European Commission as the integration by organizations of social and environmental concerns into their business activities and their relationships with stakeholders. In other words, CSR is how companies contribute to all kinds of challenges linked to sustainable development..

Ever since the PACTE Law of 22 May 2019 came into force, new provisions have been adopted to strengthen CSR:

- The corporate purpose of all companies includes consideration of social and environmental issues.
- Companies that wish to do so can provide themselves with a mission statement in their articles of association.
- The status of "mission-led company" has been created.

Data integration on non-financial risks and performance has therefore become a strategic issue for Businesses, both to attract talent and retain them and to communicate with stakeholders (shareholders, consumers, employees, government agencies...).

Also, the new Universal Registration Document (URD) defined by a European regulation that came into force in 2019, now includes precise information on security risks. For example, indicators on the protection of business travellers, local employees and expatriates are very popular.

Beyond meeting a legal obligation of the employer ("*Duty of care*", article 121-2 of the Criminal Code and article L 4121-1 of the Labour Code), they make it possible to measure the maturity of organizations in their risk analyses (not only financial risks but also security-related ones), in countries where operations and markets are deployed.

Thus, as already pointed out in 2018 by Mrs Nicole Notat, president of Vi-geo Eiris and former Secretary general of the union CFDT, during the annual conference of the CDSE organized at the OECD: "*Beyond the human, economic and financial issues vital for the sustainable performance of companies, security is now emerging as a central element of social responsibility until it becomes a competitive advantage*".

### **GOVERNANCE: THE ACT OF UNDERTAKING MEANS MAKING THE COMPANY SUSTAINABLE**

Positioned at the highest level of the company, the Security Director must report to the President or to a member of the Executive Committee (Excom). This connection guarantees the alignment of security with the business strategy and makes it possible to better anticipate risks.

The Security function, which is inherently transverse, is at the crossroads of governance of performance (value creation) and compliance (risk management), which form the two pillars of a company's governance.



Often perceived as a cost centre, security, on the other hand, supports value creation and helps to avoid certain financial losses by anticipating pitfalls, by strengthening mitigation measures or by participating, along with the Compliance or Internal Audit teams, in the operational implementation of ethical rules and business conduct (Sapin II Law, etc.) to make the company sustainable and resilient.

However, the risks anticipated and managed by security departments are often invisible in the organization's risk mapping.

Indeed, risk analysis is mainly based on a financial approach driven by the internal control/audit/risk departments governed by a battery of processes such as ERM, COSO, ISO, etc.

Yet, security risks are poorly standardized, unpredictable by nature and their financial impacts are difficult to measure, which may explain the difficulties faced by companies when it comes to budgeting for this role.

**Security is therefore part of the long term of the Company, but its maturity is not homogeneous between organizations.**

For some, it is still fiction. The security function is not properly positioned, dimensioned, and does not have a budget proportionate to the risks it has to meet. For others, the Security Director has become a fully-fledged executive.

Thus, if some companies choose to adopt a tactic that will perhaps allow them to win the next game... Those that have integrated safety into their business strategy will be able to win the championship. ■

# RECOM > MENDATIONS

- > Continue to “evangelize” the Excom and HR managers about the company Security Function.
- > Set up an educational strategy to make future leaders aware of the roles and functions of Security (ENA/INSP, Sciences PO, HEC and business & management schools...).
- > Ensure that the sector is well positioned within organizations.
- > Set up ongoing training sessions, for the benefit of the Security Directors and their teams, which are not technical, but related to “*general business management*” instead.

## THE SECURITY DIRECTOR: A STRATEGIC ROLE WITHIN A LARGE ECOSYSTEM OF STAKEHOLDERS AND SKILLS

### FABIENNE LOUVET

*Chair of the CDSE's "Careers-Employment-Training" commission  
Professions and Organization of Security Director, Renault*

Since the 2000s, faced with the diversification of threats and risks (cyber, terrorism, geopolitics, health...) and their interdependencies in a globalized, decoupled, hyperconnected economy, the Corporate Security function (SSC) in companies has grown considerably.

In France, most large companies now have a corporate security department, and everyone perceives, even more so since 2020 in the light of the COVID-19 crisis, the increasingly unavoidable nature of this service.

However, there is no typical SSC department: missions, organizations, and sizes of these departments are very heterogeneous and relate to the intrinsic characteristics of each company, its sector of activity, its risk-exposure, and its history.

## I. DEFINING THE SECURITY FUNCTION IN CORPORATE BUSINESSES

In order to see a collective positioning of the sector, its current professions, and the necessary future evolutions for "global security", the CDSE has been conducting a follow-up study on the professions in the corporate security sector, led by its "Career-Employment-Training" commission since 2017. This in-depth analysis thus aims to answer multiple questions:

- > What is the physiognomy of the sector?
- > What are the various security professions within companies?
- > What is the reality of the positioning of these roles, their levels of expertise and intervention?
- > What are the career paths and prospects of these professionals?
- > What is the degree of attractiveness of the sector and how should it progress to meet tomorrow's challenges?

This work was conducted in two phases with the assistance of consulting firms selected for their expertise and professionalism: EY, specialized in organization and prospective studies, and Arthur Hunt, specialized in Human Resources (recruitment, career paths and remuneration practices).

The first phase, published in 2019, made it possible to draw up the current physiognomy of the sector, to carry out analyses on organizations and to strengthen the positioning of these activities at a strategic level in companies. The study and structuring of professions by skills has also resulted in the development of a new document in the form of a modular SSC job reference system, adaptable to the diversity of organizations which includes, without claiming to be exhaustive, 12 benchmark job sheets.

In 2021, the second phase came to refine these founding works and deepen the levels of contribution, the remuneration practices in force as well as the career paths and prospects at all levels of the sector.

<sup>1</sup> Global security covers the prevention and protection of people, of a company's tangible and intangible assets against all accidents and malicious attacks, as well as monitoring activities, crisis management, business continuity and economic security. Depending on the company, corporate security departments cover all or part of these business areas.

This study of jobs, activities and associated skills has become a reference tool in the sector's ecosystem, to support the evolution of its stakeholders. All deliverables thus constitute an instantly operational framework for the Security Directors, especially regarding exchanges with their Human Resources department. Jean Maurin, Director of Prevention and Protection of the Renault Group, emphasizes that *"this CDSE study is very useful to us, because it describes the security professions in a very comprehensive way. It can be used as a basic reference when work is being carried out within the company on the organization or reorganization of the security department."*

**Here are the main lessons learned from the CDSE study on professions in the security sector in corporate businesses.**

### **A STRATEGIC SECTOR THAT IS EVOLVING TOWARDS A VALUE CREATION ROLE**

This is the first lesson of the study; the SSC department is **a privileged interlocutor of governances and a strategic stakeholder within the business**. Although the profession is still unknown, it is proving to be strategic, at the core of a company's challenges and operation: **in 74% of companies, the corporate security department is attached to the senior management or the general secretariat**. It is evolving from a position of anticipation, prevention, and protection, perceived as a cost centre, to a value creation role, as a real Business Partner of the Board. The Security Director therefore strives to transform this perception into a value creation strategy.

Indeed, the primary purpose of this profession is to contribute to the company's performance by increasing its resilience to risks and threats that weigh on the company. As such, its ability to take a step back and systematically analyse the strategic value of elements to be secured is decisive. Corporate security is thus increasingly positioning itself as a competitive advantage, even becoming part of the brand promise in sectors such as tourism, leisure parks, public transport, culture, and food production.

The study further shows that **the Corporate Security role asserts itself as essentially transverse, with an "extended company" scope** which translates into a great openness internally and externally. Internally, the position interacts with all the functions and roles within the company to integrate safety and security into their processes, which pre-supposes structured relationships with almost all the company's management and the co-construction of transversal processes. Externally, it sets up numerous interactions with customers and suppliers, but also with institutions and administrations.

*"The main characteristic of a corporate security department is to be both strategic and transverse,"* reports Geoffrey Fournier, Director of Health, Safety, Security and Environment of the Flex-N-Gate Group, *"This requires a certain versatility. Indeed, it deals with a multitude of topics with high added value in restricted periods of time, which makes it particularly attractive on a daily basis."* To carry out its missions, the corporate security department needs in-depth knowledge of the company (its businesses, its markets, its customers, its interlocutors) as well as of its functioning, and to build stakeholder networks. It must also have a detailed knowledge of the functioning and codes of the administration.

**AN ATTRACTIVE CAREER PATH,  
MULTI-SKILLS, EXPERTISE AND ASSERTIVE LEADERSHIP**

The SSC function covers an extremely broad range of qualifications, with fourteen lines of competence identified, eight expert positions already defined and ever-increasing requirements. Corporate security departments are therefore calling on experts that are increasingly skilled, but with a need for assertive behavioural skills, especially leadership, allowing for a decompartmentalization and an influence within the entire ecosystem.

**MAPPING THE CORPORATE SECURITY PROFESSIONS**

**Governance - Leadership**



**Expertise - Advisory - Deployment**



**Monitoring - Analysis - Follow-up**



**OPERATIONAL ACTIVITIES (COUNTRIES, SUBSIDIARIES...)**



**I. DEFINING  
THE SECURITY  
FUNCTION  
IN CORPORATE  
BUSINESSES**

The study demonstrates that **the sector is particularly attractive for professionals which come from law enforcement or institutions, as well as for business executives.** *“It is an attractive sector because of its global business vision, its significant contribution to the achievement of its objectives and its remuneration, which is significantly higher than the market,”* explains Yann de Kersauson, Executive Search Recruiter for the Human Resources consulting firm, Arthur Hunt. *“Regarding corporate Security Directors, this valuation is justified by their experience, their expertise and their ability to pull back in order to advise and accompany in decision-making at the highest level of the company. In addition, they must be very available. In their mission, they also have a prescription capacity that goes as far as the right of veto. And, depending on the situation, they may engage the responsibility of the company.”*

Globally, **the level of remuneration is 4% to 15% higher than the market (all In 2021, 91% of CSOs are professionals with a career in institutions)** A CSO is expected to have experience, maturity, and leadership skills, as explained by Jean Maurin (Renault) (See box p. 26).

Corporate security requires a sense of the general interest, to be passionate but also to have a very curious and critical mind, a good general culture at the international level, an ethics, a deontology, to love action because we are close to the field, and to be able to intervene in very varied positions: transverse or hierarchical management, prescriber, order-giver, contributor, ability to veto, etc...

They must be forward-thinking and responsible, with a strength of conviction, the ability to adapt to the challenges of the company, advice and prescription, quick decision-making under pressure, discretion on sensitive topics, good at listening, the ability to work in a team... these are all qualities expected of those in corporate security departments.

### **A NEED FOR DIPLOMAS & RECOGNIZED TRAINING**

Another salient point: although women are poorly represented in management positions, as in the regal domain, they are, on the other hand, the majority in entry-level positions in the sector, where they represent 57% of security analysts. A dynamic of feminization is therefore underway and will take some time because experience is a prerequisite to progress in the sector.

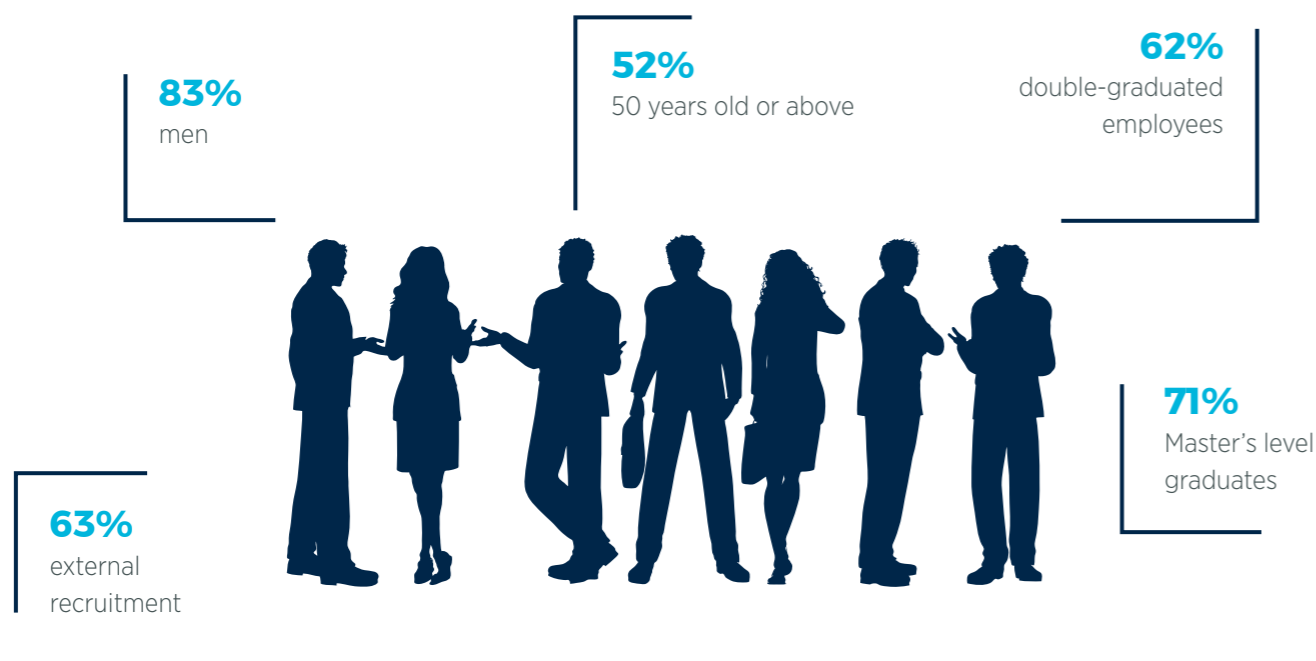
*“The rise in skills and the increasing specialization that characterizes the corporate security sector poses many challenges for the new generations,” says Natasha Lery, Cyber Threat Intelligence Analyst in the security department of the Orange Group. The corporate security sector is expected to attract new talents in cutting-edge fields such as cybersecurity. Faced with new security challenges, the corporate security sector presents intellectual and professional challenges which are constantly being redefined, which are exciting.”*

The observation drawn up by the study shows that experience prevails in an academic curriculum. The passage through the regal domain and institutions serves as a training path and a guarantee of credibility in management positions. To progress and become more and more professional and avoid the phenomenon of the “glass ceiling”, the sector must develop diplomas and recognized training and promote career paths integrating mobilities external to the sector (including public-private).

This approach committed to the visibility of the sector, development prospects and career paths should contribute to retaining and attracting talent.

With great challenges for the younger generations to take up! ■

**> For more information, we encourage you to download the main deliverables of this study available on the CDSE website > [cdse.fr](http://cdse.fr): the professional reference system, as well as the survey on remuneration and professional paths.**



### **PHYSIOGNOMY OF THE CORPORATE SECURITY SECTOR**

## THE BUSINESS SECURITY DIRECTOR'S LEADERSHIP

Perspective of Jean Maurin, Director of Prevention and Protection of the Renault Group

*"Leadership, management, governance, steering, direction... A lot of words, the study of the nuances of which is a treasure trove for those who advise, teach, testify, post, or quote them, both in business schools, at university, at symposiums or via professional social networks. These words navigating in the field of semantics try to portray the different facets of the art of exercising one's authority for the success of a common cause.*

*Uniting a human collective and mobilizing resources to achieve specific goals is nothing exceptional, it is the lot of every manager, who relies on solid fundamentals, remains pragmatic and demonstrates situational intelligence.*

*What should the corporate Security Director be like, or how should they be different, to assume their authority? In my eyes, they are no different from any other director, but must pay special attention to the following points:*

### GETTING INTO THE ARENA

*By mingling, if only a little, with the reality of the daily trials of those who carry out security and safety projects on-site. It is a general principle of life: it is in our interests to get into the arena of real life, and to know the core projects if we want to understand them as well as possible. Understanding how a site (factory) operates enables us to know its strengths and weaknesses and those of the company, the more or less functional machinery between its various departments, its internal and external environment. This knowledge of "series life" also makes it possible to perceive the common sense of the field that drives the teams, and to add substance to principles, regulations, prescriptions. This contact, based on listening and true prices, must then lead to mutual trust and respect, guaranteeing great efficiency in the event of a crisis, and shared common sense when making decisions.*

### BE BOLD

*By always seeking to act in a forward-thinking way, to be reactive, to constantly adapt to developments. To do this, fight the "don't do it machine", by inculcating the cult of the mission and the sharing of information for achieving common good. People who refuse to shake up their habits do so either out of inflexibility, or in order not to leave their comfort zone, or because they do not see the need to evolve because they do not understand the urgency of adapting to the rapidly changing environment. Being bold means first convincing your teams of the merits of the task entrusted to you.*

*Develop everyone's individual qualities. Sense of mission, sense of commitment, willingness to train, sense of community, loyalty. All these qualities can only be developed if everyone is convinced that they belong to the same family that acts for the common good of the company. We do not choose our work colleagues, as we do not choose our parents and siblings, but belonging to the same family allows us to grow, to learn, to help each other, to be raised, to surpass ourselves, to overcome all the hardships together, and ultimately to live for a cause that surpasses everyone and makes them participate in a larger narrative: the safety and security of people and property, both guarantors of the life and development of the "company" family*

### THE CORPORATE SECURITY DIRECTOR DOES NOT ACT ALONE

*In contact with their employees, first and foremost understanding the life of the company and its challenges will help them to fulfil the common mission, as a family, and to face with calm and determination the challenges that the unexpected will pose."*

# RECOM > MENDATIONS

- > Continue the professionalization of the teams by strengthening the technical training courses specific to the sector to meet the growing needs for expertise.
- > Strengthen leadership skills, in particular by including training modules on behavioural skills.
- > Design career paths integrating internal and external mobility to the sector within the company as well as with institutions.
- > Develop training courses dedicated to security executives to improve their employability and facilitate their mobility.
- > Develop nursery professions, make them attractive to young people.

# GENERAL RECOM > MENDATIONS

- > Strengthen the professionalization of corporate security roles through dedicated training courses and career paths integrating mobility outside the sector in the company and with institutions.
- > Integrate security and safety processes into the company's management system.

## WHAT ARE THE MANAGERIAL QUALITIES THAT MAKE A GOOD BUSINESS SECURITY DIRECTOR?

### CHRISTOPHE GOMART

*Director of security, risk and crisis management of the Unibail-Rodamco-Westfield Group*

If the question is asked to chief executives of the companies that employ them, the latter will answer that when recruiting them, they wanted security directors that are security professionals and managers, with all the leadership and human qualities such as boldness, tenacity, organizational skills, sociability, decisiveness, team spirit and, if possible... the provision of a public security network.

In a word, the rare pearl: a perfect being, tall, good-looking and strong, in other words it's like trying to square the circle. This rare pearl can obviously be a woman or a man.

**B**ut let's ask ourselves about the specific qualities required for competent Chief Security Officers. It is necessary to clarify at the beginning of the analysis that the role and the scope of their responsibilities is (very) variable depending on the company. While one might be strictly in charge of safety and security, another might also deal with cybersecurity and a third might encompass risk management or even business intelligence, without forgetting the one, who covers the overall security of the company, both physical and logical. It is therefore difficult to try to define the needed qualities according to the scope of responsibilities.

### THE SECURITY DIRECTOR: A MANAGER LIKE ANY OTHER...

Are the leadership qualities and human qualities ("soft skills") of a Business Security Director not the same as required of every manager, or are they specific qualities?

First and foremost, a Security Director is, in fact, a manager in charge of a more or less large team. Like any manager, they are asked to be a leader who leads a team, orientates it, and directs it to achieve the objectives set within the framework of the company's strategic plan. For this, they lead by example.

**Exemplarity is the essential quality of a manager but above all that of a leader.** Do as I do, not just as I say. A good manager is someone who unites the talents that make up their team to progress and win together, knowing that the manager disappears behind their team. They are the one who highlights and not the one who highlights themselves. The success of their team belongs to the team and not to themselves, even if their action has been unavoidable and indispensable. The Security Director, like all good managers, is someone who dares, someone who knows how to be bold wisely. They also know how to push their teammates or colleagues to dare. Because if we don't dare, we don't move forward and we don't progress. They are the one who acts the opposite of the one who waits for a solution to emerge by itself in the manner of Henri Queuille: *"There is no problem that an absence of a solution does not end up overcoming"*. They are the one who leads towards a solution and then decides to apply it, even though the initial idea came from one of their subordinates. They are a leader who sets a strategy and knows where they are going.

### ... WITH SPECIFIC QUALITIES

A company manager expects the Security Director of course, to define a security policy for the company or the Group, and to implement it. But above all, they expect them to have qualities that are indispensable to the role. The first of these is undoubtedly the ability to adapt to any new situation, to an ever-changing and evolving situation



**The ability to adapt makes it possible to take advantage of opportunities, react to consequences and adapt to potential damage.** React quickly to changes in ideas, expectations, trends, strategies and other processes inherent in any business life must be the daily concern of every Security Director. To do this, they must be able to take a step back while knowing how to get their hands dirty when necessary. Able to both reflect and to act, they are a person in the field. Moreover, few “group” level managers in companies know the field and have concrete feedback from it as well as CSOs do. This is why, if we look at the profiles of Security Directors, a high proportion of them come from the ranks of the police, the gendarmerie nationale or the French army. Their qualities are those of people who have learned through their previous responsibilities to act in times of crisis. However, having moved in these circles is not an indispensable condition for making a good Security Director. If this is an obvious added value in terms of experience, in terms of decision-making in degraded mode and in constrained periods of time... more and more Security Directors who are not from the police or military ranks come into companies and do a remarkable job. **Their strength lies in this ability to adapt to a security environment from which they do not come, and which was until recently pre-empted.**

This ability to adapt goes hand in hand with situational intelligence. This quality allows the Security Director to have a proportionate reaction to the situation. Thanks to it, they act knowingly, considering the environment, the context and the people involved in order to be effective in their reaction. This is not an innate quality. It is acquired by demonstrating a rapid understanding of the issues and the invisible mechanisms that govern behaviour, but also empathy.

### **THE SECURITY DIRECTOR MUST BE KNOWN AND RECOGNIZED**

The Security Director must not remain in the shadows within the company, they must **be known and above all recognized**. This condition is related to their ability to be understood and heard. For this, of course, having expertise in global security is a prerequisite. But what matters is having perfect knowledge of how the company operates, and their integration within it. They must become what is called a **“business partner”**. They are the one who protects the functioning of the company and facilitates it, and even speeds it up as much as possible. For this, they must **be creative**. Another of the required qualities is **resilience** because this knowledge and this integration can take time, whether it is time to know, to understand or to convince.

Beyond the essential “hard skills”, we recognize a good Business Security Director by their leadership qualities and human qualities. Their qualities are linked to the very essence of their profession, which is uncertainty.

Uncertainty in the face of the threat, uncertainty dealing with the behaviour of security providers, uncertainty dealing with the behaviour of company employees in the event of an incident, uncertainty dealing with the involvement of company managers... To deal with it, defining a strategy is the first condition. Since security is intimately linked to crisis, the Security Director must be the one who, despite the crisis, trains others and makes them surpass themselves. **For this, they will need anticipation, adaptation, understanding of the issues, humility, fortitude and of course feedback from experience.** Finally, **resolutely innovative**, they move forward by taking into account new technologies and digitalization. Because they know that security has become a differentiator for the benefit of the company's growth. ■

# RECOM > MENDATIONS

- > As a manager, the Security Director must be exemplary.
- > Able to reflect and to act, the Security Director must demonstrate the ability to adapt, take a step back be wise and smart about the situation.
- > The Security Director must not remain in the shadows within the company, they must be known and above all recognized.
- > As a business partner, the Security Director must fully know how the company operates, and show resilience and creativity.

### THE CREATION OF A SECURITY DEPARTMENT IN 2022: THE RECENT EXAMPLE OF PERNOD RICARD

#### SERGE COLLIGNON

*Security Director of the Pernod Ricard Group*

Pragmatism, openness and agility are the key words when creating a security department within a corporate business, especially when it comes to a large international group like Pernod Ricard, a leader in its sector.

joined the Pernod Ricard headquarters in 2018, which was then one of the last CAC 40 companies not to have a security department. However, these issues were not absent from the concerns of the general management of this flagship of the French economy, which has always ensured strict compliance with its obligations in this area. In fact, a company like Pernod Ricard, the world's number two in wines and spirits, with nearly 19,000 employees in more than 86 countries, is regularly confronted with security issues. Nevertheless, as a family-owned and decentralized company, these functions are very present in Pernod Ricard's organization, but the group did not have a central, corporate vision.

In fact, the head of Security who sets up this new function within a group of this scale does not assume the costume of a revolutionary. They must put themselves at the service of the other departments, meet with all those responsible for them and start patiently mapping out all the measures or policies that are already effective, as well as those that must be effective in the future.

The head office, which represents less than 3% of the workforce, is responsible for defining the strategy. The more than 80 direct subsidiaries around the world are made up of six major brand companies in charge of manufacturing our products (Chivas Brothers in London, Irish Distillers in Dublin, the Absolut Company in Sweden, Winemaker in Australia, Havana Club in Cuba and Martell/Mumm/Perrier Jouët in France), which will then be distributed by our market companies from the United States to Japan, via Mozambique. Due to this great cultural and geographical diversity and in the absence of a Security Director for the Group and common rules, there are great disparities in the solutions and practices that had been implemented (or not) in all these subsidiaries.

### **CREATING THE FUNCTION, MAKING YOURSELF KNOWN AND RECOGNIZED**

---

The Security Director must clearly explain the importance of these issues and embody its various components, often divided between different departments, sometimes perceived only as constraints with a kind of ambiguity over the concepts of Safety and Security. The goal of the new security role is therefore to rationalize these policies, to make them more explicit in order to instil this culture of security. Indeed, a company in the agri-food sector, which is not an OIV [Organisation of Vital Interest], may falsely consider that it is immune to certain issues such as data theft. However, a large, listed group such as Pernod Ricard, which has jewels in its brand portfolio and has recorded solid performances, can only arouse curiosities, including malicious ones. Hence why it must protect its interests.

Highlighting the role and making oneself known is thus the first challenge. In this regard, assigning the role to a member of the Executive Board, in the person of the Director of Human Resources Cédric Ramat, and the proximity of the General Management were decisive for quickly meeting with the main leaders of the group during their visit to the headquarters. If the COVID health crisis was subsequently a catalyst, it also accelerated the integration of a security department by directly contributing to securing mask supplies.

Because the second primary challenge is to be recognized and to provide added value in the form of help or concrete support to the problems encountered by subsidiaries. This is certainly a positioning for the benefit of the “customer” (“consumer centric”) according to Pernod Ricard’s internal terminology). This requires a certain agility to identify and collect needs, considering local specificities. Availability and reactivity are therefore paramount in decision-making. On the other hand, one of my daily great satisfactions lies in the diversity of exchanges, since I interact with almost all the entities of the group and on a tremendous variety of topics.

In order not to get swamped by challenges, it is necessary to distinguish long term from short term, to discern what is important from what is urgent: divide your action between the creation of the position and the response to emergencies, carefully filling the deficiencies as soon as they are identified, while not forgetting to monitor crises over time.

### **RECONSIDER YOUR ROLE AND YOUR FIELD OF COMPETENCE AT ALL TIMES**

---

Building your mission statement is therefore an exceptional opportunity and an exciting experience that requires you to constantly reconsider your role within the company and your area of expertise. After only two years, my scope has evolved considerably compared to the roadmap I had proposed when I was recruited. The current global situation has impacted me as much as all my counterparts around the world; the COVID crisis has of course changed the initial priorities as it has profoundly reconfigured the - environment in which I evolve. Proof of this is the “new” need to respond primarily to the Duty of Care by contributing to the health and safety of our travellers and expatriates. Moreover, while my role initially only covered Security, it has been extended since the summer of 2021 to Health & Safety, for all non-industrial sites and subsidiaries.

Pernod Ricard's health and safety policy is one of the first priorities identified, with the ambition of being among the best in the sector. Integrating and considering H&S issues (for a significant part of the group) and for which I was not trained, is a challenge that has required a significant personal investment. Thanks to the internal support I was able to benefit from and despite the additional work generated, this expansion of my scope allowed me to strengthen the actions I had undertaken in the field of Security and to create synergies between Safety and Security. By way of illustration, the rules that apply to travellers and expatriates as well as to their management, are now included in the minimum common basis for Health & Safety policy.

In the missions of a Security Director who listens to the real needs of his company, nothing is therefore fixed. The key to success, in my opinion, lies in the ability to adapt your roadmap, which necessarily brings its share of small frustrations, but above all new opportunities and new challenges to overcome.

I will soon benefit from a reinforcement to carry out the missions entrusted to me, with two networks to animate and train, the networks of "Security referents" and the networks of contact points and "Health and Safety coordinators". With new site security procedures to be drafted and implemented, with business intelligence to be developed, the integration of new risks, the revision of crisis management models, synergies to be developed with the cybersecurity directorate, the enhancement of networks, improving the security of headquarters and events... the challenges are many and varied. In a world where risk is increasingly present and multifaceted, put to the test by the health crisis, the security department must be an integral part of the governance of a company with an international dimension. ■

# GENERAL RECOM > MENDATIONS

- > **The security department must be an integral part of the company's governance.**
- > **Rationalize existing security policies, explain them better in order to instil a culture of security.**
- > **Put yourself at the service of all departments of the company.**
- > **To highlight the role, to make oneself known and then recognized, by bringing concrete added value to subsidiaries.**
- > **Demonstrate pragmatism, openness and agility: constantly reconsider your role within the company and your area of competence.**
- > **Spread activity between the creation of the position and the response to emergencies, monitor crises over time.**

## THE NECESSARY CO-PRODUCTION OF SECURITY

### ÉMILE PEREZ

*Director of security and economic intelligence of the EDF Group  
Vice-President of the CDSE in charge of International*

In any society, as in any company, regardless of its size and nature, the Security function is paramount. Security (or safety on the acceptances of the terms) means **protecting the company's assets against any malicious act.**

**A**nd the wealth of a company is always incredibly diverse: its human assets, first and foremost, its greatest wealth, the people who make up the lifeblood of the company; its real estate assets; its intangible assets, its know-how, its information; its production, its commercial and financial activity...

### FACING THE THREAT...

It's about protecting all of that **against risks and threats** of all kinds and impacts, wherever they come from. The company could be the target of attacks by individuals, competitors, terrorist or criminal organisations, or governments. More than ever, the expression of this threat can take on more of a dangerous or pernicious character, **cyber-attacks**, themselves of criminal, terrorist, or state origin.

It's not just a movie script, it's everyday life.

Companies remain a potential target, or a place of expression for these phenomena of radicalization or criminalization, with all the consequences it can have in terms of image and social or financial cost.

In short, this threat is global. But malicious, criminal or terrorist activity always translates to the local level. This is what I call **GLOCALIZATION**. It is always happening somewhere in France or in the world. And this can impact the interests of the company, our interests, wherever they are. Therefore, it is necessary to **be ready at all times and everywhere** where our company is represented. Especially internationally when our agents, expatriates or on assignment, are far from their base.

**And let's never forget that the same is true for the public Security function provided by various state services.**

The security that we all then implement, in compliance with laws and regulations, as well as with our own prerogatives, must allow us to **anticipate and prevent** these risks and threats.

**Security must also be glocal:** global to perfectly cover all our interests, our total assets in the face of all threats; and local to be perfectly adapted to the level of the field. Otherwise, we risk paralyzing our own business.

**In addition to the necessary awareness-raising or internal training actions to develop a genuine security culture, it is therefore necessary to strengthen the close cooperation between the company and each of the relevant departments of the State, or private partners, both at international, national, and local levels.**

## NECESSARY IN-HOUSE CO-PRODUCTION...

Faced with the risks and threats that may affect the interests of the company, it is imperative to strengthen, or even push forward, mechanisms for prevention, deterrence, or intervention. The company alone cannot achieve this. The aim here is to develop, both internally and externally, a real company “security” net, to strengthen its networking skills in order to multiply its abilities, and to systematically organize the **sharing of information**, enabling appropriate decision-making.

For the company-state relationship to be efficient in this area, the security culture within the company still needs to be truly shared. It is necessary to mobilize everyone, and that is not always easy...

**In-house**, at the company level, the signing and implementation of an **asset security policy in the face of malicious intent in general** makes it possible to gradually evolve the “security culture” shared within each of the entities and subsidiaries. The nomination of a **manager or a correspondent for the asset security** for each of these lays down the conditions of a tight net that makes it possible to detect, as early as possible, security risks and threats.

**In terms of crisis prevention**, any company must equip itself adequately, with a global risk management and control policy, or a crisis management policy allowing situations to be controlled. Afterwards, it needs to strengthen a network system (monitoring, warning, advice, new risks, and weak signals) as well as its information-sharing practices.

**A close relationship with the Business departments** is paramount, as is clearly shown by the coordinated development of **shared security programs**.

**Based on a well-prepared warning and triggering mechanism**, the company must develop, for all departments concerned, a **strategic crisis unit** in the most diverse fields. Said mechanism needs to include systems of permanence and alert reporting, an articulation with public authorities and crisis cells at different levels and the implementation of continuity and business recovery plans (pandemics, information systems, electrical continuity, VIGIPIRATE).

In all three phases (prevention, deterrence, or intervention), the **principle of in-depth defence** is more than ever necessary. The aim here is to exploit several security techniques in order to reduce the risk when a particular security component is compromised or fails. This will make preparatory acts or attempts to commit malicious, criminal or terrorist acts more complex. Also in this area, partnership co-production is fundamental, as it is daily demonstrated by the action of certain state units within sensitive installations.

**Finally, to better prepare for the intervention, the implementation of simulation exercises and in-house and external inspections is of the utmost importance.** They make it possible to clearly determine conditions of intervention of all units concerned, and improvement measures to be taken in terms of security.

Within the company, the consideration of safety or security therefore remains an **intelligent in-house co-production affair**, in compliance with the prerogatives and obligations of everyone, including those of the Security Director.

## AND EXTERNAL CO-PRODUCTION...

**Beyond the company**, it is equally necessary to combine forces when we are all disadvantaged, in a weak situation in the face of certain risks or certain threats. We must do this all the more because the state itself can no longer do everything... and the state security monopoly is in crisis.

Regardless of the company's size, there is a driving need for **real external security co-production** with state partners as well as private security, strategic or business intelligence providers. In this same logic of networking, exchanging and sharing between peers is essential for companies, which have been mobilizing for a long time to create links in-between them, often taking advantage of the special profile of many of their security or safety directors, former civil servants of different ministries. This is how the Club of Business Security Directors (CDSE) was born in 1995, and this is how it is sustained and develops.

**First, the Company-State co-production requires complementary measures to be taken.** It is up to the company to take into account the design and operation of its installations (installation configuration, conduct, maintenance, site protection, security guard provision...), to fulfil its duty of information to public authorities, or to have a precise knowledge of the materials held for example. However, the prevention of terrorism, intelligence, site surveillance, the prohibition of overflying sensitive sites, and interventions in case of trespassing remain within the State's prerogatives.

Here again, **information sharing is essential**, and not only at the company's level. This is what we must strive to formalize as well as to develop **between companies and various state actors**: supervisory ministries where appropriate, Interior, Defence, Foreign Affairs (MEAE), General Secretariat for Defence and National Security - SGDSN, National Cybersecurity Agency of France (ANSSI), or Specialized Command for Nuclear Security (CoSSeN) depending on the sectors of activity.

A good knowledge of the state machinery is therefore most useful, as it will determine the quality of relations with state services in all aspects of asset protection. Therefore, it will not be uncommon to exchange with the public security of the police nationale, the Préfecture de police de Paris, or the gendarmerie nationale, with representatives of homeland or foreign intelligence services, the crisis and support centre of the Ministry of European and Foreign affairs, the services of embassies and other consulates, or the Direction de la coopération internationale de sécurité (DCIS)...

**To strengthen mutual trust**, it will be appropriate to detail these modes of exchange in the face of this "glocal" threat, at the local level (in France as abroad).

In compliance with laws and regulations, through screening, field exchanges, it will then be more constructive to **share information as early as possible** to better detect and counter any threat that may affect the community within or outside the company.

Indeed, the systematic development of this co-production, both for the company and for state services, will make it possible to better counter the threat, especially the terrorist threat, whether internal or external.

Gradually, each of them has understood the possibility and the need to make their goals coincide in a **win-win relationship** where the entrepreneur, or even the administration, make a commitment to accept a certain level of uncertainty, and the researcher, to ensure the realism of the recommended solutions.

Hence there was a major discussion launched in 2008 in the field of strategic training and research. Under the aegis of the **SGDSN**, coordination and mutualization are now required between ministries and large companies and have been so through the **Higher Council for Strategic Training and Research - CSFRS** which combined the work of structures such as the IHEDN or the INHES-J (now the IHEMI).

In line with these recommendations and the "*White Paper on Defence and Security*", the bodies of the industrial security sector including the **French Security Industry Sector Committee (COFIS)** and **the Council of Trust and Security Industries (CICS)**, were simultaneously formed in 2013, and merged to finally create in 2018, under the aegis of the Ministry of Industry, **the Strategic Committee of the Security Industries Sector (CSF)**. This body is a good example of co-production since it brings together offerors (large industrialists, SMEs, start-ups), customer-users, notably represented by the CDSE, and the State within its governance. But all this remains fragile, as everyone does not apprehend the **necessity for this enterprise-state sharing to become a long-term commitment**.

## BASED ON SHARED TRUST

In 2018, on the initiative of Prime Minister Edouard Philippe, the Ministry of the Interior launched a broad reflection on the “security *continuum*”, entrusted to the deputies of the majority Alice Thourot and Jean-Michel Fauvergue (also former leader of the RAID, French police tactical unit). This work was carried out in several phases: first the Thourot / Fauvergue report submitted to the Prime Minister in September 2018, then a White Paper on Homeland Security published in November 2020, a proposal for a Thourot / Fauvergue law and finally a law “*for a global security preserving freedoms*” promulgated in May 2021. The CDSE has been associated with each stage of this reflection and has thus been able to push forward **13 proposals** (see box), a good number of which - on the profession of private security guard in particular - have been included in the law.

### The 13 proposals of the CDSE as part of the reflection on the security *continuum*

#### > For a security *continuum* driven by the exchange of information

1. Facilitate public/private information exchanges in a “circle of trust”

#### > For the supervised and unashamed use of new security technologies

2. Provide biometrics and facial recognition with employment rules under the strict control of the CNIL (France’s National Commission on Informatics and Liberty)
3. Revise the technical standards for video surveillance/video protection and facilitate the interoperability of networks
4. Establish a screening of digital companies that are candidates for sensitive markets
5. Bring out a competitive “sovereign” or “trusted” cloud solution

#### > For a qualified and strengthened private security guard profession

6. Establish a financial guarantee for private security companies
7. Introduce a limitation of subcontracting at one level in private security services
8. Systematic publication of the sanctions imposed by the CNAPS for companies and managers
9. Establish a unique and high-quality uniform for private security agents
10. Establish legal protection for security guards
11. Strengthen the professionalization of the sector and the quality of training
12. Integrate fire safety into book VI of the internal security code
13. Integrate the activities of security and defence services companies into book VI of the internal security code

## I. DEFINING THE SECURITY FUNCTION IN CORPORATE BUSINESSES

### Proposal N° 1 focused on the establishment of a circle of trust to facilitate the exchange of information between the public and the private sectors:

#### Facilitate public/private information exchanges in a “circle of trust”

Since December 2018, every Saturday of the demonstration of the so-called “*Yellow Vests*” movement, the CDSE has been informed in real time of the evolution of events by the office of Paris’ Police Prefecture. This is a valuable link for companies that can best protect themselves from malicious acts that may accompany this movement.

In order to give substance to the security *continuum*, to the evolution of security professions within companies, and to the recognition of security directors as main points of contact, the State could promote this type of exchange of operational information with companies by extending it to the national territory and to more sensitive topics thanks to the establishment of a “*circle of trust*”. This would consist of “*company representatives*” subject to a prior authorization procedure or screening.

Although this proposal was adopted in the recommendations of the Thourot/Fauvergue report<sup>1</sup>, then in the conclusions of the White Paper on Homeland Security<sup>2</sup>, it was not, however, translated in the law. We can thus regret a missed opportunity, especially since this is not a new recommendation for Business Security Directors in companies: it was already included in the CDSE’s first White Paper, in 2011.

All the measures and protective actions that we put in place within the company have a double objective: **to protect and develop**. To protect our assets (starting with the human therefore) and to continue to develop our business activity without major disruption.

<sup>1</sup> “From a security continuum to a global security”, Report of the Thourot/ Fauvergue parliamentary mission, September 2018, page 58:

“Proposal 14: revaluating the role and positioning of security managers in companies:

- Create a status of Security Correspondent (SC) within companies.
- Have candidates for a Security Correspondent position approved by the CNAPS (France’s National Council for Private Security Activities).
- Opening up the possibility of empowering the holders of these roles to confidential security clearance level. [...]”.

<sup>2</sup> “White paper on internal security”, November 2020, page 155: “Business Security Directors are stakeholders in the security continuum [...]:

Proposal: strengthen the recognition of the role of Security Directors within companies in the continuum and involve them in the animation of the continuum by setting up a relationship of mutual trust sharing the secret. [...]”.



As we can see, things are moving forward with all stakeholders. But, as it is often the case regarding cooperation, progress is achieved by piling up measures according to the immediate responses to be provided to successive crises or faults. This is the case in terms of international cooperation, and it is the case for national co-production, which we all wish to strengthen in respect of everyone's prerogatives, but also in the interests of all.

**Global vision and inclusive strategy still need to be strengthened.**

Because here, the only real question for all of us remains: **what is the most important threat to the company as well as to society as a whole: the intensification of cooperation, of this necessary internal and external co-production, or the intensification of acts of terrorism, crime, or simple malice? ■**

# RECOM > MENDATIONS

## CONDITIONS FOR SUCCESS & SPECIFIC PROPOSITIONS

### Three general conditions

Among the conditions for success is this necessary co-production that I have mentioned throughout my speech. Both for its implementation and in its results, it is necessary to always emphasize on this triptych of coverage, networking, sharing.


- > 1. A strong coverage of territories, of each one's fields, and of the issues, to be able to better detect threats and risks early.
- > 2. Controlled networking that will allow us to multiply our own abilities by allowing everyone to count on it and for those who are connected in this way.
- > 3. A widespread sharing of our knowledge, expertise, and soft skills, of our relevant information.

### A specific proposal from the CDSE formulated since 2011

- > 4. Facilitate public/private information exchanges in a "circle of trust".



**II. FUNDAMENTALS  
& MISSIONS**  
OF THE SECURITY  
FUNCTION



## **THE SECURITY DIRECTOR FACING INTERNATIONAL CHALLENGES: ARNAUD KALIKA'S PERSPECTIVE (MERIDIAM)**

### **ARNAUD KALIKA**

*Corporate Security Officer at Meridiam, Chair of the CDSE's "International" commission and CDSE Administrator*

If it was necessary to find a focal point between the Bataclan attacks on 13 November 2015, the crisis in South China, the Crimea crisis and then the invasion of Ukraine by Russia, the Ethiopian mass graves, the Nagorno-Karabakh war, and the Covid-19 pandemic, it is perhaps a return/throw-back to reality. Even if these tragedies had all been anticipated by all the intelligence services of the planet, the shock coupled with the surprise of a reality marked by an extreme violence took aback even the most hardened among us. A merciless reality that is as clear as day, one which we know perfectly well might happen, even though we too often remain oblivious to its weak signals. The Security Director is the actor of reality. They are here to shake up the most cautious, in the face of the upcoming threats, in order to anticipate and to prepare solutions.

**T**he entrenchment of terrorist acts by ever more creative perpetrators of violence is an obvious fact that constitutes the brazen thread of insecurity in the 21<sup>st</sup> century. The simplifications of the world cleverly distilled in the wake of the dissolution of the USSR have fizzled out: we

all know that what we are experiencing is very different from what a handful of salon intellectuals were able to sell through "the end of History" or the "clash of civilizations". The world has left the straitjacket of concepts to become one with the Braudelian (cf. Fernand Braudel) concrete. A difficult reality that puts the Security Director to the test. They can no longer simply be stooge of a CEO in search of notoriety; they must get their hands dirty to become, in a way, the life insurance for the economic development of the company, from the safety of expatriates through reputational risk and the protection of its tangible and intangible assets.

### **GEOPOLITICAL RISK & ECONOMIC DEVELOPMENT: A FORCED MARRIAGE**

In the company's ecosystem, there are those who consider that the signing of a deal takes precedence over the rest, relegating the support functions that include "security" to a role of figurehead, or even "court jester". However, the box is ticked for the ISO standard since the Security Director was, at one time, in the loop. Such a vision of development makes the Security Director a simple cost centre, a troublemaker that should be "neutralized" administratively.

Of course, such an approach is a primary mistake, like that of a beginner chess player who falls into the trap of the "Scholar's Mate". In the Anthropocene Epoch, sustainable finance and responsible markets, the only companies that will survive will be those that embrace the long-term vision and position security as a pivot for development.

This "pivot" Security Director benefits from a 360-degree vision to better de-risk in the long term. In their international portfolio, geopolitical risk is their core target. Indeed, no one can now invest long-term in even innocuous geographical areas like Finland or Chile without taking into account this risk. It is up to each company and its Security Director to build, according to their own interests, a matrix and procedures producing objective indicators project by project; each scoring criterion will trigger a form of action both in anticipation and in reaction.

Geopolitical risk cannot be industrialized; it should be treated in an artisanal way that is coherent with the strategic vision of the company.

Thus, embarking on an economic project in Morocco requires a thorough examination of the Kingdom's geopolitics beforehand, proceeding from the analysis of its internal and external threats, or even a mapping of the stakeholders who matter in relation to the envisaged market. This is an analysis that can be internalized (it is usually better, but it involves hiring a Security Director who has knowledge of these kinds of topics) or outsourced. The results of the analyses are shared in a project management meeting, with the Security Director necessarily having to be involved in all developments. Information sharing is strategic because no one owns a trend or a weak signal in geopolitics.

No CEO can afford to invest a market anymore without going through the security antechamber which must de-risk its development. It is, of course, a "forced marriage" due to the pressure of globalized insecurity, but above all a marriage which one would have to be blind not to consent to.

### **INTERNATIONAL TOOLS AT THE SERVICE OF EXPATRIATES**

Investing in the international field involves, on the one hand, endowing oneself, and, on the other hand, building a network of experts. Many elements that seem abstract in appearance, but which in practice can make it possible to anticipate crises and inconveniences for expatriates.

> **GETTING EQUIPPED IN GEOPOLITICS:** the Security Director cannot afford to be held hostage by major newspapers, news agencies or Youtubers of all stripes. They must anticipate and know more than everyone else. Therefore, endowing oneself in geopolitics is first to work on oneself to get rid of all prejudices. In geopolitics, there is no place for egos, much less for theories of the "good sovereign". Unfortunately, there is no magic bullet or miracle solution in this matter. It is necessary to read as much as possible while taking notes, filling "small notebooks", delve into history, ethnology, cross perceptions, survey the terrain... It is then about knowing how to sort the wheat from the chaff among the information that arrives at our fingertips.

Not letting oneself get tied up by the knots of the infosphere and social networks where each tweet drives out the other. Often thankless, this part of the Security Director's job involves being able to isolate themselves, press the "freeze frame" button and think before delivering their views at the strategic level, or even to the CEO. In this regard, to form a team of analysts internal to the security department from diverse backgrounds (academia, political science, diplomacy, economic intelligence) with multiple and specific expertise (OSINT...) can prove to be strategic.

> **BUILDING A NETWORK OF EXPERTS:** too often, Security Directors turn to intelligence companies and other private intelligence firms for information of a geopolitical nature, while the only quality expertise in this field lies in the "think tanks", the universities and the correspondents of the French diplomatic network. We must not forbid ourselves anything because the "think tanks" affect the academic, with whom the Security Director must forge links. The "think tank" is the reservoir of experts that the company often needs but which it deprives itself of due to ignorance or prejudice. As for the diplomatic network, the Quai d'Orsay Crisis and Support Centre (CDCS) is at the service of companies, an essential support for all international risk management. When I go to a new geographical region, my first reflex is, on the geopolitical side, to make an appointment with the various deans of universities in the country in question to find out their feelings on the general situation and very often, I come out of these interviews with a wealth of information. The same applies to the diplomatic network, which you must meet on the spot, to share perceptions, fears... Step by step, the network is formed and maintained, sometimes in synergy with other divisions of the company (Public affairs, Institutional Relations...).

All the information collected constitutes the basis from which the Security Director can start working with their partners for the protection of expatriates. As soon as I have the geopolitical keys to the region of deployment of my expatriates, I can calmly consider possible security plans for all my subsidiaries. ■

# RECOM > MENDATIONS

> **Get a grip on an international topic to integrate it into the needs and strategy of the company.**

In many structures, the international is considered a distant subject, which affects human resources in the management of expatriates. The “business development” units do not share information with security and see security only as the firefighter of a possible fire, which may never happen... and when it happens, it is already too late. It is therefore a question of breaking this mechanism of isolating the Security function, in order to involve it in all the company’s projects.

> **Develop a targeted awareness cycle.**

In the international, everyone thinks they have the truth. Everyone has their own ideas about China, India, Russia, Africa... even France... but, in the end, it doesn’t lead to anything. Conducting a regular, quarterly awareness-raising session on our current developments is an excellent way to gather what is scattered.

> **Get personally involved in international topics.**

To position themselves in anticipation of crises, the Security Director must take the initiative to take ownership of the topics and show that they are a creator of value.

> **Make contact with CDCS.**

It would be unrealistic to want to do without the CDCS or without the diplomatic network, because the “France” brand hunts in packs. In order to be received by our diplomats, it is important to share information, to establish a dialogue in both directions.

> **Subscribe to country monitoring tools.**

The Security Director must work on the thematic and geographical outline of their country monitoring, according to the interests of their company. These tools can of course be subcontracted.

## CRISIS MANAGEMENT CANNOT WAIT ANY LONGER

### “CRISIS MANAGEMENT & BUSINESS CONTINUITY” COMMISSION OF THE CDSE

*This article was written under the aegis of the CDSE’s “Crisis management and Business Continuity” commission, by **Gabrielle BERTHELOT** (Kering), **Anne PICOT-PERAC** (Atos) and **Joelle RIETJENS** (EDF), under the direction of **Jean-Yves OGER**, deputy Director of Prevention and Protection of the Renault Group, and Chair of the commission.*

A recent study finds<sup>1</sup> that companies believe they are facing more crises today than they were ten years ago. With the diversification of threats and risks (cyber, terrorism, geopolitics, health...), the art of protecting companies has become a major challenge. Nowadays, most large companies have an organization dedicated to crisis management led by a team of professionals. The Covid crisis has accelerated this trend.

**T**hese past eleven years have also shown us that it is essential to “*think the unthinkable*”<sup>2</sup>. Recent major crises have very often been surprising because of their nature and their consequences. In 2009-2010, the H1N1 crisis had limited consequences for our organizations.

In 2022, the impacts of the Covid crisis are major, and affect all dimensions of the company (HR, supply chain...). The risk-based approach and a better integration of monitoring and analysis of weak signals are both keys to success in better anticipating tomorrow’s crises.

## II. FUNDAMENTALS & MISSIONS OF THE SECURITY FUNCTION

To meet these challenges, our professions have become core functions in the company’s strategic goals. Security departments play a major role in the animation of crisis measures. In their DNA lie the capacities of anticipation, reactivity, and organization that are essential for crisis management. Our activity must be even more transversal to shine throughout the ecosystem and develop all behavioural skills necessary to support Board members in crisis management.

Large-scale events that organizations have faced since 2010 have only confirmed the fundamentals-already identified-of an effective crisis management system. **Key success factors that it is essential to continue to strengthen:**

**> LEADERSHIP/COMMITMENT OF MANAGEMENT.** Nowadays, the ability to respond immediately in the event of a crisis and/or the ability to maintain operational activity under any circumstances is an imperative for all companies. It is essential that these issues are integrated into the company’s strategic plans and brought to the highest level. The involvement of management, whether prior to or during the management of real crisis situations is an indispensable prerequisite for success, mobilization, and commitment of teams.

**> PROFESSIONALIZATION/EXERCISES/FEEDBACK.** Team training and exercises are the keystone of effective crisis management. However, the preparation and training schemes often remain too marginal. They need to be strengthened, integrated into the training of all managers, including leaders, and must propose ambitious exercise scenarios. As such, feedback is fundamental. Feedback makes it possible to rethink the organization, the decision-making methods and, above all, to rely on the collective memory of events in order to be able to get things moving at high speed in a crisis situation.

<sup>1</sup> “Crisis management for resilient companies”, Deloitte, 2021.

<sup>2</sup> See article “Thinking & imagining the unthinkable, managing uncertainty”, page 127.

## II. FUNDAMENTALS & MISSIONS OF THE SECURITY FUNCTION

> **UPDATE THE BENCHMARKS.** As early as the conception of its crisis management system, the organization must integrate the maintenance of benchmarks that will be used in the event of a crisis. The benchmark is both what will serve as a support for crisis management, but also what will make it possible to measure the potential impact on the organization and to support decisions: policies, checklist, useful contacts, communication plan, business continuity plan, business recovery plan, risk mapping, list of threats and vulnerabilities, inventory and location of products and company assets, external backup of the information system...

> **DISSEMINATE A CULTURE OF CRISIS MANAGEMENT.** The most resilient structures are also the most agile, those that know how to adapt to constraints, take them into account and even create opportunities. In this objective, each employee of the organization has their role to play, each at their own level. It is therefore essential to invest in raising the awareness of all teams, beyond the actors of crisis management, and extend it to the entire ecosystem of the organization (internal and external). However, the intercultural component should not be underestimated, because while some decisions from corporate may seem legitimate and justified in times of crisis, they can then significantly complicate the organization's relations with the country in which it operates, or its local teams.

> **MONITORING.** Crises have become increasingly complex and global. Identifying weak signals and developing analysis on identified risks will help companies to better anticipate crises. Recent examples such as Covid-19 or the shortage of semiconductors perfectly illustrate the need to set up a robust monitoring system very early to facilitate decision-making.

> **ABILITY TO ANTICIPATE IN CRISIS.** The complexity of our world and the interdependent relationships between large systems make it difficult to predict both potential sources of crisis and the dynamics of their amplification. But the greater the unpredictability of events, the greater the need to anticipate potential impacts on organizations. Nowadays, the establishment of anticipation units meets a vital need of organizations to support strategic management in crisis.

> **PUBLIC/ PRIVATE COORDINATION, FOR A SIMPLIFICATION OF EXCHANGES.** The complexity of interdependencies and the increasing competence of crisis organizations reinforce the need for exchanges between actors. In a crisis, information is key! In order to respond to the multiplicity of the economic actors concerned, it is important that privileged and unified channels of information exchange between state services and companies be defined, in a "one-stop shop" logic: this would allow efficiency, reliability, equal access and information sharing.

> **CLARIFY THE PERIMETERS.** In the 9001 or 27001 standards, it is a question of "*knowing how to address stakeholders*". Having a good visibility internally and externally of the entities that can help, slow down or, on the contrary, disrupt the recovery and the return to normal must make it possible to anticipate reactions. Depending on the organization, there may be a local level (site, country, geographical region, market divisions, department...) and a global level. For each stakeholder, it is necessary to define who within the crisis organization oversees the actions and fuels the relationship. The question is not "*who does what?*" but "*who reports to who?*"

> **CAPITALIZE ON DIGITAL TOOLS.** More and more digital tools are being developed to save precious time for crisis teams and increase their efficiency as well as the traceability of actions carried out. The COVID crisis has been an accelerator of the transformation towards virtual or hybrid crisis spaces. On the other hand, it is necessary to take into account the time required for implementation, configuration, training, the overall cost, and the adherence of the teams especially if these tools are dedicated solely to crisis situations. Particular attention should be paid to the dependence on these tools, as they can become a risk for the organization in the event of malfunctions, data leaks, etc...

> **GLOBAL AND SYSTEMIC CRISES.** Covid-19 pandemic has given an overview of a global, systemic and multidimensional crisis. The diversity of the actors concerned, and their interconnections complicate the response, and each decision has repercussions on other actors. It is imperative to collectively prepare to face these future large-scale events. This makes it possible to better know one's abilities as well as their limits, and potentially to create synergy.

**Faced with the complexity of crises, the response now must be collective: all companies, all sectors of activity combined, have an essential role to play.** Through this approach of structuring and rationalizing the crisis management system, but also raising awareness among their employees, customers, partners, through closer public / private cooperation, companies can be valuable contributors to the dissemination of a crisis culture among populations. Through this action, organizations can also strengthen their relations with public authorities in the countries in which they operate. Because they ultimately contribute to the resilience of civil society. ■

# GENERAL RECOM > MENDATIONS

- > Strengthen crisis preparedness work through risk analysis and the development of a monitoring mechanism.
- > Appoint a crisis management and business continuity manager within each entity.
- > Disseminate the crisis culture throughout the company's broader ecosystem.
- > Train and practice for the crisis collectively (with all the internal and external actors concerned).
- > Using digital tools in crisis involves providing alternative workarounds, with particular attention to data security.
- > Expand public/private cooperation and consider all economic actors / sectors of activity essential to the resilience of the Nation.



## ESSENTIAL PLAYERS IN THE SECURITY CONTINUUM FOR A RESPONSIBLE PURCHASER & A QUALITY PRIVATE SECURITY

### THE “PRIVATE SECURITY” COMMISSION OF THE CDSE

This article was written under the aegis of the “Private Security” commission of the CDSE by **Claire NICLAUSE**, head of Private Security at RATP, and **Christian CREMEL**, Security Director of the Bouygues Group and Chair of the commission.

The Company remains confronted with ever-changing threats. It must protect its rights of way, its products, or its reputation in the face of multiple risks and meet the safety expectations of both its employees and its customers. For a long time seen as a cost to the Company, expenditure on security is now gaining to be perceived through the prism of the “avoided cost”, as an investment with a certain profitability, a value, and a competitive advantage, in the same way as the requirements related to corporate social responsibility (CSR).

In order to meet this security responsibility and ensure the smooth running of their economic activities, companies and their Business Security Directors are experiencing an increasing need for private security services. In 2020, 79% of the turnover of companies providing private security was provided by private orders, compared to 21% for public orders<sup>1</sup>. As such, as the main “purchasers” of security providers, the Business and its Security Directors, constitute an essential link in the security *continuum*.

### BETTER BIDDER VS. LOWEST BIDDER THE ROLE OF THE BUSINESS SECURITY DIRECTOR IN THE PURCHASE OF PRIVATE SECURITY

The role of the security departments is essential in the purchase of security services. Thanks to their expertise and experience, the Security Director appears to be able to influence the choices of their company in all phases of the tender leading to the choice of the service provider.

However, they must work in direct liaison with the “Purchasing” departments, whose temptation might be to turn to the “lowest bidder”, where it is absolutely necessary to favor the “better bidder”.

In its Technical Guide entitled “*La prestation de gardiennage : le guide du donneur d'ordre*” [“*Security services: Guide for the contracting authority*”] (The CDSE Technical Booklets, January 2020), the CDSE recommends respecting a fair balance between the qualitative requirements imposed by the operational staff and budgetary constraints. If all the stakeholders contribute to the success of the tender, the pairing of the “Purchasing” and “Security” functions probably appears to be the most coherent tandem to manage this process. This does not mean that costs are the overriding criteria, but that the synergy between the business competence and the purchasing process competence remains essential for the smooth running of the tender:

> **In the preparation phase of the tender**, it is a question of forming a project team that is balanced between the different corporate functions, in order to define very precisely the needs of the client. The “Security” function, thanks to its knowledge of the sector, facilitates the quantitative and qualitative analysis of market players.

> **In the phase of identification of technically admissible tenders**, after publication of the call for tenders, the security department must clearly decide on the restrictions, or even exclusions, with regard to certain tenderers whose quality does not appear to be at the required level. This step helps to avoid an irrelevant financial negotiation. It is appropriate here to rule out an abnormally low offer, i.e., one which is clearly out of step with the others.

## II. FUNDAMENTALS & MISSIONS OF THE SECURITY FUNCTION

<sup>1</sup> E2021 Prevention & Security branch survey on 2020 data (Xerfi Spécific).

> **In the contract award phase**, basis only on the cost, i.e. “the lowest bidder”, is strongly discouraged, because it generates several high-level risks in terms of the service quality : internal control of the provider, local management, non-payment of social and employer charges, concealed work, illegal work or non-compliance with current legislation, insufficient training of staff, failure of the provider... Note that during the checks conducted by the CNAPS (France’s National Council for Private Security Activities), “*findings likely to constitute criminal offences (concealed employment...)* are the subject of a report to the Public Prosecutor on the basis of Article 40 of the Code of Criminal Procedure”. In this context, “*the co-responsibility of the client can be criminally retained*”<sup>2</sup>.

> **In the financial negotiation phase**, the “*Purchasing*” function takes the lead in negotiating with all technically valid bidders. They can thus retain the “*better bidding*” service provider.

The Law of May 25, 2021 “*for a global security preserving freedom*” establishes a framework regarding subcontracting for private security activities: a service cannot be fully subcontracted, and the first-tier subcontractor can only subcontract himself if they justify the absence of know-how, lack of technical means/capabilities, or a one-time shortage of staff. The main contractor must validate this justification. Then, the purchaser must verify that the main contractor has validated this reason for using subcontracting. The second-tier subcontractor may not subcontract for any reason.

In this regard, the CDSE recommends that the purchaser compel the main contractor to provide them with a written certificate confirming that the latter has validated the reason for using subcontracting. More generally, the CDSE recommends prohibiting the use of subcontracting, considering the risks it entails (quality of services, compliance, relationship between client and service provider...). If, however, this process proves necessary (occasionally and by way of derogation), it should be properly supervised to maintain control over it.

For all these reasons, and in order to perpetuate win-win relationships with private security providers, contractors need to build a more fluid relationship with the CNAPS (France’s National Council for Private Security Activities), in order to work together and request the advisory mission of the public regulatory institution of the sector.

### THE EXPECTATIONS OF CONTRACTORS IN TERMS OF QUALITY OF SERVICE

To meet all its security challenges, the Company must be able to rely on private security companies that are at the forefront of providing quality services. While France is on the verge of two major events on an international scale, with the Rugby World Cup 2023 and the Olympic and Paralympic Games in Paris 2024, the CDSE considers that it is becoming more necessary than ever to strengthen the professionalization of the sector and the quality of agent training. In addition, needs of companies are constantly evolving and must be taken into account, especially with regard to the rise of violent forms of protest (activism and social movements) requiring expertise in crowd management and behavioural analysis.

The law “*for a global security preserving freedoms*” has already tightened the conditions for access to the profession and plans to reform by ordinance, by 2023, the modalities of training, examination and obtaining professional certifications as well as the control of private security training activities. This is an unmissable opportunity to upgrade the skills of private security agents through initial training redefined in consultation with the professional branch of prevention and security companies (employers’ organizations and employee unions) around a robust common base and additional skill blocks in line with the concrete missions of agents in the field and the needs of clients.

This reform must also lead to the emergence of proper intermediate management with the operational qualifications and human qualities required to exercise this function. Such a restructuration of the sector around skills, expertise, missions and supervision is the real mark of quality human surveillance provisions, involving remuneration re-evaluated accordingly for a sector that will increase in attractiveness.

<sup>2</sup> [www.cnaps.interieur.gouv.fr/Vos-demarches/Vous-souhaitez-acheter-une-prestation-de-securite-privee](https://www.cnaps.interieur.gouv.fr/Vos-demarches/Vous-souhaitez-acheter-une-prestation-de-securite-privee)

## II. FUNDAMENTALS & MISSIONS OF THE SECURITY FUNCTION

### STRENGTHENING THE ROLE OF THE COMPANY & PRIVATE SECURITY IN THE CONTINUUM

Private security and the Company constitute “*the third security force of our country*” affirmed the Minister of the Interior, Gérald Darmanin, Thursday, 16 December 2021, during the annual colloquium of the CDSE. Nevertheless, private security in France still suffers from an image deficit that has yet to be filled. In this regard, several notable advances - called for by the CDSE in its various contributions to national reflections on the *continuum* - are to be credited to the law “*for a global security preserving freedoms*”: this text establishes legal protection for security agents, identification elements on their uniforms, or the exceptional authorization of missions on public roads against terrorist acts that could target the property in their custody. One last point that is particularly structuring for the *continuum* still needs to be clarified, especially in the perspective of the Rugby World Cup and the 2024 Olympic Games, namely the development of a real doctrine for the use of private security with regards to its interactions with law enforcement agencies in crowd management during major events.

From an economic point of view, the limitation of subcontracting mentioned above provides a first guarantee in terms of more virtuous practices in the sector. This makes it possible to reduce the risk of dumping inherent in the phenomenon of cascade subcontracting. Nevertheless, an additional effort in terms of economic regulation is still needed: **the establishment of a financial guarantee-type mechanism**. This measure, which has been a consensus between contractors and service providers since 2018 (GES<sup>3</sup> and CDSE), would make it possible to ensure the financial capabilities of private security companies and the willingness of their managers to take a sustainable and responsible role in this market. The 2023 Rugby World Cup and the 2024 Paris Olympics require the private security sector to be more economically robust and less atomized, an essential prerequisite for the increase in the competence of agents and a better quality of service, as pointed out by the Court of Auditors in its 2018 annual public report<sup>4</sup>. Such a mechanism has proven itself in other regulated sectors (travel agencies, real estate agencies, temporary work companies...) and would make it possible to definitively install private security as an indisputable player in the security *continuum*.

Private security agents, as first responders, are valuable sensors of weak signals and the materialization of the threat. The latter report to the purchaser, the Security Director who, if necessary, ensures the transmission of information to the public authority. It seems necessary to promote such a sharing of information, and in return to allow the public to transmit to the private in a relationship of trust. As such, Business Security Directors are an essential vector, a pivot between the private and the public. That is why the CDSE has been advocating since 2011 for the creation of a “**circle of trust**” establishing Security Directors as privileged interlocutors of the law enforcement and the State in the Company. A “**security contact**” who would have been subjected to a prior authorization procedure or screening allowing information to be shared, both in terms of public order and more sensitive topics. A measure of this kind would definitively give substance to the security *continuum*. ■

<sup>3</sup> Joint press release SNES, USP (since merged into the Groupement des entreprises de sécurité - GES) and CDSE in favour of a renewed economic regulation allowing a sustainable functioning of the private security market (15 October 2018).

<sup>4</sup> Court of Auditors - 2018 Annual Public Report (February 2018) - Chapter 2, “*Private security activities: an increasing contribution to public security, insufficient regulation*”.

# RECOM > MENDATIONS

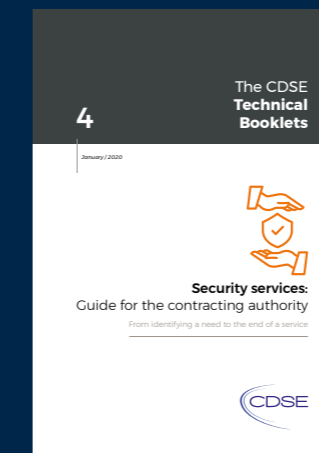
## WITH REGARD TO PUBLIC AUTHORITIES

### > Reform professional training in private security:

- By upgrading the skills of private security agents through a redefined initial training in consultation with the professional branch of prevention and security companies (employers' organizations and employee unions).
- By building a robust common base and additional skill blocks in line with the concrete missions of agents in the field and the needs of clients.
- By creating the professional role of private security supervisor.

### > Establish a financial guarantee-type mechanism for private security companies.

- > Facilitate exchanges between the purchasers and the CNAPS, especially within the framework of the advisory mission of the public regulatory institution of the sector.
- > Create a public-private "circle of trust" establishing Security Directors as key players in the security *continuum* and privileged interlocutors of the law enforcement and the State in the Company.



To consult the CDSE technical booklet "*Security services: Guide for the contracting authority*" (available in English)

- **If you are a member of the CDSE:**
  - Visit your members' area "Mon CDSE"
  - > "Boîte à outils" tab
  - > "Les publications du CDSE"
  - > "Les cahiers techniques du CDSE."
- **If you are not a member of the CDSE:**
  - [contact@cdse.fr](mailto:contact@cdse.fr)

## THE SECURITY DIRECTORS & CORPORATE CYBERSECURITY ISSUES

### JEAN-PAUL BONNET

Chief Security Officer of the k Group  
Chair of the CDSE's "Cybersecurity & information security commission and CDSE Administrator

Almost everything has already been said about the security of the digitized world and to have a chance at capturing people's attention, it is better to use the term "cybersecurity", even if the term cyber safety would be more appropriate. At admittedly different levels, the resilience of CDSE member companies depends globally, if not almost entirely on the security of the digital world: cybersecurity. In the same way as it depends on the good management of its resources, the competence of its commercial forces, the quality of its products and services...

**W**hy is there a need to come back to the topic again and again? Perhaps because some obvious things need to be regularly reminded in **a field that is evolving at such a speed that no one can claim to master the entire subject.** Including the most cutting-edge experts. Is it then enough to state that human, organizational, and technical means make it possible to deal with the topic? This is the beginning of an answer, but it is not enough.

### THE ONLY GOOD ORGANIZATION IS ONE THAT WORKS

It is preferable to refrain from asserting peremptorily that the ideal organizational model to be set up within the company to tackle the topic is universal. **The only good organization is one that works depending on available resources, the sector of activity, the history and experience of the company and its managers.** To try and define a typical organization, where the company's information systems security lies in the Security Director's hands or not, is illusory. At best, some models can be described, with their advantages and disadvantages, but **it is up to the managers to choose the one that seems most appropriate to them.** And to be able to ask the question regularly about the distribution of missions between the different lines of defence of the company in the face of this risk.

Some have called our world volatile, uncertain, complex, ambiguous. It is this perspective that should drive the action of a Security Director, especially in the field of cybersecurity. Whether it is **qualified as global or systemic**, their approach allows them to apprehend complex interdependencies and relationships with an open and agile mind, to value the sum of specific expertise that, in isolation, are soon limited. Is the priority knowing who reports to whom? **The priority is ensuring that the company's security objectives have been defined as a whole, that threats are identified and that the risks, formally accepted by managers aware of the actions undertaken or to be initiated, remain at the established tolerable risk level.**

From this virtuous loop follows the process that makes it possible both to define **specific security policies** for each domain, and **to control their implementation independently.**

Each expert finds his place in this mechanism, regardless of the organizational schema chosen. **The Security Director is a major player in this.**

## II. FUNDAMENTALS & MISSIONS OF THE SECURITY FUNCTION

It is not a question of predetermining who the scapegoat in the event of a major incident will be. It is a question of ensuring that all roles are fulfilled, and missions are evenly distributed. Many recent examples have confirmed that a systemic crisis involves a systemic response. This is perfectly suited to the security of companies whose digitized processes expose them to attacks on an increasingly large area while their ability to defend themselves largely depends on their ecosystem and their partners.

### **A CYBERWAR IS WELL UNDERWAY**

The feeling of helplessness that may have taken hold of some victims of major attacks on their information systems should prompt us to put forward **the fundamentals of a global approach, phases of which are well detailed in related international standards** (ISO27K family of standards, NIS Directive, NIST Cybersecurity framework...). **It tends to guarantee the essential security of both tangible and intangible assets, the convergence of which is illustrated by the omni presence of the Internet in everyday life, professional or personal.** Awareness-raising and training in reflex actions or barrier gestures of cybersecurity must therefore begin at an early age. **Throughout professional life, regular reminders adapted to the activities of everyone should be organized by the competent experts.**

Nevertheless, it is not debatable that there are, and will be, many victims on the digital battlefield. Should we accept or reject this warrior vocabulary? Whether it is larvae, cold again, asymmetrical or irregular, **a cyberwar is well underway.** The marketing term does not change the observation, this cyberspace created by humans and enriched by humans is also diverted from its initial objectives by humans to fight their battles there. And the company constantly operates in this digital operating theatre, sometimes in a still surprising denial of reality, especially on the topic of organized cybercrime linked to UN member states or that of industrialized espionage, including between close allies. Therefore, the company constantly runs the risk of being **collateral damage from a fight in which it does not partake directly** but amid which it evolves and exposes itself with more or less protection, out of naivety or denial.

### **BEHIND THE CYBER, THERE IS ABOVE ALL THE HUMAN**

**Because everything is really a story of human behaviour.** Both on the defence and attack side. The offensive technical skill only serves as a lever for a human intention. Which will benefit from the inattention or defensive technical incompetence of another human being.

The benefit of the digital revolution and all the progress it brings is therefore at hand **if security concepts, especially digital ones, are integrated from the very beginning to any approach within the company,** if they are included in profitability calculations, both in choosing which cybersecurity solutions to use, and in defining processes and associated human behaviours, as an inseparable evidence of the success of this activity's life cycle. **If security is integrated a posteriori, then it represents a disturbing constraint and additional cost, which are therefore bypassed or even rejected.**

The sovereignty of the company has a price, that of its ability to limit malicious digital interference in achieving its goals. And since interdependencies are becoming greater and greater between actors in the same ecosystem, by strengthening its cybersecurity position, each company contributes to strengthening that of its partners and its environment, in a responsible approach. Which company would specify in its mission statement that it intends to contribute to the development of a less secure world, by being the weakest link in its environment? What company would not care whether its external partners who connect to its information systems have previously secured their own systems? ■

# RECOM > MENDATIONS

- > Adopt a systemic approach.
- > Ensure that the company's security objectives, which have been defined by managers aware of the actions undertaken or to be initiated, remain at the established tolerable risk level.
- > Define policies and set up an independent monitoring system for their implementation.
- > Continuously train and raise awareness.
- > It is all about human behaviour, not techniques.
- > Each individual/company contributes to the cybersecurity of its ecosystem and relies on others.

## STRATEGIC AND COMPETITIVE INTELLIGENCE, A VECTOR OF ASSET ENHANCEMENT

### STRATEGIC AND COMPETITIVE INTELLIGENCE COMMISSION OF THE CDSE

*This article was written under the aegis of the CDSE's "Strategic and competitive intelligence" commission by **Fabien LAURENÇON** (associate researcher at IRSEM), under the direction of **Jean-Louis KIBORT**, Security Director of the L'Oréal Group, Chair of the commission, and CDSE Administrator.*

Strategic and competitive intelligence (SCI) is conceived as a key link in the sustainability of organizations. Since 2020, the COVID-19 crisis has initiated an in-depth reflection on the concept of sovereignty while it appears that the world is entering a new cold war, which pits China against the United States. For companies, it is a question of enhancing material and intangible assets previously considered peripheral, therefore relocatable, and questioning risks and opportunities of our interdependencies.

**B**ased on this observation, the SCI commission of the CDSE has oriented its work around the crucial need to "rethink the notion of value". To this extent, what are the alternative ways of enhancing a company? How can SCI implement them? How can we protect this value creation?

### EXPANDING THE ENHANCEMENT LEVERS

The value of an asset, whether it is intangible (patent for example) or material (production site, laboratory), is still widely understood from the financial perspective and from a short-term strategy. Rather than automatically reselling a patent or a dormant patent portfolio, or selling a site, it is now crucial to think about different long-term strategies to identify other positive externalities. In March 2021, the end announced by the French State of the so-called “whatever it costs” measures<sup>1</sup>, leads companies, in a strategic logic, to think about other modes of partnerships that can be substituted for financing solutions (Loan guaranteed by the State, Future Investment Program...). SCI, in a long-term vision supported by its “influence” pillar, has the mission of strengthening reputational enhancement (enhancing the brand image<sup>2</sup>) of the organization and its assets.

SCI can therefore help to rethink the societal and political value of companies and their resources. The maritime transport crisis (shortage of certain strategic equipment, rise in costs of raw materials and their repercussions...) has accelerated awareness of the limits of our consumption patterns and the overall cost of these practices. Whenever possible, the creation of local, territorial, or national value – which is imposed as a fundamental expectation of consumers – should be prioritised. Consumer behaviour is a central variable, which is the target of SCI.

### PROTECTING KNOWLEDGE & HUMAN VECTORS OF INNOVATION

The crisis has highlighted, at all levels, the decisive action of the human factor: medical personnel, researchers mobilized on accelerated vaccine development programs, mass distribution professions.

In the case of researchers, priority must be given to the protection, monitoring, and promotion of high potentials. SCI plays its full role here by detecting high potentials, whether in public or private R&D&I, by accompanying their protection against all forms of meddling by third parties (poaching, espionage,

manipulation, destabilization...), alongside Human Resources departments and IT security experts. Innovation incubators and ecosystems, which constitute the next key stage, that of the transition from scientific discovery to its industrialization, must be protected in the same way, whether they are employees of a large cybersecurity company or a private subsidiary under public service delegation specializing in health innovation, by going beyond the existing legal tools (patents, intellectual property), which have advantages as well as limitations.

The economic war is first and foremost a war of intelligences as well as a race for scientific knowledge and disruptive innovation. It is thus conceivable to apprehend protection and assistance measures according to three concentric circles of enhancement and different types of assets (goods, services, knowledge/know-how, research including basic research), which call for three levels of economic security:

#### > CIRCLE 1: strategic assets, essential for the survival of the country.

Complete control of the sector by companies located on the national territory and with state-controlled capital in which operational decisions can only be taken by a person of French nationality authorized by the State (nuclear deterrence, cyber...). The mobilization of dedicated state services is carried out with the assistance of the companies' SCI to protect these assets. Independence is defined as the ability to maintain one's freedom and autonomy in decision-making: the electro-nuclear sector, electronic components and technological locks (semiconductors, Internet literacy, etc.), cryptology, certain industrial flagships or even certain luxury and cultural activities, which France is famous for, are among these key sectors.

<sup>1</sup> The set of economic measures to support companies and organizations deployed by the French State during the Covid-19 crisis.

<sup>2</sup> We have seen the damage in Australia of the work of undermining and methodical denigration carried out for five years by the domestic opposition (part of the local political class) and competitors from Germany (TKMS) and Sweden (Saab) against the Attack program, despite the technological excellence of the French proposal and the strength of the strategic partnership proposed at bilateral level.



## II. FUNDAMENTALS & MISSIONS OF THE SECURITY FUNCTION

### > **CIRCLE 2: fundamental assets essential for the business continuity of the country and its inhabitants in the medium and long term (OIV - Organizations of vital importance and OSE - Operators of essential services).**

The activity of these companies (hydrogen production, consumer electronics, food processing, transport, medicines, space...) should be in one of the EU countries with one of these countries monitoring its operational decisions and its capital. It is therefore necessary to promote a European regulation allowing this approach and a development of the R&D&I *continuum*. These companies make it possible to build national independence within European interdependence. As such, they must be valued, in a logic of creation of a European industrial, scientific, and technological base<sup>4</sup> (BISTE), goods, services and fields of science mentioned above (also agriculture and food security), on the basis of the acceptance of mutual or cross-dependence between Member States' economies.

### > **CIRCLE 3: non-strategic assets, not OIV or OSE, which can be located outside the EU, but whose relocation can generate positive benefits for the territory or the State, or for the strengthening of circles 1 and 2.**

For CDSE member companies, this interdependence has been a reality for a long time. It is a question of quickly being able to produce or replenish a production capacity on the territory of the EU. The State and the company can cede technical control while maintaining control of expertise and methods. The challenge here is to keep levers of capital control, IP (intellectual property) or others within a time compatible with the impact of an embargo imposed on us by an aggressive state on these areas, or for which the French state or the company would be willing to give up.

These sectors are poorly covered or poorly known by state services, which do not always have the necessary expertise (for example on the topics of AI, quantum, and hydrogen [circle 1], smart cities [circle 2] or chemistry [circle 3]. Providing experts from companies and research for the benefit of the State (for example in standardization bodies) could be another area of enhancement. What is interesting about a patent is not the proceeds from its sale and the immediate but limited financial gain, but rather the medium and long-term benefits on a given territory through job creation, tax revenues and the negotiated maintenance of a scientific activity on the territory.

It is up to the State to set its priorities for the three reading grids, in interaction with the EU at its level [circle 2 & circle 3], and of course to companies for these three levels of assets, in interaction with Brussels and the State from which it comes. The case of cloud, cyber, or hydrogen strategies are levers to promote a European market.

Only the European Commission can finance a ten-year programme for a specific sector, such as for autonomy on electronic chips. But France, for reasons of deterrence, might require complementary controls, which would then be financed by the country alone on specific sub-segments (high-power lasers, genomic research, CBN protection) in a strategy of technological and scientific barriers.

### **In the latter case, a Union-wide economic security strategy, which opens a dizzying field of topics, could be based on two pillars:**

- Harmonizing economic security practices (for example the PPST - Protection of the scientific and technical potential of the nation) between ministries of Member States to strengthen entry control mechanisms (in the mode of IEF<sup>5</sup>). This approach is now theoretical, but the evolution of the European Commission is a positive sign<sup>6</sup>.
- Exchanging good practices between professional federations: since 2018, the CDSE has initiated several contacts with its German counterpart of the ASW (Akademie für Sicherheit und Wirtschaft). Further contacts could be deepened with Italy and Spain. The SCI commission could play a leading role in bringing together the actors of safety and security in Europe, complementary to the action of the States<sup>7</sup>.

<sup>4</sup> The notion joins the call from the President of the Commission in favour of European defense sovereignty.

<sup>5</sup> Monitoring system for "Foreign investments in France".

<sup>6</sup> Within the CDSE, an inter-commission approach in partnership with the "Fraud & Compliance" commission deserves to be studied.

<sup>7</sup> While remaining attentive to the introduction of new rules and standards by a State for the benefit of its stakeholders.

## CONCLUSION

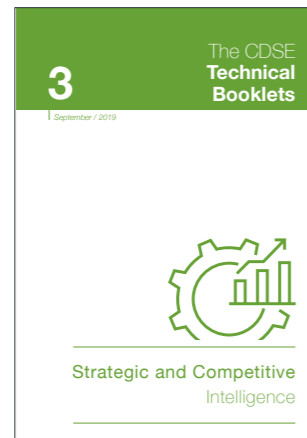
SCI has its place in the deployment of this arsenal of sovereignty, of which it is only one link among other functions of the organization.

In the face of an ever-changing and hardening business environment, sovereignty is a guarantee of the resilience of the state as well as companies.

This **resilience** is not synonymous with passivity. It is also important to think about our means of “retaliation”: what are our opponents’ weaknesses? As part of this **offensive strategy**, let’s not forbid ourselves from mapping the weaknesses and strengths of our competitors, each in its own field and with its own resources: the State has its sovereign means, with its specialized services, and it’s up to companies to define their own vulnerabilities, in their sector, in the face of their competitors.

This knowledge of our strengths and weaknesses is not static, it must adapt to ever-changing ecosystems, for research, business, and the State, which are called to work together.

This coordination/cooperation between institutional and private actors is the key to our **sovereignty**, and to the **influence/outreach** of our country. ■



To consult the CDSE technical booklet  
“*Strategic and competitive intelligence*”  
(available in English)

- **If you are a member of the CDSE:**  
Visit your members’ area “Mon CDSE”
  - > “Boîte à outils” tab
  - > “Les publications du CDSE”
  - > “Les cahiers techniques du CDSE”
- **If you are not a member of the CDSE:**  
contact@cdse.fr

# GENERAL RECOM > MENDATIONS

- > **Identify levers for enhancing the assets of the company and the State** through SCI in a longer-term vision at the expense of a short-term enhancement. For this, companies must be aware of the priorities of the State, the latter must avoid competition between them in favor of harmonization of value chains.
- > **The integrity of value chains makes it possible to secure strategic segments.** That is why it is necessary to identify the sensitive elements that may be located in the different circles of interest. It is essential that the State can rely on research experts and companies to obtain a vision integrating all the scientific and technical barriers of this value chain.
- > **Protecting knowledge and human vectors of innovation: researchers, entrepreneurs, intrapreneurs,** by asking the State to set priorities in the three circles in terms of security, based on the principle that SCI cannot protect everything, whether it is carried out by the State (economic security policy) or by the company (security department).
- > **Acting for a Union-wide economic security strategy:** conduct influence actions with Europe to share priorities with harmonization at the level of the Member States and Europe: the challenge is to build an applied and theoretical R&D, i.e., a European ecosystem ranging from research to industry (*continuum*).

## COMPLIANCE & FIGHT AGAINST FRAUD: TWO GROWTH LEVERS FOR THE BUSINESS SECURITY DIRECTOR

### RUDOLPHE PROUST

*Security Director of the Altea Group  
Chair of the CDSE's "Fraud & Compliance" commission*

In an economic context of complex and international exchanges that are increasingly digitalized, companies face ever more sophisticated fraudulent attacks, both from their more or less close external environment, and from their own employees, partners or customers.

**P**revention thus requires the implementation of a corpus of adapted rules and solid processes, or even increased resilience based on an adequate and rapid treatment of fraudulent incidents. These are the key elements for effectively combatting these attacks and minimizing both material and intangible impacts on our groups.

Likewise, the regulatory context is becoming more and more restrictive for companies (controls and sanctions). With a transversal vision, a corporate Security Director participates in the company's compliance mission, ensuring the search and response to any deviations and responding to fraudulent incidents. They take a proactive approach and propose appropriate corrective measures alongside operational services, legal services, or disciplinary bodies.

The objectives of the fight against Fraud and its corollary, Compliance, are therefore to set up effective prevention, ensure operational responsiveness in the treatment of fraud and allow permanent adaptation for the purposes of anticipating and taking into account risks by setting up appropriate internal structures and processes.

The function of a corporate Security Director is based in the organization of companies, alongside other actors according to the organizations specific to each group culture or specific regulations (legal or risk directors, internal control, and audit...). Given their areas of competence and intervention and their positioning within the structures, the Security Director has a central role to play in the implementation of both organizational and operational means to guarantee the company's compliance and ensure trust for managers and employees, as well as for all partners regardless of who they are.

### FOR A CONTINUUM OF THE FIGHT AGAINST FRAUD

The Security Director is an important link in the security *continuum*, which maintains links with various state entities, under the aegis of the Ministry of the Interior in particular. Nevertheless, the fight against fraud could require the creation of a joint working group between the state law enforcement agencies and an organization bringing together the directors of security and safety of large companies, such as the CDSE. Such a public-private body would thus make it possible to improve the consideration of the treatment of frauds suffered by companies (absence of systematic complaint filing due to expired delays, lack of knowledge of police nationale and gendarmerie nationale departments in charge of complaints for attempts or damages suffered by legal entities and non-natural persons, etc.), and improve the feedback on frauds suffered and information sharing (absolute necessity for the implementation of immediate corrective measures, implementation of preventive measures for other companies, etc.)

In this same logic, Security Directors could intervene, during exchanges or training, with the staff responsible for taking complaints and leading investigations to raise awareness of the challenges and constraints of companies when tackling fraud.

## II. FUNDAMENTALS & MISSIONS OF THE SECURITY FUNCTION

## **THE SECURITY DIRECTOR & COMPLIANCE**

The corporate security department strives to promote all measures designed to guarantee the independence of people dealing with Ethics and Compliance topics. The Security Director participates in formalizing the rules that allow most cases to be handled (code and procedures) and instigating an Ethical and Compliance culture to change practices in depth (not stopping at the deployment of new procedures). To do this, they must ensure that this culture is carried by the leaders (exemplarity and “Tone on Top”), define a training plan for all employees as well as for sensitive populations and bring this culture to life through awareness-raising and recurring communications or with newcomers as soon as they join. The role must support the reporting of questions or deficiencies via the hierarchical path or any other compliance chain (Compliance officers, deontologist, etc.). And thus, encourage employees not to remain alone when faced with a delicate situation. For this, the company must set up an alert channel, for cases that could not be reported via the hierarchical route, in order to allow the company or the organization to deal in-house with these situations.

The Security Director must take part of the responsibility for the evaluation of all third parties with whom the company or organization works, in order to protect the reputation of the latter and avoid risks of financial or other sanctions. In this context, carrying out a “blank” check with a view to being checked by an authority can be an effective initiative. The aim here is to identify the monitoring points to be reproduced in the in-house monitoring scheme, and, if necessary, to implement corrective actions.

Finally, to exercise their responsibilities in this area with complete calm, the corporate Security Director must handle alerts within a formalized framework. This is particularly the case for the framework internal investigation processes, the modalities and limits of which are precise.

It may also be useful to measure the company’s ethical culture via a barometer focusing on awareness and the level of trust in the alert system.

## **FOR A MORE GLOBAL VISION OF THE STRUGGLE AGAINST FRAUD & COMPLIANCE**

The effectiveness of the company’s protection against internal and external fraud will depend on the commitment and deployment of a culture of all business stakeholders (managers, employees, service providers, suppliers, customers). We call for a better representation of the function of the corporate Security Director in working groups within state bodies (Ministry of Economy, Ministry of the Interior, Ministry of Justice... and regulatory bodies (public authorities, administrative authorities, etc.). The interest is to “disengage” this responsibility in companies and to integrate the skills of a corporate Security Director in dealing with Fraud & Compliance.

# RECOM > MENDATIONS

- > Creation of a joint working group between state law enforcement agencies and Business Security Directors (CDSE) to improve the consideration of the treatment of fraud suffered by companies.
- > Participation of corporate Security Directors (CDSE) to the training of state personnel in charge of complaints and investigations on the challenges and constraints of companies in terms of fraud.
- > Promotion of all measures guaranteeing the independence of treatment of Ethical and Compliance topics in the company and all measures for the development of a compliance culture in the company.
- > Participation in all initiatives for monitoring the effectiveness of the system as well as measuring the ethical trust of employees.
- > Integration of Business Security Directors (CDSE) alongside the other directorates (legal, risk, audit...) as representatives of the company's interests in the field of compliance with regulatory authorities.

## PRODUCT LIFE CYCLE & SUPPLY CHAIN

### PRODUCT SAFETY, TRAFFIC & SUPPLY CHAIN: FOR A GLOBAL FIGHT AGAINST TRAFFICKING

#### EDMOND D'ARVIEU

Chief Security Officer of the Sanofi Group  
Chair of the CDSE's working group  
"Product life cycle safety and fight against counterfeiting"

Counterfeiting, illicit trafficking, embezzlement and theft of products affect all companies internationally marketing products with high added value or conveying a recognized brand image. These ever-expanding criminal activities are increasingly orchestrated by highly organized networks.

Trafficking poses serious threats to public health, in particular regarding medicines, cosmetics, food, tobacco or alcohol. Other sectors such as the toy, electrical, chemical or transport industry are also impacted, counterfeit products leading to risks of environmental pollution, electric shock, fire, or accidents. According to the WHO, the trafficking of falsified medicines alone causes the death of 100,000 to 1 million people every year<sup>1</sup>.

<sup>1</sup> Press release published on the WHO website, <https://www.who.int/fr/news/item/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified>, November 2017.

## II. FUNDAMENTALS & MISSIONS OF THE SECURITY FUNCTION

For the European Union, counterfeiting represents 6.8% of total imports, or an estimated value of 121 billion euros, which therefore translates into a lack of tax revenues of 19 billion euros and the massive loss of 40,000 jobs per year<sup>2</sup>. With regard to France, the Organisation for Economic Co-operation and Development (OECD) estimates that it is, on a global scale, the most impacted after the United States<sup>3</sup>. For companies that are victim to it, market share losses can reach 60% on certain products, especially in emerging countries.

The legal, image, and reputation risks can also be disastrous if, in the face of consumers who might be seriously impacted, companies do not demonstrate that they are organizing and acting to combat this scourge. This particularly impacts SMEs who have neither the resources nor the expertise to monitor their products both on their physical and digital markets.

Criminal organizations sell their productions by seeking to infiltrate lawful distribution channels, especially on the Internet via social networks. Benefitting from the porosity of markets and borders as well as insufficient controls of sometimes complicit and corrupt authorities, exploiting product price differences, filling the void generated by supply disruptions in the face of peaks in demand, expired, misappropriated, or falsified products invade the markets or reach consumers directly.

Before the digital age, product trafficking was mainly present in emerging countries. But with the development of digital sales platforms and the generalization of online purchases further amplified by the lockdown imposed in the context of the COVID 19 pandemic, illicit products are now accessible to all individuals, including those from developed countries who have become the first victims. Regarding health, for example, more than 90% of online pharmacies are illegal and 50% of the products sold are falsified (source). This is particularly the case in France where the Internet is directly at the origin of the appearance of fake medicines on the national territory. Indeed, the physical drug distribution circuits are controlled end-to-end by the National Agency for the Safety of Medicines and Health Products (ANSM), which avoids any risk of contamination of the logistics chain. The development of online commerce complicates the detection of entry thanks to the multiplication of small volume orders shipped by postal parcels.

**To be effective, a control strategy must be global, end-to-end, operational, instrumented, shared, and communicated.**

### A GLOBAL, END-TO-END CONTROL STRATEGY...

**A GLOBAL STRATEGY.** If a large majority of counterfeit products circulating on world markets comes from Asia (60 to 80% depending on the sector), illicit trafficking in genuine or counterfeit products significantly affects other regions such as the Middle East, Eurasia, Eastern Europe and South America. It is therefore fundamental that the affected companies can know and monitor worldwide the sales of their products on real markets and on the Internet.

Conversely, some products (especially food with high commercial value) are counterfeit in Europe and target the Chinese market.

**AN END-TO-END STRATEGY.** Avoiding the diversion, theft, or infiltration of legitimate distribution channels by counterfeit products requires continuous and end-to-end control of the entire product life cycle. This is to avoid a break in quality and continuity in the delivery of products to end customers which would be very detrimental to the company. If, thanks to the security strategy put in place, the occurrence and impact of incidents are reduced, the company can obtain favourable conditions from insurers and thus reduce or limit the sometimes-high costs of its insurance premiums.

At each stage (supply - production - transport - storage - distribution - destruction), it is necessary to carry out a risk analysis adapted to existing threats in order to develop prevention and control measures aimed at minimizing the identified vulnerabilities.

Standardized procedures, equipment and audits make it possible to assess the level of security maturity of the sites, to control normal and reserved access, to monitor the handling, storage, loading and circulation areas of products, packaging, and safety labels, to check incoming and outgoing flows as well as, if necessary, returns and destruction of products.

<sup>2</sup> Joint report OECD (Organization for Economic Co-operation and Development)/EUIPO (EU Intellectual Property Office), "Trade in Counterfeit Pharmaceutical Products", March 2020.

<sup>3</sup> OECD report, "Trends in Trade in Counterfeit and Pirated Goods", March 2019.

In this regard, the Transported Asset Protection Association (TAPA) provides standards for safety measures and audits as well as training and qualifications concerning the safety/securitization of the carriers and distributors who refer. In Europe, a protocol is being implemented with the police forces responsible for tracking cargo thefts. It therefore makes it possible to have an exhaustive overview of the locations and types of thefts, the operating procedures, and the cost of the stolen goods.

Alongside the purchasing and supply chain departments, **the security department must be involved in the selection processes of logistics suppliers, carriers, or distributors** with which the company is likely to contract. It will then be able to carry out the appropriate due diligence to verify the integrity and compliance of the applicant companies as well as detect possible implications of legal or natural persons in past suspicious cases. Security clauses inserted into contracts can thus provide for the possibility, depending on the sector and where possible, of carrying out checks and audits of distributors and prescribe the expected security requirements such as certifications, requests for agreements in the event of subcontracting, rules for announcing carriers on site, security equipment to be installed and preventive measures to guarantee the integrity of the supply chain.

It is also essential to include cybersecurity clauses to assess the cyber resilience of suppliers, ensure compliance with the rules and standards in force - especially those on private data -, verify the presence of reliable back-ups for critical data, coordinate responses in the event of a cyber incident and demand to be immediately alerted in the event of an attack, data leak or encryption.

### **... THAT IS OPERATIONAL & INSTRUMENTED**

**AN OPERATIONAL STRATEGY.** The operational control strategy revolves around detection, analysis, and investigations.

#### **Detection**

“Detection” aims to find falsified products in the real or virtual distribution networks and to identify illicit trafficking. The effectiveness of detection depends on the quality of the process of searching, analysing, and exploiting information. To do this, it is necessary to resort internally or externally to specialized analysts with tools and access to databases to identify criminal organizations, know the modus operandi, trafficking areas, actors, and products of interest.

Depending on the nature of the products, it is interesting to determine the areas and conditions conducive to counterfeiting and trafficking. The contexts of crisis, war, shortages, pandemics are particularly favourable because they generate major disruptions in the state services responsible for controlling imports and product quality.

A regular exchange of information globally and regionally with the company’s various business entities and supply chain planners also helps to better target areas of interest for criminals, by analysing, for example, sales figures to detect inexplicable variations from one period to another or anticipate stock outages.

Depending on the critical nature of the products and the markets, field verification campaigns can be organized to detect the presence of falsified or illicit products.

On the Internet, detection aims to identify product offers on specialized websites, sales platforms and the most used social networks, in all languages, using a mix of global and national experts. It is then necessary to verify the legality of the offer and, if not, to resort to test purchases to try and identify the origin of the products, while acting with the platforms concerned to obtain a withdrawal of online offers.

### **Analysis**

Obtaining samples of suspicious products in the field or via the Internet allows analysis by internal or specialized laboratories to characterize the nature of the counterfeit. This is essential if the rights holder wants to take legal action or testify as an expert at the trial of a criminal network that would be dismantled by the authorities.

### **Investigation**

The detection of a counterfeit or illegal product usually leads to the opening of an investigation. It is essential to be able to identify effective private investigation companies in each country of interest that meet the criteria of discretion and compliance to identify illicit circuits, trace the supply chains and develop information files that can be used by the analysts of the security directorate.

It is also necessary to identify the state operational units that are in charge and in a position to proceed, according to the information files transmitted, with operations for dismantling production sites and distribution channels. This requires establishing a relationship of professionalism and trust with these units by the correspondents of the local security directorates. In this regard, it is particularly important to be able to use the same survey and information processing tools as the State services, to be able to share data with them in a format that is understandable and usable by their systems.

On the Internet, it is a question of sending the competent units the lists of illicit sites and the detections of illicit sales online to benefit, when possible, from the contribution of the investigative and identification tools of national and international experts.

**AN INSTRUMENTED STRATEGY.** Existing technologies can provide valuable help to strengthen the airtightness of distribution circuits, the integrity of products and ensure their authentication.

### **Airtightness**

Air, sea or land carriers currently have highly effective technological means to prevent access to goods, such as systems for lockdown, opening detection, forced immobilization and signalling in the event of a course anomaly.

### **Tracing**

Various solutions make it possible to trace products, pallets and containers throughout their journey and thus be able to locate them in the event of theft. Based on communicating digital chips, they also offer a range of integrated logistics services, such as continuous temperature monitoring.

### **Authentication**

Digitalization now makes it possible to offer solutions that cannot be copied by counterfeiters, unlike those of the previous generation, based on visible or invisible holograms or visible encodings.

Some systems exploit the unique imprint of the paper weft used on labels or packaging. A simple digital application makes it possible to photograph this fingerprint and to make a comparison with the scanned image during the passage on the production line, making it possible to immediately know if the product is authentic or not.

The use of blockchain could also guarantee the continuous monitoring of each product throughout its life cycle.



### ... SHARED & COMMUNICATED

The scale of counterfeiting, the complexity of distribution channels, geographical diversity and the limited resources of private companies call for the implementation of a concerted information exchange and control strategy.

**BETWEEN INDUSTRIES WITHIN THE SAME SECTOR.** Networks of criminals engaged in counterfeiting or illicit trafficking of products do not target a particular company but rather a range of products. Several companies can therefore be simultaneous victims of the same network and therefore have an interest in cooperating in this non-competitive field. It is very profitable to organize in this way at the national and international level to formalize a cooperation that can take the following forms:

- Exchange of information on investigators and contacts with authorities in countries.
- Sharing information on threats, the modus operandi of criminal networks.
- Pooling of resources to finance detection campaigns or field investigations.

The Pharmaceutical Security Institute (PSI) thus brings together the forty major international pharmaceutical companies to orchestrate joint detection campaigns on drug ranges, as was the case for COVID 19 treatments and vaccines. The PSI also organizes regional awareness-raising campaigns with specialized state services and sets up survey tools and databases for the use of analysts from the various members.

**BETWEEN INDUSTRIES WITHIN THE SAME COUNTRY.** In most industrialized nations, associations bringing together companies from the same country in all sectors, such as UNIFAB (Union of manufacturers for the international protection of intellectual property), or companies from a particular sector, such as the G5 Santé for the pharmaceutical industry, aim to help their members victims of intellectual property infringement to assert their rights with public authorities. These associations can inform organizations about the impact of counterfeiting on their activities, the general public and states, develop concerted positions as well as initiate legal or regulatory initiatives, cooperate with the authorities to increase the effectiveness of the fight against criminal networks.

**BETWEEN THE PUBLIC & PRIVATE SECTORS.** The State and the company share a significant common interest in combating counterfeiting and illicit trafficking in products:

- The company to protect its market share, future growth, image and reputation.
- The state to preserve jobs, tax revenues and, in some cases, public health.

To be effective on the ground, it is essential that the public and the private sectors cooperate in an organized, operational, and continuous way.

Companies bring a unique knowledge of their products, characteristics and markets allowing them to carry out upstream operations to detect and characterize counterfeiting or illicit trafficking. They can also mobilize their resources located in many geographical areas and thus shine a particular light on state services.

The State can mobilize the various investigative services concerned, use special investigative techniques, mobilize international cooperation, and prosecute criminally.

Cooperation can take several forms, up to and including the signing of an official partnership, such as the one between G5 Santé and the French Central Office for Coordinating Environmental and Public Health Crime (OCLAESP), on the following actions:

- Mutual information through regular case reviews and exchange of data from investigations or cyber surveillance.
- Training of specialized customs, police and anti-fraud services on the authentication of products and the detection of counterfeits.
- Operational intervention by the authorities after identification of networks to arrest traffickers and dismantle production sites or demand the closure of illegal online sites or the withdrawal of offers of counterfeit or illegal products on social platforms and networks.
- Filing complaints, provide testimony and provide judicial expertise to support the action of public authorities in criminal matters. In this regard, we can only regret the fact that counterfeiting, in many countries, is still perceived from a legal perspective as an infringement of intellectual property, with economic and financial impacts that are certainly important but not vital. A perception of counterfeiting that would be more widely considered as a serious public health risk, which causes serious diseases and many deaths depending on the products concerned, and therefore punishable by a criminal complaint would be more relevant. This observation has many consequences:
  - The fight against counterfeiting, even of medicines, is not one of the priorities of the State services, which, for legitimate reasons from the tax point of view or public order, are more focused on the traditional struggles against the trafficking of narcotics, tobacco, weapons, and human beings. As a result, counterfeiters know that the risks of being arrested are low.
  - Counterfeiters are not tried as criminals and often face only light sentences, both civil and criminal, often suspended, which is little deterrent. This feeling of immunity is exacerbated on the Internet, where sales can take place anonymously and discreetly by playing with borders. Faced with this flexibility, State services are making progress, but administrative and judicial procedures are still cumbersome, inefficient, and reactive. The organization of the courts and the powers of judges need to be strengthened and specialized to respond effectively to the complexity of international digital traffic.

**A COMMUNICATED STRATEGY.** To increase the effectiveness of the fight against counterfeiting and illicit trafficking, it is important to raise awareness among potential victims and to communicate internally and externally about the reality of these scourges.

### Internal awareness

**Awareness-raising aims to make the reality of existing trafficking recognized by:**

- The governing bodies, to obtain their support and the resources necessary for the implementation of an effective strategy.
- The functions involved in the product life cycle, in order to convince them of the usefulness of implementing risk prevention and control measures.
- The sales forces who are the ears and eyes of the company, to teach them to report any suspected defective product without delay.

### External awareness

**External awareness-raising plays both a preventive and mobilizing role for:**

- Potential victims, in order to make them more vigilant, by becoming aware of the risks of counterfeiting. Depending on the type of risks and products, more specific campaigns and supports may be aimed at certain targeted regions or populations, parents, children, travellers, etc. When it comes to Internet purchases, the most vulnerable populations are young people who, often persuaded by a seemingly good deal, are not aware of the risks of counterfeiting or consider them negligible in view of the price difference.
- National and international organizations or associations, to mobilize public authorities, strengthen legislative mechanisms and means of intervention.
- Public authorities, to encourage them to strengthen their legislation and the means of control.
- The specialized state customs and investigation services, training them to recognize the characteristics of the original products and the prevention technologies implemented.

### **Communication**

Regular communication in the form of symposiums, interviews, campaigns, and articles is necessary to educate the general public about the dangers of counterfeiting, the risks of Internet purchases as well as possible possibilities to verify the legality of the seller and the authenticity of the product.

### **CONCLUSION**

Faced with the continuous growth of criminal activities in counterfeiting and damage to the integrity of the supply chain and considering the dramatic risks reaching the general public as well as the impacts on companies, it is crucial to significantly amplify the current means of control, both at international and national level, public or private.

Efficiency will require stricter legislation to be truly dissuasive; reactive and mandatory systems, especially on the Internet, to limit distribution channels; and enhanced cooperation between rights holders and state services. ■

<sup>4</sup> Information report by the Commission for the Assessment and Monitoring of Public Policies of the National Assembly presented by MPs Christophe Blanchet and Pierre-Yves Bournazel in October 2020.

# GENERAL RECOM > MENDATIONS

- > **Strengthen state action in combatting counterfeiting by implementing the recommendations of the Blanchet-Bournazel report on the evaluation of the fight against counterfeiting<sup>4</sup>.**
- > **Strengthen the judicial arsenal both in civil matters, by increasing the amounts of damages and interests for rights holders in a dissuasive way, and in criminal matters by strengthening penalties, both with regard to legal or natural persons engaged in illicit trafficking, and virtual intermediation platforms.**
- > **Institutionalize and better federate the public-private partnership to make it more operational by identifying an ad hoc structure capitalizing on the experience of the National Anti-Counterfeiting Committee (CNAC).**
- > **Improve the effectiveness of the fight against counterfeiting by ensuring that Customs can send seized samples to companies holding rights for scientific analysis to characterize the possible danger to public health and thus mobilize the authorities to ensure the protection of populations.**

- > Identify an international organization that could house and maintain a database fed by the various sectors concerned to report incidents with supply chain operators.
- > Create a “Counterfeiting” section to allow suspicious products to be reported on the PHAROS, the online illegal content reporting platform.
- > Using the model of the G5 Sante-OCLAESP partnership, depending on the sectors, threats and risks, extend official agreements with general business federating bodies (CDSE, MEDEF, UNIFAB...) or sectoral and the various state organizations (Customs, DGCRRF, OCLDI, SIRASCO, TRACFIN, ANSM invested with a direct or indirect mission to combat product crime to facilitate exchanges, provide a legal basis for cooperation, promote detection and prevention mechanisms, increase the flexibility and efficiency of operations, neutralize potential public health crises and create a long-term relationship of trust.
- > Work firmly for the adoption by the European Union of the strengthening measures proposed at the end of the consultations within the framework of the Digital Service Act and work with the private sector to implement them quickly and effectively.
- > Set up public-private mechanisms to detect and seize counterfeit products, in particular those harmful to public health, in transit through the ports of the European Union.

## PROTECTING CRITICAL INFRASTRUCTURES: A COMPONENT OF GLOBAL STRATEGIC REFLECTION FOR BUSINESSES

### MICHEL POZZO DI BORGO

*Deputy Security Officer of the Bank of France  
Chair of the CDSE's "OIV & protection of installations" commission*

Characterizing the critical nature of an infrastructure is far from easy. Each manager may indeed consider, in good faith, that the premises within which the activities for which he is responsible are conducted, or which participate in the realization of these, must be imperatively preserved in all circumstances.

**A**nd, de facto, consider that they are critical and must be subject to the highest level of protection... Mastering such an approach, a source of inflation of demands and therefore related costs, requires analyzing the criticality of infrastructures at the global level of the company while taking into account interdependencies with other operators. In this corporate approach, infrastructures whose full operability would compromise the company's vitally important missions or generate a risk to the health or even the life of the population must be considered critical in the sense of physical security.

## II. FUNDAMENTALS & MISSIONS OF THE SECURITY FUNCTION

This definition inevitably refers to the strategic analysis of business processes and associated risks, which must make it possible to prioritize them and ultimately identify the essential premises, areas, or perimeters on which protection efforts - and the corresponding budgets - should be focused.

Significant collaborative work is therefore to be carried out by corporate Security Directors in close connection with the business lines and based on a perspective that creates synergies between risk mapping approaches, BIA<sup>1</sup>, strategic mapping or business continuity...

In the end, this census work makes it possible to deliver an accurate mapping of the company's sensitive infrastructures, which are of variable size (e.g.: Security commands, technical rooms, fluid production areas, trading room...) and can be nested in each other.

### THE PROTECTION APPROACH: FROM THE GLOBAL ANALYSIS OF THREATS TO THE IMPLEMENTATION OF MECHANISMS

**Risk assessment is at the heart of every physical security decision. A progressive approach, in successive concentric circles, is essential:**

The objective of the global threat analysis is to assess the potentially hostile environment in which the company operates. These can be conventionally divided into passive threats (climatic, environmental, technological hazards, etc.) and active threats (caused by a person or a group of people) and must be evaluated in terms of impact and probability, taking into account the operating characteristics of the company. By way of illustration, threats as diverse as those related to terrorism, social activism, malice, but also exposure to natural risks (flood, seismic zones...) or industrial (possible proximity of Seveso or AZF type activities ..) must be analysed in this way. On a practical level, this general panorama can take the form of:

- Transverse analyses, or even very general trends, using, for example, PESTEL-type strategic analysis methods<sup>2</sup> to characterize the company's environment.
- Detailed analyses of the various threat themes: each study aims to clarify the subject, to identify the events that have really affected companies whose activity is close or comparable to assess their impacts and probability and to list the protective mechanisms that have proven to be effective, or conversely, useless.

This work of permanent monitoring of "what could happen" (realistic or credible threats), both in normal and exceptional operating situations<sup>3</sup> must rely on all available sources of information (historical data, benchmarks from comparable organizations, relations with security forces or ad hoc state services...).

- Once the credible threats (the collection of which constitutes the company's danger environment) have been identified, a vulnerability assessment must be carried out as close as possible to the field, taking into account the strengths and weaknesses of each "zone" of the company (e.g. public area, semi-public area, restricted access areas, ultra-confidential areas...). To do this, the experience of the company's security personnel is essential because they must be able to imagine possible scenarios of events and to characterize the process and the practical modalities (e.g. use of explosives, use of battering vehicles, attack via a "reception committee", use of drones, use of chemical or biological agents...). The combination of threats and vulnerabilities makes it possible to characterize the risk and, de facto, to initiate actions aimed at preventing it or limiting its impacts: this work constitutes the permanent challenge of corporate Security Directors and the only justification for the - significant - resources that they are required to mobilize in the organization.

<sup>2</sup> Areas of analysis of the PESTEL method: Political, Economic, Sociological, Technological, Legal and Environmental. In particular, the greatest attention should be paid to the situations caused by the carrying out of works (subsidence of perimeter defenses, use of numerous service providers, implementation of degraded procedures...).

<sup>3</sup> In particular, the greatest attention should be paid to the situations caused by carrying out works (subsidence of perimeter defenses, use of numerous service providers, implementation of degraded procedures...).

<sup>1</sup> BIA: Business Impact Analysis: an approach to assess the impact of various events of varying nature and magnitude on the conduct of activities.

> With regard to the protective mechanisms to be implemented, it will be useful to refer to the concepts and approaches usually used in the profession. Although the list presented below cannot be considered exhaustive, several concepts emerge as a priority:

- The concept of “in-depth defence” makes it possible to design a gradually reinforced security from the building perimeter to its core, based on a zoned approach;
- The concept of 4D – Deter/Detect/Defence/Delay<sup>4</sup> establishes the essential objectives of protection;
- The HOT approach (Human/Organizational/Technology) dictates the absolute need to combine technical, organizational and regulatory mechanisms... but also human, to achieve effective and efficient protection.

Finally, the greatest attention should be paid to the regulatory framework governing the organization’s activity, if any. In close coordination with the legal department, corporate Security Directors must be in a position to keep themselves in compliance with the multiple - often complex and always costly - imperatives established by the state authorities (for example, the Defence Code and the IGI 6600 of January 2014 on the security of activities of vital importance, the national security directives for each sector of vital importance, the security requirements of information systems imposed by the Military Programming Law, GDPR, and so on). ■

<sup>4</sup> Deter/Detect/Defend/Delay.

# RECOM > MENDATIONS

## For the attention of Security Directors

- > Consider the protection of critical infrastructures as a result of the company’s overall strategic thinking. To do this, create synergies between the different approaches prioritizing the criticality of activities and/or risks and actively cooperate with the business lines that use these infrastructures.
- > Establish a detailed mapping of critical infrastructures and have it validated by the company’s management bodies (COMEX or equivalent).
- > Set up a permanent monitoring process on the nature of threats and their evolution, and periodically bring this panorama to the attention of the governing authorities.
- > Ensure the complementarity of human, organizational and technical protection devices.

### **For the attention of the authorities**

- > Involve corporate Security Directors from large companies in the development of reference texts in order to assess their relevance and estimate the resulting cost.
- > Strengthen the convergence and consistency of the texts, so that corporate Security Directors can benefit from a simpler and more homogeneous general framework of reference.

## GLOBAL SECURITY

---

## **DEFINING A GLOBAL SECURITY POLICY WITHIN THE COMPANY**

### **ANTOINE CREUX**

*Security Director of the Société Générale group  
and CDSE Administrator and treasurer*

The security issues that companies face have become more significant in recent years, while diversifying and intertwining.

In France, companies must face a terrorist risk that is not abating, even though it has changed in nature, mainly conducted today by isolated individuals, under the influence of the Islamic State and its propaganda. The release of several dozen Islamists convicted for terrorism as well as that of radicalized prisoners over the next few years also amplifies the terrorist threat. Actions carried out on the side-lines of protest movements have reached an unprecedented level of violence, as shown by the “Yellow Vests” crisis, and civil disobedience actions are multiplying with their direct impact on the activity of certain companies.

## II. FUNDAMENTALS & MISSIONS OF THE SECURITY FUNCTION

The same structuring trends are observed abroad. The impact of the pandemic on the geopolitical context and the intensification of ongoing conflicts will continue to fuel regional security issues. Whether it is social unrest in developing countries, mainly related to the slowdown in global economic activity, emerging terrorist threats, especially in northern Mozambique and the Gulf of Guinea, which are in addition to those expanding in the Sahel region, conflict management in the Middle East, the rise of protest movements in Europe, economic tensions as vectors of conflict, security challenges are and will remain major for the operations and development of French companies internationally.

Finally, the current context is marked by an extremely elevated level of cyber threat, confirmed by the exponential number of companies that have been subject to attacks with significant impacts in 2021. Cybercriminals are often looking for financial gains, but companies can also be the subject of attacks, often of state origin, with the aim of stealing information that is sensitive, or potentially destabilizing.

This non-exhaustive panorama of threats requires **an assessment of the security risk for companies, regardless of their size, at a high level. Potential impacts are manifold and can be systemic for a company:** damage to the physical integrity of employees, deterioration or destruction of critical infrastructures, theft of sensitive information, damage to the company image, constraints on its development... Only a global approach can allow the company to reduce its security risks, which interweave and overlap.

### **A BETTER CONTROLLED ENVIRONMENT FOR DEVELOPING THE BUSINESS**

It is therefore down to the security department to define a **global security policy** that applies this global approach to risks in order to anticipate, protect, be able to react and continuously improve responses to security risks, in order to **allow the company to develop its business in a better controlled environment.**

This global security policy integrates all security areas: personal and property security, tangible and intangible, strategic intelligence and economic security, crisis management and operational resilience. It must be built in close partnership between all the teams that contribute to security within the company and in constant dialogue with the professions.

It is based on the fundamentals of a security approach:

- > Evaluate the **threat level** and identify the resulting risks;
- > Define the **security policies of the various domains** and good practices;
- > Design and implement **security mechanisms** adapted to the threat level;
- > Support **business development**;
- > Meet the **legal and regulatory obligations**;
- > Define and test **contingency plans**;
- > Provide expertise in **crisis management**;
- > Evaluate and draw up **insights**;
- > **Raise awareness, teach, train...**

Depending on the field of activity of the company, its locations and other possible criteria, the security department may make efforts in this or that area, but it will always have to ensure that it devotes sufficient resources to anticipation. It is recommended to formalize the security policy and have it validated at the highest level of the company. Finally, the implementation of KRI (Key Risk Indicator) type indicators makes it possible to measure the effectiveness of the choices made.



## THE CONDITIONS FOR A SUCCESSFUL GLOBAL SECURITY POLICY

The effectiveness of a security policy is of course down to the quality of its implementation and the resources devoted to it. Thus, an entire mechanism that must be mobilized in order to reduce the company's exposure to security risks.

The effectiveness of **GOVERNANCE** is based on the involvement of the general management and the various heads of entities (business units, factories, subsidiaries, etc.) and on an alignment of teams contributing to security in the various fields and within all the establishments or locations of the company. The security department has in this context the important role of animation of the security community in a hierarchical or functional framework depending on the organizations.

In addition, the company's **EXTERNAL RELATIONS** developed with State services contributing to security are likely to inform the assessment of situations as well as the sharing of experience with our peers, in France and abroad. The CDSE provides valuable support to Security Directors for this.

Finally, **ACCOUNTABILITY** of all the company's employees on security issues remains essential, as the human factor can be a source of vulnerability. Many actions must be undertaken for this mobilization: training, regular communications, dedicated events. ■

# RECOM > MENDATIONS

- > A risk analysis focused on the company's activity and its environment is a prerequisite for the implementation of a global security policy and anticipation is key.
- > A global security policy must address all areas: security of people and goods, tangible and intangible, strategic intelligence and economic security, crisis management and operational resilience.
- > The implementation of a security governance including the company's management, unifying all teams, and mobilizing employees on security issues is a prerequisite for the success of any global security policy.



**III. NEW  
SECURITY  
CHALLENGES**  
& PERSPECTIVES



## **THE RADICALIZATION PHENOMENON: A RISK FOR THE COMPANY**

### **PIERRE TRAMIER**

*European Security Director of the Danone Group  
Chair of the CDSE's "Radicalizations" commission*

The company is a mirror of society. Whether it is out of ideological, religious, political, ethnic conviction, or out of increased sensitivity to the great challenges of our time, an increasing number of people adopt deviant behaviours to assert their ideas or beliefs.

**T**he crystallization and hypersensitization of society, widely relayed and fuelled by social networks, favour the emergence of this type of attitude. Previously isolated, individuals are finding a foothold for their fears or certainties in the internet space and quickly becoming actors, conscious or unconscious, acting in the name of defending or promoting a cause that they have made their own.

The company is now facing these new internal and external actors who are challenging the organizations more and more frequently, resorting to violent or spectacular action to echo their convictions and draw the attention of as many people as possible to their initiatives. The visibility offered by the internet and social networks on an international level encourages the appropriation of causes by everyone and an acceleration of the radicalization process.

Moreover, if in the past an application for a job was often motivated, among other things, by the prospect of career development, the salary, the security that the organization could offer, nowadays it is the societal choice, the investment in causes perceived as "just", in which the person finds himself, which the youngest generation prioritises when making choices.

### **DEVIANT BEHAVIOUR: A WIDESPREAD THREAT**

---

Faced with this new situation, the company, in search of legitimacy and anxious to attract talent and capture expertise, risks losing its neutrality and being in turn engaged in a militant process. The risk posed by activism, or the various forms of radicalism is very present, and essentially threatens image and reputation. Indeed, the notion of brand is widely abused and very often questioned or challenged by radical movements.

In the food industry, for example, sowing doubt in the consumer's mind about the legitimacy of the company or its ability to guarantee food safety is enough to permanently weaken everyone's trust capital and sometimes leads to the outright disappearance of the organization. In industry, a questioning of ethics exploited by radical groups can otherwise be fatal but at least force the industrialist to profound reorganizations that can be costly and unstable.

### THE SECURITY DIRECTOR: A MAJOR PLAYER

If action on this social phenomenon is located outside the company's control perimeter, it is however up to the security department to participate in the awareness-raising action, under the leadership of Human Resources, in order to implement, in advance, a favourable framework to protect the company.

**For these purposes, four steps seem to be necessary:**

**RAISING THE AWARENESS** of the boards of directors and taking into account the risk of radicalism in the field of possibilities is an indispensable first step. For many of us, the phenomenon of radicalization is still systematically associated with religious convictions and the transition to violent acts, to terrorism. Since their activities have never been impacted, many organizations do not feel concerned.

With the support of a sponsor within the Board of Directors, the HR department will be able to initiate a transversal approach by setting up a roundtable of the finance and legal departments, as well as all the company's entities with legitimacy to deal with this topic. The security department will provide its analysis and expertise.

This second phase, dedicated to **ANALYSIS** will consist of:

- Identifying, naming and defining precisely within the company the behaviours that it considers to be in line with its values and its operations.
- Promoting and installing a pragmatic approach, devoid of any emotional notion when handling subjects of radicalism. It is not a question of judging the value, the interest or the merits of a particular belief or conviction. It is a question of defining whether the expression of these is compatible or not with the operations of the company.

The third step will be the **FORMALIZATION** by the company or the organization, in all its statutory and regulatory documents, of behaviours that comply with the expectations of the organization. The more precise this formalization will be, the easier it will be to identify deviant behaviour and treat it.

Finally, the last stage will be devoted to **TRAINING** the entire managerial structure by ensuring that managers are equipped with all necessary tools and escalation management procedures to be followed to deal with cases of deviant behaviour they may come up against.

It is by establishing a real transparent, objective, and sincere dialogue, devoid of any emotional aspect, that the organization will be able to accurately define its identity and create the necessary conditions for its protection. By doing so, the security department protects, on the one hand, the serenity, and the ability of the company to take risks in order to develop and, on the other hand, actively participates in the role of education and training that is increasingly incumbent on organizations. ■

# RECOM > MENDATIONS

- > The security department must participate in awareness-raising action on the phenomenon of radicalization in order to implement a favourable framework to protect the company.
- > Raise the awareness of the boards of directors and consider the risk of radicalism in the field of possibilities is fundamental.
- > Promote and implement an approach that is pragmatic and devoid of any emotional notion when handling subjects of radicalism.
- > Identify, name, and define precisely, within the company, the behaviours that it considers to be consistent with its values and its operations, and formalize them in all its statutory and regulatory documents.
- > Train the entire managerial structure by ensuring that managers are equipped with all the necessary tools and escalation management procedures to be followed to deal with cases of deviant behaviour.

## DIGITALIZATION OF THE SECURITY DEPARTMENT: OPPORTUNITIES & RISKS

### CDSE LAB

*This article was written under the aegis of the CDSE Lab by **Clémentine de LAMBILLY** (Orange) and **Pierre-Arthur MAZEAU** (Thales) under the direction of **Jean GARCIN** (Manpower), co-chair of the CDSE Lab*

The invention of the PC in the mid-70s marks the tipping point of our society towards the “digital age”. This era is characterized by an exponential growth in the number of digital devices in circulation and their uses. In companies, these easy-to-use tools have made it possible to streamline and accelerate the circulation as well as the mass dissemination of information, especially thanks to the Internet.

**M**oreover, new technologies are transforming uses while providing new solutions. The use of security technologies by the security department in corporate businesses is a perfect illustration of this. This constant digital transformation is accompanied by the appearance of new risks and the increase in the attack surface of companies and organizations. Thus, the digitalization of activities inevitably requires the implementation of defensive measures in the face of the evolution of the threat.

### **TOWARDS AN “ENHANCED” SECURITY FUNCTION**

For the corporate security departments, the use of AI (artificial intelligence), big data, the exploitation of free access data, or the use of devices such as drones constitute a revolution capable of allowing ever greater deterrence, reaction and anticipation. This revolution is to be put into perspective with the technical evolution of more traditional means of protection (fences, doors, shields, etc...) which, thanks to technology, are becoming more reliable, safer and easier to use because they can be interfaced with digital developments.

This increased digitalization involves rethinking the functioning of the Security function in companies, without ever neglecting the importance of the human. Indeed, while it is not decently possible to make a security chain entirely based on technological systems, these must support human action by providing decision support and by allowing the automation of certain tasks. A proportionate and assimilated use of technology thus allows an increase in the competence of the sector, integrating new professions with new and more technical profiles, at the service of a more efficient overall security.

The digitalization of monitoring, analysis and crisis management tools is therefore an opportunity. It allows a reduction in the processing time of information (up and down), an -automation of tasks (monitoring, integration with internal-external tools), ease of preparation and access to information (format of security procedures, cross-platform access, instant notifications). Good integration and use of adapted digital solutions thus makes it possible to increase productivity and increase the speed of execution of a task. In addition, each company has an exponential number of data specific to its environment and its activities. For corporate security departments, the processing and analysis of this data through business applications can make it possible to refine the perception of areas of vulnerabilities, to build dedicated protection strategies, and to better anticipate. For these purposes, the corporate security departments increasingly have data scientists in their ranks.

The security departments can develop their own tools or purchase solutions to quickly and intelligently process this mass of information on a daily basis. However, the multiplication of tools, needs and costs can make it difficult to choose between different solutions. If the security departments want to have high-performance solutions, it is often necessary to resort to foreign solutions, which implies questions in terms of compliance and data sovereignty. While digital sovereignty must become a criterion of choice, monitoring at European level to qualify suitable tools could be a compromise between demand/need and legal constraints.

The digitalization of the security function, and more broadly the digitization of society, bring with it crucial issues regarding the acceptance by the greatest number as to the use of these new technologies. Safeguards are therefore essential in terms of respect for individual freedoms. The definition of the legal framework specific to each tool, the implementation of guarantees relating to the protection of personal data (CNIL monitoring) and the company's information assets are essential prerequisites for this acceptance. As such, the 2024 Olympic Games represent an exceptional opportunity to accelerate the transition

### **MULTIPLE CYBERSECURITY CHALLENGES**

This digitalization of the Security function is not without risk. All security systems are computerized on local or corporate networks, making organizations more exposed and more vulnerable to cyber risks. Security must therefore be at the heart of IT security issues and the corporate security department must collaborate effectively with the IT professions, and in particular the SSI (Security of Information Systems) experts of the company. The implementation of a set of security techniques and solutions to protect the confidentiality, integrity and availability of data is essential to guarantee reliable systems. Methods such as security by design allow, from the design of a solution, to integrate security into the source code. That is why the help of SSI experts is essential in order to guarantee a secure network architecture as soon as new security tools are installed.

On the other hand, the daily use of digital tools by the greatest number in the private sphere has pushed consumer tools to the heart of the professional world. This use entails a real problem for the IT security of organizations and in particular with regard to the appearance of shadow IT: the use of hardware and software technologies by company employees without the agreement of their CIO (Chief Information Officer). The lack of support, of service availability, data sovereignty and the level of IT security of the general public all lead to internal flaws within organizations. Thus, the large American consulting firm Gartner predicted in 2016 that *“a third of successful cyberattacks against companies [in 2020] would target their Shadow IT resources”*. The major cyber-attacks, such as NotPetya in 2017, the laws for the protection of personal data or the military programming law and its security constraints for OIV (operators of vital importance) have enabled a certain awareness of the importance of cybersecurity issues.

### **NEW TECHNOLOGIES & LEGAL ACCEPTABILITY**

Our organizations are facing digitalization and an increased dependence on digital tools. This mutation introduces new standards while we are only at the beginning of the digitization phenomenon as demonstrated by the “smart city” projects or the advent of the Internet of Things. In the light of the Paris 2024 Olympic Games, the State must establish a precise legal framework for the use of new security technologies such as biometrics or facial recognition, both in the public and private domain, and in particular in companies.

Indeed, the lack of clarity can hinder digitalization efforts, since companies do not always have the legal means to deploy new tools. Despite the entry into force of the GDPR and the increasing control of the CNIL, the use of new security technologies is still perceived as being particularly intrusive. By adapting the legal environment and therefore the framework for the use of these new techniques, the State would not only optimize the effectiveness of public security, but it would also support the mission of corporate Security Directors in their mission to protect their interests, their employees and their customers for a more global security of all citizens while guaranteeing the protection of their personal data. ■

# RECOM > MENDATIONS

- > Provide security technologies with a legal framework, under the strict control of the CNIL in order to guarantee the protection of public and individual freedoms.
- > Implement hybrid policies in the security departments combining a greater contribution of security technologies allowing humans to gain reactivity, anticipation, and competence.
- > Integrating the skills of analysis and data processing (big data) within the Security function.
- > Integrate SSI from the design or implementation of new security technologies.
- > Provide non-digital alternative solutions to security technologies in order to protect against a cyber-attack and test the implementation of these solutions during planned exercises.
- > Integrate and promote sovereignty criteria in the choice of digital solutions.

## ANTICIPATION DES CRISES

### THINKING & IMAGINING THE UNTHINKABLE, MANAGING UNCERTAINTY

#### THE “CRISIS MANAGEMENT & BUSINESS CONTINUITY” COMMISSION OF THE CDSE

*This article was written under the aegis of the CDSE's “Crisis management and Business Continuity” commission, by **Gabrielle BERTHELOT**, head of crisis management within the security department of the Kering Group and **Anne PICOT-PERCIAC**, Chief Security Officer of the Atos Group.*

Thinking the unthinkable, managing uncertainty... these ambitions could make you smile, and yet it is necessary to dwell on them in order to increase your chances of survival in an ever-changing world, in which upheavals have been accelerating at breakneck speed since the beginning of the 20<sup>th</sup> century, therefore making it more and more complex.

**H**owever, our human brain does not appreciate uncertainty and often refuses to imagine the unthinkable. Regardless of the nature of the cataclysm or the attack, the only considerations to be taken into account are the effects and impacts on the organization and how to limit and overcome them. The scenario is ultimately only an aid to the imagination and the analysis of the impacts makes it possible to develop a pragmatic response in order to prepare.



This reflection exercise helps to reduce the effect of surprise when a disruptive and unforeseen event occurs.

Among the many existing models to support change management, that of Dr. Kübler-Kloss can be used to understand the stages through which individuals can go when faced with sudden change (shock, denial, anger, fear, sadness, depression, acceptance, forgiveness, search for meaning, serenity, growth). The whole point is to limit the time spent in the first stages, which are very energy-intensive for the human brain, in order to quickly reach the so-called “acceptance” phase, which allows you to take action with a more positive and enlightened state of mind.

Perceiving beforehand that a fact is going to happen, is the best way to anticipate a disturbing event, an incident or a crisis. At least at the corporate level, it is necessary to set up alerts on:

- > The geopolitical, health and climate situation where the organization has interests.
- > Keywords in social media.
- > New legal texts, case law and regulatory developments.
- > New computer viruses, new vulnerabilities, and updates.

**We must not neglect the internal monitoring of the organization** (examples: monitoring computer networks, “listening” to the social climate...). The exchanges that each department may have externally with partners, customers, or competitors in its own sector of activity or in others must also be included in the monitoring system. This practice makes it possible to capture trends and evaluate qualitative aspects.

#### **HOW TO IDENTIFY THE ORGANIZATION'S RISKS**

Several ISO standards and benchmarks have a risk-based approach to security: looking at the company's processes, **identifying useful assets/resources** to carry out this process successfully (examples: sites, people, supply chain, information systems...), and the threats and vulnerabilities that weigh on these assets, and finally assessing the probability and impact in the event of one of these risks materializing. The next phase consists in defining the action plans to limit the impacts.

An interview with the members of senior management allows a complementary approach: it offers the opportunity to ask each of them what would be **“their worst nightmare for the company”** in their field of competence. This point of view constitutes a good working basis for imagining crisis scenarios.

#### **HOW TO LEARN DECISION-MAKING IN UNCERTAINTY?**

While it is essential to practice crisis simulations based on realistic scenarios adapted to the organization's activity to test plans and procedures, it is also necessary to train the teams that will have to face a major event, to apprehend the effect of surprise, manage uncertainty and thus develop their adaptability.

The rapid and effective start-up of the crisis organization therefore depends on the teams, on their ability to quickly understand the situation, ask the right questions and find the resources to answer them.

Before each appointment, and regardless of their field of activity, a manager should be sensitized about the issues of “information feedback” of a disruptive event, crisis management and business continuity. There is a high probability that he or she will face it directly or indirectly during his or her career.

**But if experience is a factor of success, it can also lead to biases,** and this requires a lot of effort and humility to approach each situation with a fresh look, in order to address the issue, understand the impacts, define what falls within the scope of responsibility of the organization and integrate constraints that cannot be monitored.

To develop, train and strengthen the cognitive abilities of crisis teams, it would be interesting to train them to think, react and decide while being destabilized and out of their comfort zone. Swapping the roles of everyone in the crisis cell at each training session, or the roles of the crisis cells between them, working on unknown or even completely ludicrous scenarios, or removing the usual means and tools can be ways to develop cohesion and empathy, better understand the issues and constraints of each while considering the unthinkable with humility.

The use of technology in our working methods gives a false feeling of assistance, security, and control. However, faced with extreme situations that would exceed all forecasts and / or deprive the organization of its means, it could be useful to be able to count on teams that know how to make decisions with common sense, and trusting their intuition despite the uncertainty.

At the beginning of the crisis, it is of course recommended to research similar crises to be inspired by good practices and use the elements as a basis for work. This has two virtues: to save time on understanding the issues, the pitfalls, and the identification of the actors of the crisis and to avoid starting with a blank sheet of paper. The inevitable corollary is that, in the minds of the members of the crisis unit, a parallel can be established between the two crises.

We must be careful. The task assignment (information collection, analysis, projection of the impact for the organization) to separate teams must contribute to this.

A truth at a given moment may turn out to be false a few hours later. Here again, models such as the Deming circle or the OODA loop make sense. **Observe, Orient, Decide, Act, and resume** the observation and analysis of the changes at the end of this first loop to launch the second. **Accept being wrong.**

**The members of the crisis teams must be reassured, their responsibility clearly explained, and their scope of decision and action defined with limits related to the organization and specific skills.** Beforehand, the objectives of each crisis unit must be stated. The crisis unit must refocus on these at regular intervals. A private company is not going to replace the emergency services. On the other hand, it is responsible for interfacing well with them in the interest of its employees and its business continuity.

In conclusion, if it is impossible to think the unthinkable, it is possible to reflect on the consequences of the unthinkable for the organization and thus, to manage uncertainty. ■

# RECOM > MENDATIONS

The objective is to see how the organization can put in place countermeasures to compensate for this unavailability.

Then, by looking at disaster scenarios, it is possible to project this unavailability in the proposed context and adjust the proposed plans.

With this rational approach, it will be easier to convince senior management to invest in a countermeasure even if the proposed scenario has a low or zero probability.

> Reflect on the unavailability of resources:

- People

What would we do if employees for X reason(s) could not come to work?

What would we do if they were not able to work, even from home?

- Sites

What would we do if the sites were inaccessible, partially or completely destroyed?

- IT system

How would we manage without a computer network? Without an IT system? Without a communications system?

- Supply chain

What would we do if our suppliers could no longer deliver to us?

> Analyze the impact of apocalyptic scenarios on the organization.

> Equip crisis teams to deal with extreme situations by developing their cognitive abilities under stress.

> Dare!

## CORPORATE SECURITY DIRECTORS WITHIN THE SECURITY CONTINUUM: A DESIRE TO BE REALIZED

### ANNICK RIMLINGER

Director of Security, Cyber & Data Protection of the Aema Group

The 2015 attacks highlighted, in a country traumatized by these events, that the Nation's security is also "everyone's business", referring to an assertion popularized by many experts and politicians.

A new paradigm that gives a role to each of these actors is also manifested by the appearance of a new semantics around the notion of *continuum* which had never been used in this way to describe the transfer of certain missions and the role of new actors. The security *continuum* therefore aims to make a chain of collective intelligence in security, which can contribute to the vital objective of spreading a culture of vigilance, forming the best safeguard for the defence of the Republic and its ideals.

Following the launch in 2017 of the reform of the Daily Security Police force (PSQ) in the first months of Emmanuel Macron's five-year term, the government wished to conceptualize this chain linking all national security actors, the basis of a global security built on full collaboration between public security forces and private actors.

From this point of view, the work of the MPs the LREM majority Alice Thourot and Jean-Michel Fauvergue constituted a first step. In their report entitled "*From a security continuum to a global security*", commissioned by the Minister of the Interior Gérard Collomb and provided to the Prime Minister Edouard Philippe in September 2018, the two parliamentarians formulated 78 proposals, a number of which were related to the place of companies and Security Directors in the security *continuum*, such as:

- > **Re-assessing the role and positioning of Business Security Directors.**
- > **Creating a security correspondent (CS) status within companies.**
- > **Opening up the possibility to grant confidential security clearance level to holders of these roles.**

Taking over from Gérard Collomb, place Beauvau, in October 2018, Christophe Castaner, appropriated these recommendations and indicated, during his speech at the opening of the 2019 edition of the CDSE symposium, that the Security Director "*must be a central actor for the reputation of a company, for its employees in France and abroad, for its customers and suppliers, for its manufacturing processes or its information systems*". The Minister of the Interior continued by assuring that "*the State is willing to help the Security Director to carry out their mission, including by creating a network of trust in order to exchange sensitive information at the highest level*". "*It is essential that this circle of trust is built between us*", he emphasised.

Nevertheless, it must be noted that two Security Directors are not alike, and that there are as many areas of responsibility as there are organizations of the Security function within businesses. Despite this contrasting landscape, their positioning is well anchored in the framework of the *continuum* but at this stage, is not yet assertive enough to weigh in on the public debate.

#### DIVERSE SECURITY DEPARTMENTS WITH A NEW VISIBILITY

Since the 2000s, the vast majority of companies have become aware of the importance of implementing a security approach within their organisational structure. For some groups, this is a genuine strategy that, like others, promotes its business development. Leaders have indeed clearly understood that it is up to them to organize the security and safety of their organization. But most of the time, it still remains to implement an organization in line with the objectives assigned to the Security Director.

The Business Security Directors' mission is complex and extensive. They must simultaneously identify new risks related to the most sensitive or valuable assets of their companies while ensuring the protection of their employees and their customers, fight against image or reputation damage and finally prevent all forms of malicious acts perpetrated in the physical world or in cyberspace. The scope of a Business Security Director's mission is wide and the global security approach, which everyone calls for, is not the daily routine of a number of them, faced with a breakdown of responsibilities with expertise that can be exercised in other directions.

Nevertheless, the CDSE's study on the professions in the corporate security sector<sup>1</sup> shows that 75% of CSOs are attached to the senior management, the general secretariat, or the board of directors. This allows a significant number of Security Directors to influence the strategic decisions of companies and to be real "business partners". This new internal positioning acquired thanks to the decisive role taken during crises (attacks, covid, internal incidents, risk prevention...) reinforces the decision-making role of the latter. This internal legitimacy gained from the management and the professions is also reflected in a new external visibility promoted by the lobbying of the CDSE with the policies and services of the State.

The CSO is therefore both the representative and the interlocutor of his company with the institutions in the first rank of which, the Ministry of the Interior, and becomes de facto partner of the security *continuum*. It is this role that Minister Christophe Castaner recognized in his speech mentioned above

#### THE ROLE OF SECURITY DIRECTORS IN THE CONTINUUM

The role of Security Directors in the security *continuum* has therefore found full recognition in the conceptualization work carried out by the State since 2018. Nevertheless, the presence of a Business

Security Director today depends solely on the will of the company that decides to invest in considering the security risk. Functions of the Business Security Director make him the legitimate interlocutor of the state security services. This recognition constitutes a first link in the *continuum* chain. For some particularly exposed companies, the idea of this professional being authorized as "security clearance level" has flourished. This is also the case regarding the State, more particularly the SGDSN<sup>2</sup>. Nevertheless, although the idea of creating such a "circle of trust" has been taken up and presented in different instances, it has not yet found fruition.

Security Directors are therefore called upon to become the focal point for the desired collaboration between the public security forces and the private sector. They are therefore expected to report to the various state services the information they have and potential issues they encounter (weak signals, suspicions of radicalization...). These exchanges have existed since the arrival of the first Security Directors in companies and benefit from legal guidance for Business Security Directors working in OIV<sup>3</sup>, due to their status as a Chief Security Officer. For others, this exchange of information is often structured around personal networks relating to the director's past career (in institutions or law enforcement) or to bridges built empirically at the heart of a crisis. However, although the exchanges exist, they often remain unilateral, with Business Security Directors rarely receiving feedback on the reported situations. In this regard, the lobbying of the CDSE, however, makes it possible to bring together the directorates and services of the State (SGDSN, ANSSI, Police, Gendarmerie, intelligence services...) and Business Security Directors on the occasion of sectoral commissions and conferences.

However, the *continuum* can also materialize through local and pragmatic initiatives: since December 2018 and the beginning of the so-called "Yellow Vests" movement, the CDSE has been attending a meeting led by the Paris police prefect every week ahead of the demonstrations. The information shared allows companies to anticipate and better protect themselves against malicious acts that may accompany these movements.

Companies can also raise their points of attention with the services of the Paris Police Prefecture in a "win-win" exchange.

<sup>1</sup> See: "The Security Director: a strategic function at the heart of a wide ecosystem of actors and skills", page 18.

<sup>2</sup> SGDSN: Secretariat-General for National Defense and Security.

<sup>3</sup> OIV: Operator of vital importance.

A second link of the *continuum* is embodied in the new training courses on corporate security that have been developed and bring together a mixed audience composed of public officials and private employees. These high-level courses offered at IHEMI, IHEDN, ENSP and EOGN make it possible to perfect a form of mutual knowledge and to highlight the contributions of the private and public in terms of security. These trainings illustrate the porosity now assumed between public and private security, as well as mutual needs. But in a context of permanent, terrorist, or economic threats, companies also benefit from awareness-raising actions by state services, such as the DGSI (General Directorate for Internal Security) or Territorial Intelligence, which make it possible to spread a common culture on issues such as economic interference, radicalization, cybersecurity, and thus to associate and empower at the highest level of the company. Business Security Directors are often the initiators of these interventions and thus become de facto the natural interlocutors of the requested services.

Finally, the *continuum* security is illustrated by the ability offered to security directors to request, anywhere in the territory, security referents, police officers and specialized gendarmes, in order to be accompanied on issues specific to their assets, in terms of the optimal level of security to be implemented for certain sensitive sites or the installation of video protection systems.

The intervention units of the police nationale and gendarmerie nationale, the RAID and the GIGN, also offer a chance for Business Security Directors working in groups particularly exposed to terrorist risk, to share a mapping of their company's assets. The goal is to be able to intervene in the event of a crisis by knowing the geography of the buildings, while benefiting from a privileged and mobilizable interlocutor, the corporate Security Director.

Abroad, the Business Security Directors of large French companies can count on the network of internal security attachés, present in each embassy, and managed by the International Security Cooperation Directorate (DCIS). The latter allow them to have information on the state of threats but can also lend them support and assistance in certain situations that expose their employees.

#### THE PLACE OF THE BUSINESS SECURITY DIRECTOR IN THE CONTINUUM IS YET TO BE CONSOLIDATED

The *continuum* and the new public-private association that it promotes no longer poses an issue and seems to have aligned itself in the direction of history. But the modalities of its implementation have yet to be specified... and especially for corporate Security Directors.

The formalization of the *continuum* often leaves it to companies to be proactive and make themselves known to the State services (regardless of the OIV and the largest of them that benefit from their notoriety). Business Security Directors working in these “less visible” companies must therefore have a proactive approach and go to meet the various regional interlocutors, as the security services are often unaware that such professionals exist.

The level of relationship also remains subject to regulatory obligations. The “circle of trust”, which today only some of these professionals working in OIV and OSE benefit from<sup>4</sup>, must extend to all corporate Security Directors. Thus, for the directors who might request it, the implementation of the “security clearance level” authorization, requested since 2011 and the first “CDSE White Paper”, would be a strong signal and would fuel the momentum. A relationship of trust is not decreed, it is built over time. In fact, the *continuum* cannot exclusively rely on the existence of interpersonal relationships that make it possible to obtain information. Security Directors, by the functions entrusted to them, are trusted partners and must “be able to know about them” but also “be able to share them”.

The issue of the simple census and identification of all these professionals, in each company, remains a pitfall for which no solution has been imposed to date. The issuance of a professional card by the CNAPS<sup>5</sup>, mentioned by some observers, cannot be satisfactory insofar as it would mean entrusting the careers of the client and their service provider to the same public regulatory institution. If the client must act with full responsibility, the function of the Business Security Director within a company is neither regulated nor regulatable: it cannot fall within the scope of control of the CNAPS<sup>5</sup>. However, a voluntary register of Security

<sup>4</sup> OSE: Operators of Essential Services.

<sup>5</sup> CNAPS: France's National Council for Private Security Activities.

Directors for the Ministry of the Interior would have the advantage of making them visible and accessible to the services. And therefore, make it possible, at all times and for all sites, to have a high-level interlocutor capable of getting them to open every door of the company when needed.

The *continuum* must also be embodied and facilitated in order to be anchored in the security landscape in France. The Ministerial Delegate for Partnerships, Strategies and Security Industries (DPSIS) of the Ministry of the Interior plays this role of interface and facilitator. But its role could be strengthened by becoming the real entry point for all the sectoral demands of Business Security Directors.

### TAKING INSPIRATION FROM CSR TO PROMOTE THE POSITIONING OF THE SECURITY FUNCTION: INTEGRATING SECURITY INTO THE COMPANY'S LISTING CRITERIA

By adopting the CSR (Corporate Social Responsibility) model, considered for several years by the Banque de France as a **“lever of transformation of practices and governance, vector of innovation and generator of efficiency in the long term”**, security could be integrated, as had been proposed at **the 2019 CDSE conference**, in the scoring of the company to have a more global vision of it, better understand it and thus refine the analysis of its resilience.

Security could, whenever the information collected allows it, be taken into consideration to assess the overall profile which makes it possible to refine an extra-financial criterion. The fact of giving this new role to security would favour the positioning of the Security Directors and would encourage the CEOs to invite them to sit on the management committee or the board of directors.

To publicize the missions of Business Security Directors, the training of police and gendarmerie managers should include a module on corporate security. Directors could get involved there to train the officers on the specificities and constraints of their profession and, by doing so, to promote future exchanges.

Although the *continuum* has become a little more efficient, especially with the action of the Ministry of the Interior and ministries that historically deal with corporate security issues (Prime Minister, Armies, Europe and Foreign Affairs, Economy and Finance...), it has little materiality with others (Health, Work, Culture...), except through the action of Senior Defence officials, yet at the forefront in the management of the health crisis or the terrorist threat. Moreover, in the security of everyday life, there is little or no link between companies and the representations of these ministries in the territories.

In 2020, the propositions of the Fauvergue-Thourot report were able to find a new echo in the White Paper on Homeland Security. This document, the result of a broad consultation conducted by the Ministry of the Interior, proposed developments to take into account all actors and a global approach to internal security issues. It positioned *“corporate Security Directors as stakeholders in the security continuum”* and proposed *“to strengthen their recognition as such “by setting up” a relationship of mutual trust sharing professional secrecy”*. Nevertheless, these recommendations have not been implemented in the law of 25 May 2021 for a *“global security preserving freedoms”*. This text, although tabled by MPs Thourot and Fauvergue, deals with all the contributors to the *continuum* (police municipale, private security, state security forces...) yet omitting companies.

However, private companies are the first actors in their own security and safety, as well as that of their stakeholders (employees, customers, service providers...) and, therefore, they are the first purchasers of private security. Corporate Security Directors thus participate every day in the *continuum* through the actions, missions, and schemes that they implement.

The State and companies must now bring them closer together in a concrete way, in order to get to know each other better, develop regular interactions and establish mutual trust. “*We are consulted more and more, and very often we are more listened to than heard. However, there is no doubt that it is possible to do even better*”, indicated Stéphane Volant, president of the CDSE, in an interview published in October 2021. This “better” must finally be materialized by law, in a text that enshrines the function of corporate Security Director and the role that these professionals daily play in companies.

Because companies are never just an extension of the territory of the Republic.

And Security Directors are strong links of the global security chain, of the security *continuum*. ■

<sup>6</sup> Interview with Stéphane Volant, President of the CDSE, *Le Monde de la sécurité*, 14 October 2021.

## RECOM > MENDATIONS

- > Integrate modules dedicated to business security into the training of executives of the police nationale and gendarmerie nationale.
- > Strengthen the role of the DPSIS of the Ministry of the Interior as facilitator of the *continuum* for Security Directors.
- > Allow voluntary registration of Security Directors with the Ministry of the Interior as part of a census and identification effort.
- > Define Business Security Directors as stakeholders in the security *continuum* and strengthen their recognition as such by law.
- > Facilitate the exchange of public/private information in a “circle of trust” built on professional secrecy or a clearance process.



## **WHAT SKILLS ARE NEEDED FOR TOMORROW'S SECURITY DIRECTOR ?**

### **AURÉLIEN LAMBERT**

*Security Director of the Egis Group*

The pressure is continuously increasing on security issues in organizations. Due to the complexity of risks and the need for trust that this phenomenon has entailed for stakeholders, the issue is recognized as strategic. Thus, more companies, of all sizes and in all sectors of activity, are deciding to appoint a Security Director to strengthen their capabilities or their positioning.

**T**he role of security director<sup>1</sup> has become a profession and is gradually being normalized to meet these needs. The position is progressively evolving from a technician role, linked to the application of regulatory constraints, to that of a conductor, directly supporting activities..

With this evolution, the Security Director in France still remains on their own when it comes to training, structuring the role or defining standards for their organization. While the pressure is increasing, a key issue in the coming years to continue this increase in competencies will be collective work carried out by the professionals themselves.

### **A FUNCTION THAT IS SLOWLY AND DIVERSELY DEVELOPING IN FRANCE**

When we analyze the past decade, we note a certain contradiction. On the one hand, there have been many disruptions in the private sector environment: terrorism at home and abroad, Covid-19, Ebola, serial natural disasters, acceleration of the threat by the cyber vector, trade war between the USA and China, Brexit, agreement then rupture with Iran, armed conflicts in the Levant, Mali, Libya, Ukraine, etc.

Despite these events, we have observed a relatively slow progression in the role of the Security Director in France. The function remains mainly based on the same jurisprudence as ten years ago, and therefore often associated with a rationale of regulatory constraint, rather than a rationale of investment for the benefit of organizations and their activities. There are many reasons, probably relating to a lack of alignment of professionals in the sector, to a carelessness of many organizations, to the lack of vision of the State on the opportunity of the security *continuum* to protect its economic fabric. Yet organizations are often on the front line in the face of increasing risks. The acceleration of threats by the cyber vector has led to an awareness among many leaders and within the state. This leads each organization to organize and invest in a truly diverse way. Thus, the lines of attachment, perimeters, degrees of authority, team sizes, budgets, etc. of Security Directors vary greatly, depending on the organization.

<sup>1</sup> "Sécurité" is understood in this article as covering one or more topics that may come together under this term. Depending on the organization, this scope can vary and integrate safety, health, security, information security, crisis management, business continuity, etc.

#### **THE COMPLEXITY OF RISKS LEADS TO A NEED FOR TRUST**

Far from simply adding up, risks are interwoven and multiplied. Consequences of Covid-19 illustrate this perfectly, and all organizations have been affected. A health risk for employees gives strong incentives to change working methods, because it increases the threat in terms of cybersecurity, fraud, psychosocial risks, etc. But the pandemic is also increasing the risks to supply chains, reputation, compliance, and the political and geopolitical environment. Issues, and therefore expertise, which were often considered separately now intersect, are interdependent, just like the globalized, reticular world.

The uncertainty brought by the risk complexity leads to a need for trust on the part of stakeholders, whether they are internal or external to the organization. Customers, insurers, regulators but also employees, risk and audit functions, demand guarantees of security and resilience. The blank check and discretion that have sometimes surrounded the security function in France are turning into a requirement for results and transparency. The Security Director is thus gradually taking on the strategic dimension that belongs to him in an increasing number of organizations.

#### **THE SECURITY DIRECTOR, A SERVICE IN TRANSITION BETWEEN THE POSITION OF “TECHNICIAN” AND THAT OF “CONDUCTOR”**

Trends of increasing risks and the need for trust lead the Security Director to gradually move away from technical issues. Because they cannot have all the keys to cybersecurity issues, health measures, physical protection of infrastructure, business continuity, etc. They must understand them enough to combine them in a coherent way, to give each one a direction, a rhythm. They orchestrate a dynamic between different functions, on multiple topics, at several levels of their organization and within an often-international geographical perimeter. This new position however, is not a novelty, as it has been internationally observed for several years already, especially among the Anglo-Saxons with the creation of the role of “Chief Security Officer”.

It is thus possible to lay out skills that become necessary for the Security Director in this evolutionary process. This list does not claim to be exhaustive but rather to highlight those that become unavoidable. These skills complement the invariable ones, such as mastering the security risk management process, understanding the legal aspects of the role, etc.

- > BUILD A STRATEGIC VISION SPECIFIC TO YOUR COMPANY:** faced with complexity, the first challenge is to methodically prioritize action. This can only be done with a deep knowledge of the organization, its sector, its risks, formal and informal decision-making centres, and the company’s strategy. The Security Director must thus grasp all the complexities of their organization in order to propose a realistic security strategy, aligned with the company’s priorities.
- > MEASURING GOALS AND RESULTS:** like any role, investments require identifying a target to be achieved and regularly measuring progress through clear performance, risk and control indicators (the “KPI, KRI, KCI”). This leads the Security Director to quantify their action even more and make it intelligible to the company.
- > REASSURE, CREATE A COMPETITIVE ADVANTAGE:** the methodical approach, an in-depth knowledge, sometimes reinforced by certifications (ISO 31030, 27001, etc.) should make it possible to meet the need for stakeholder trust. The Security Director has the opportunity here to position their subject as a competitive advantage, which will strengthen the business posture of the service.
- > BRINGING TOGETHER AND MOTIVATING A COMMUNITY:** faced with more complex risks, the scope and interdependencies are increasing. The team in the broadest sense (direct, indirect, internal, external) is expanding and is enriched with experts from multiple disciplines and horizons. The Security Director identifies, gathers, coordinates, and motivates these resources so that their actions complement each other to cover the organization’s risks. For this, the Security Director adapts to interlocutors who have very different visions, languages, cultures, from the geopolitical analyst to the SOC (Security Operation Centre) specialist, to the data analysis expert, to the project manager, to the internal control manager, to the risk director, to the legal director, etc.

- > **EMBODY AND INFLUENCE:** since organizations often constitute a matrix structure, the security department rarely has very strong vertical authority. In opposition to this organizational constraint, the risks (cyber, health or terrorist) nevertheless require employees to be permanently vigilant. It is therefore through influence that the security department must change individual behaviours at all levels of the organization, from members of the board of directors, to managers, to employees and subcontractors. It is also through their influence and ability to embody that they will be able to defend their issues vis-à-vis the boards of directors, general managers, financial directors, and therefore get the resources needed.
- > **HAVE A SOLID “BUSINESS ACUMEN”:** like any role in an organization, the Security Director must adapt to its objectives, its hierarchy, its culture, its processes. A full understanding of the activities, priorities, constraints, formal and informal rules is required. The Security Director masters the transversal processes of budget management, human resources, project management, compliance, performance, etc. Finally, they are fluent in English and office automation tools at advanced levels. On all these aspects, the Security Director cannot perform worse than his peers in the organization: this is a condition of his credibility vis-à-vis his stakeholders.
- > **STAY CLOSE TO THE REALITIES ON THE GROUND:** the complexification sometimes tends to develop an administrative approach to security, through dashboards and reports. Although these are essential tools, if the Security Director relies only on these, they run the risk of detaching themselves from reality. It is crucial to maintain a regular, personal link with the operations side. Agreeing to regularly and realistically test your organization makes it possible to measure progress and detect potential flaws in order to adjust their action. Knowing the reality of the field also makes it possible to adjust the measures to be put in place, to meet the needs of operations.

#### THE INCREASED COMPETENCIES REQUIRES MORE COLLECTIVE ACTION

In France, the role of Security Director has slowly evolved in recent years and still lacks structure. Today, under the effect of the risk complexity and the resulting need for transparency for organizations, the pressure is increasing and is now having an impact on the entire French economic fabric, especially under the effect of the cyber threat, Covid-19, and the Ukrainian conflict. This allows the role of Security Director to continue its recognition in organizations and therefore its standardization and professionalization.

To continue - or even accelerate - the development of the role and the increased competencies that accompanies it, the Security Director must be able to have access to training courses, organizational or technical references, good practices, experience sharing, recruitment channels, etc. By way of comparison, several models have been observed that have allowed this evolution to take place internationally. In the United States, the centrality of the ASIS (American Society for Industrial Security) has made it possible to structure this sector, even becoming an international benchmark. Another example is the regulation of the role of Security Director in Spain, through the private security law of 2014, which gives a framework to its missions, training, and skills.

Taking inspiration from these examples, the essential first step is therefore to strengthen professional associations and their alignment (CDSE, ASIS France, CESIN, Clusif, etc.). This will make it possible to have the necessary debates between security professionals, either to proactively define a common framework, or to closely collaborate with the State to regulate the role. Time is running out, because recent events in Ukraine show that changes are happening faster than ever. It is up to professionals, then, to keep abreast of these developments and to propose solutions that make it possible to best protect our organizations. Otherwise, the risk is that the State will apply a framework that does not match the need. ■

# RECOM > MENDATIONS

## > GO BEYOND THE PURELY TECHNICAL ROLE

To meet the needs of their organization, the Security Director must understand the general context and participate in the realization of the company's strategy. Technical aspects do not disappear but are subordinated to the "business" objectives that need to be achieved.

This can mean, for example: encouraging knowledge sharing at all levels of the organization between the security role and the strategy, finance, legal, etc. roles to develop closer links between stakeholders.

## > EMBRACE THE COMPLEXITY AND BRING CLARITY

Organizations, society, and risks are ever-changing.

In this complexity, an added value of the Security Director is precisely the ability to identify priorities and give transparency to decision-makers and stakeholders on the real level of risks and the actions to be taken.

## > DEVELOP THE CENTRALITY OF PROFESSIONAL ASSOCIATIONS

The Security Director in France will strengthen their own legitimacy and approach if these are backed by solid and credible professional associations.

# 18

## STRUCTURAL **RECOM >** **MENDATIONS**

# 18

## STRUCTURAL RECOMMENDATIONS

FOR A SECURITY FUNCTION THAT IS STRATEGIC TO THE COMPANY & FULLY INTEGRATED INTO THE SECURITY *CONTINUUM*

### FOR A STRATEGIC & TRANSVERSAL SECURITY ROLE AT THE SERVICE OF BUSINESS

#### 1. INTEGRATE THE CORPORATE SECURITY DEPARTMENT INTO THE COMPANY'S GOVERNANCE

By being attached to the senior management and/or to a member of the board of directors.  
For > [Business leaders](#)

#### 2. DEVELOP A GLOBAL & ETHICAL SECURITY POLICY

By addressing all areas of security & safety: security of people and tangible and intangible assets, cyber, strategic intelligence and economic security, supply chain, fraud and compliance, international, crisis management and operational resilience, radicalities.  
For > [Security Directors](#)

#### 3. MAKE YOURSELF KNOWN & RECOGNIZED WITHIN THE COMPANY

The Security Director must put themselves at the service of all departments of the company and bring concrete added value.  
For > [Security Directors](#)

#### 4. SEIZE THE INTERNATIONAL TOPIC TO INTEGRATE IT WITH THE NEEDS & STRATEGY OF THE COMPANY

As a transversal actor, the safety and Security Director benefits from a 360-degree vision to better compete internationally in the long term.  
For > [Security Directors](#) > [Business leaders](#)

#### 5. ENTRUST THE SECURITY DEPARTMENT WITH A MAJOR ROLE IN FACILITATING CRISIS & BUSINESS CONTINUITY SCHEMES

The Security function has in its DNA the capacities of anticipation, reactivity, transversality and organization essential for crisis management and business continuity.  
For > [Business leaders](#)

#### 6. SENSITIZE FUTURE BUSINESS LEADERS TO THE ROLES & FUNCTIONS OF SECURITY

By developing an educational strategy for higher education (ENA, Sciences PO, business and marketing schools...).  
For > [Security Directors](#) > [Business leaders](#) > The CDSE and the actors of the profession

#### 7. STRENGTHEN THE PROFESSIONALIZATION OF THE CORPORATE SECURITY SECTOR

Through dedicated training courses and career paths integrating mobilities external to the sector in the company and with institutions.  
For > [Security Directors](#) > The CDSE and the actors of the profession

## FOR A SECURITY DIRECTOR INTEGRATED INTO AN EFFECTIVE AND PRAGMATIC SECURITY CONTINUUM

### 8. CREATE A PUBLIC-PRIVATE “CIRCLE OF TRUST” BUILT ON PROFESSIONAL SECRECY OR A CLEARANCE PROCESS THAT PROMOTES INFORMATION SHARING

By establishing Security Directors as key players in the security *continuum* and privileged interlocutors of law enforcement and the State in the Company.

For > Public authorities

### 9. INTEGRATE MODULES DEDICATED TO BUSINESS SECURITY INTO THE TRAINING OF EXECUTIVES OF THE POLICE NATIONALE & GENDARMERIE NATIONALE

For > Public authorities > The CDSE and the actors of the profession

### 10. DEVELOP EXCHANGES BETWEEN SECURITY DIRECTORS, THE CNAPS<sup>1</sup> & THE DPSIS<sup>2</sup>

In particular within the framework of the advisory mission of the public institution regulating private security activities, as well as for a more direct relationship between Security Directors / purchasers and the Ministry of the Interior.

For > Public authorities

### 11. FOLLOW THE RECOMMENDATIONS OF THE CDSE TECHNICAL BOOKLET “SECURITY SERVICES: GUIDE FOR THE CONTRACTING AUTHORITY” TO PURCHASING PRIVATE SECURITY SERVICES

Define the positioning of human surveillance in the company’s overall security strategy, entrust the management of the tender process to the pair of “Purchasing” and “Security” roles, prioritize the “better bidder” rather than the “lowest bidder”.

For > Security Directors > Business leaders

# 18

## STRUCTURAL RECOM > MENDATIONS

### 12. REFORMING PROFESSIONAL TRAINING IN PRIVATE SECURITY

To enhance the skills of agents, to create a real profession of private security supervisor, to improve the quality of the offer and services.

For > Public authorities

### 13. ESTABLISH A FINANCIAL GUARANTEE-TYPE MECHANISM FOR PRIVATE SECURITY COMPANIES

To ensure the financial capabilities of private security companies and the willingness of their senior management to register sustainably and responsibly in this market.

For > Public authorities

### 14. STRENGTHENING STATE ACTION IN THE FIGHT AGAINST COUNTERFEITING

By implementing the recommendations of the Blanchet-Bournazel report on the evaluation of the fight against counterfeiting<sup>3</sup>.

For > Public authorities

<sup>1</sup> CNAPS: France’s National Council for Private Security Activities.

<sup>2</sup> DPSIS: Ministerial Delegate for Partnerships, Strategies and Security Industries.

<sup>3</sup> Information report of the Evaluation Committee of the National Assembly presented by delegates Christophe Blanchet and Pierre-Yves Bournazel in October 2020.

## **FOR CONTROLLED CYBERSECURITY & SECURITY TECHNOLOGIES**

---

15.

### **ADOPT A SYSTEMIC APPROACH TO THE STRATEGIC POSITIONING OF THE ISS IN THE COMPANY**

To try and define a typical organization, where the Information Security System (ISS) of the company must be the responsibility of the Security Director or not, is illusory. Each company has its own organization according to its sector of activity, its history and its culture.  
For > [Security Directors](#) > [Business leaders](#)

16.

### **INTEGRATE & PROMOTE SOVEREIGNTY CRITERIA IN THE CHOICE OF DIGITAL SOLUTIONS**

Choosing to turn to sovereign digital solutions means limiting the risk of malicious digital interference and better protecting your data.  
For > [Security Directors](#)

17.

### **INTEGRATING ISS BY DESIGN OR THE IMPLEMENTATION OF NEW SECURITY TECHNOLOGIES**

The help of ISS experts is essential to guarantee a secure network architecture as soon as new security tools are installed.  
For > [Security Directors](#)

18.

### **PROVIDING SECURITY TECHNOLOGIES WITH A LEGAL FRAMEWORK**

Under the strict control of the CNIL to guarantee the protection of public and individual freedoms.  
For > [Public authorities](#)





161 boulevard Haussmann  
75008 Paris  
01 72 31 73 18  
[contact@cdse.fr](mailto:contact@cdse.fr)

**cdse.fr**