Club des Directeurs
CDSE
de Sécurité des Entreprises

WHITE PAPER

The Security Department and the Chief Security Officer in Corporate Businesses

Issues and answers


SÉCULIÈREN
SECUNDO
deuxièm
SÉCURITÉ
dée qui
comme
SEDAN.

CDSE

Club des Directeurs de Sécurité des Entreprises
(Club of Business Security Directors)

Over the years The CDSE has become a major European association gathering Corporate Security Directors from over 80 international companies. Their daily commitment contributes to the definition of norms and the building of a security community sharing experiences and ideas.
Presided by Alain Juillet, former National Head of Business Intelligence who succeeded to François Roussely, former CEO of Électricité De France, the CDSE intends to be :

- a European network and think tank of actors working in the corporate security field, thanks to the annual seminar organised at the OECD headquarters, or through its eight specific commissions ;
- a platform for technical support and network building for its members ;
- a vector for disseminating the specific knowledge about security, through the magazine "Security and Strategy" and the CSOs Newsletter edited by the CDSE ;
- a prime interlocutor with the public sector, as demonstrated by trusted partnerships with the SGDNS, ANSSII, the DCRI (MI5), the Ministry of Defense and the Crisis Center of the Ministry for Foreign Affairs.

White Paper
CDSE, Paris
December 2011

Publishing Director
Olivier Hassid

Editorial Staff
Mathieu Pellerin/Julien Marcel

Graphic Design
Aurélie San Emeterio
www.pointcommun.fr

Photo credit
Vincent Gérard

Printing
Morvan Fouillet imprimeurs

MAIN

TOWARDS COMPANIES

- Identify each business' vulnerabilities in matters of security and define policies to mitigate them.
- Help the Security function evolve towards a more global role, including risk and crisis management.
- Have the CSO report directly to a member of the Board to reinforce his/her position throughout the company.
- Position the role in a global and open process.
- Integrate security topics in future managers' training.
- Generalise security feedbacks and share them with other departments.
- Ensure all the personnel's safety wherever they are, home or away.
- Ensure the implementation of ethical principles in security policies.

TOWARDS AUTHORITIES

- Promote security classification of " business/corporation confidential " by the government.
- Bring the law on the " business secrets " to the European level in order to harmonize and regulate company practices.
- Create a public/private and governmental think tank on existing norms related to business security with a European and international perspective.
- Involve the CDSE in the drafting of all legislative and regulatory texts on corporate security.
- Communicate upstream all sensitive information related to a company to concerned CSOs.
- Include companies represented by an accredited CSO in all governmental crisis management cells.

SUMMARY

3 NEW STAKES FOR SECURITY

CONCLUSION

Note to the English Readers

The original texts sometimes use the words "sécurité" and at other times "sûreté". Contrary to the English language, the two terms may be used in France approximately for the same scope and do not cover exactly the same meaning as "security" and "safety" do in English.

The trend however is to use "sûreté" for security, and "sécurité" for safety. The two words are more than once used indifferently to designate one same world : business protection.

The choice in French may vary according to the size of the company, its core business or still the exact scope of the CSO. Consequently in the following texts some of them will use "sécurité" while others prefer "sûreté", or still "sécurité/sûreté" to better respect the name of their function within their company and give a more precise idea of their scope.

When possible, the translation will sometimes target sécurité or sûreté where the meaning is made obvious by the context.

INTRODUCTION

ALAIN JUILLET

President of the CDSE

Alain Juillet

President of the CDSE

Presided over numerous French and international companies before being nominated Director of strategy for the DGSE (French MI6) from 2002 until 2003. He then created and occupied the function of High Delegate to Business Intelligence, reporting to the Prime minister. After that he integrated the lawyers firm ORRICK as a senior consultant. He was raised to the grade of "Commandeur de la Légion d'honneur" on July 14th 2009.

Do you remember those old western movies in which you had this sympathetic character of the scout accompanying the troops and the immigrants to their promised land ?

He knows the terrain, his way around, the local populations and their customs, the specific risks of the region and its environment as well. Cunning but loyal, seasoned, he contributes to the success of the adventure by defining with the head of the convoy a strategy to avoid the traps, and what direction to follow. Without him the success of the group is largely hypothetical. He does not pretend to take the place of the soldiers. He does not take too much interest in the travelers' businesses except when robbers try to interfere with the caravan. Staying aside, or slightly ahead, he guarantees the safety and security of the trail and the possible success of the trip.

This is exactly the role of the Corporate Security Director today. And for a CEO it would be as unwise to do without him as it would have been yesterday to engage into such trips to unknown territories without his advice and expertise.

Today the risk and the dangers are everywhere. Indians, thieves, snakes, booby traps are even behind the frontline most of the time. Through globalization, information technologies, risks have been multiplied precisely when our societies were promising more and more security for everyone and imposed on CEOs and companies to participate in the global production of security by a whole array of texts. Laws and jurisprudence are more and more constraining whereas Fort Apache has physically disappeared. It has been replaced by a virtual world, ever changing, polymorphic. The truth is eluding us. Trust is not here anymore. Contracts are not enforced.

To confront this unstable and elusive world, the temptation may be great to go one's way with a good insurance only, praying all along the sky does not fall on one's head. Yet solutions exist to mitigate those challenges. It is important to knock on the right doors though.

These are the stakes of this White Paper.

This paper wants to convince entrepreneurs as well as the public sector that the Security Director of a corporate company has know-how, the experience and the expertise required to thwart most of the risks encountered in his/her daily activities.

Reading the following texts will amply demonstrate this. Not only they show the capacities of the Chief Security Officers, CSOs, but they also explore prospective ideas that honor this new profession that is now fully expanding. The CDSE is happy to commit itself to fostering them with a public not always aware of this role, its content and its usefulness.

The CSO is neither a "barbouze", as we say in French, i.e an ex villain of some weird army corps, nor a man or a woman coming from the shadow, or still a nuisance or an aging civil servant taking his retirement in the private sector. He/she directly contributes to the wealth of the company by his specific knowledge which he/she maintains at its top for the accomplishment of his daily duties
There is no doubt to me that the current CSOs will consequently accept the challenge, demonstrate their capacities and definitively recognise this function as an absolute necessity. One day, one will even wonder how we could have done without it before.

This last remark is an opportunity to underpin two things I truly believe in, and which act as a watermark in this White Paper.

■ The State cannot provide all the security needed by businesses. The State is even shying away from it for many reasons that would take too long to explain here. It is therefore up to businesses to guarantee their own security, even those which have the luck to be retained on the sensitive infrastructures list (which could beneficially be reviewed by the way). One cannot import or duplicate all the government's services into one's company. Every man has his trade ! What we want to do is encourage the creation of multiple windows between the public and the private sectors which in France tend to ignore one another when they are not too close, which is equally damaging. The ethics of these return moves between the two worlds - public and private - is at the core of the CDSE and its members' thoughts. Security and corporate social responsibility will become increasingly overlapped as the borders between general and private interests will be increasingly blurred.

■ The profile of the CSOs will consequently evolve in coming years. On one side we will find all the managers of physical, IT, IP etc, security. These technicians need a highly specialized knowledge as laws, regulations, good practices ceaselessly raise the level of compliance. Without that specific knowledge, companies would be at risk in terms of reliability. It is not surprising that now some companies even recruit Compliance Officers whose level may be very high in the organisation. On the other hand there will be a need for a conductor of all these specific jobs so the score be well rendered in harmony by all the musicians of the security field. These conductors are required to possess a strong sense of strategy and a good capacity to "sniff out" unexpected dangers and mitigate them.

This is the new scope of global security, should we say resilience ? A scope without definite borders but that surely goes far beyond compliance only. Reporting to the highest level in the company and why not a member of the board, this CSO must have the budgetary means and the personnel to address all the issues that will come and to accompany his/her strategy of safeguarding commercial activities.

The road ahead is still long. This White Paper is only a first step, many others will follow. At least the goal is fixed.

Enjoy your reading, most especially if you are a CEO still pondering what use there is for a CSO. Be sure that these strange people in security are not trying to annoy you, but on the contrary, they will help you across Indian territories. Trust them ! ■


DÉFINITION

1 DEFINING SECURITY

SAFETY AND SECURITY IN BUSINESS STRATEGY

Éric Le Grand

Director of Prevention and Protection at RENAULT SAS

Eric Le Grand has spent all his career in security roles in corporate businesses including the department of security/safety at LA POSTE.

Over the last decades the liability of enterprises has been evolving in an ever more constricting environment. Laws, norms and regulations have multiplied. Consequently, business had first to learn how to control its own risks, i.e. those regarding its own activity (work accidents, process incidents, health, etc). As for outside risks and protection against external threats, whether they be from Nature (earthquakes, pandemic diseases), geopolitical (war, terrorism...) or criminal (loss, break-ins, counterfeiting, industrial spying) most companies were expecting states in which they were operating to guarantee their security.

Take 9/11, or still the Karachi jurisprudence (a case where a French company - DCN, lost 11 employees in a bombing in Pakistanand where the court stated that the employer had an absolute obligation to protect its personnel even abroad), threats of pandemics, or still the nuclear and earthquake disasters in Japan : all these events have entailed that companies now have no choice but addressing questions of security to mitigate their liability.

Businesses are indeed faced with new forms of risks. They operate in unstable environments, are targeted by all sorts of prowlers, but it is mostly because of the way they have oriented their organisational strategies that they have become more fragile. The interdependencies for their activities, their outsourcing or the extensive use of providers for vital functions, the shortening of supply chains, the entire dependency on IT technologies, globalization, severe competition, all these have weakened companies so that the least impact on any point of the chain may have critical consequences for clients, personnel, assets, physical and information assets, reputation, but also for the global resilience of the civil society to which the business contributes.

SECURITY AND SAFETY AT THE CORE OF THE COMMAND AND CONTROL OF RISKS

To do business is always risky. With no other choice than moving forward, companies that do not take risk (new products, new markets, new organisations) will no longer be here tomorrow. And it will be the same on the opposite side for those companies that have taken too many risks. The right amount of risks and how to control them is therefore at the very core of the entrepreneurial strategy.

Companies must, before taking any decision, analyse, assess and anticipate risks. When implementing a strategy they have to prevent them from happening, and in case they do, set up continuity plans and crisis management processes. Security and safety are the indispensable companions of risk taking. The safety/security function that used to play an underdog role in companies comes now on the forefront of the strategy.

SECURITY AND SAFETY AT THE HEART OF GOOD GOVERNANCE

The reading of many codes of conduct or of governance rules posted by numerous companies show that security and safety have gained a fundamental role in good governance. Obligations regarding the clients integrate security and safety as by products of proposed services and goods. Obligations toward stakeholders also impose a keen watch on security and safety of personnel and all other assets. Safety at work, security of travel is the very basis of the liabilities owed to the personnel. As for the continuity of activities or still the contribution to the resilience of the states in which companies are settled, they are now part of the duties of care all companies must show towards civil societies. To be well governed, a company must be safe and secure.

SECURITY AT THE CORE OF SUSTAINABILITY POLICIES

Huge projects have been launched these past years among corporate businesses regarding quality but also sustainable development. How can you boast the quality of a product when it is not safe ?

A system of information must also be secure and safe to guarantee its quality and continuity. It is the same with sustainability policies that rely mostly on the safety of products and security of processes. In risk assessment, the hazard of an accidental pollution is not the only danger any more, one also has to envision all sorts of crimes or even terrorism.

It is usefull therefore to remind everyone that any quality process is built on a pre-requisite : safety and security.

SECURITY AND SAFETY AT THE CORE OF TRUSTWORTHINESS

A bad Security organisation does impact the global results of a company. A bad security indeed threatens the responsibility and reliability of the business, damages its image and that of its top managers'.

Giving information and non-financial facts on a voluntary basis to stake holders (shareholders, consumers, employees, governments), has become a major part of annual reports. It is as of now a crucial element of trust. Among the information pieces that are required, social and environmental data are usually the most common ones. Up to today though, there is no specific chapter for security and safety even if they are relevant indicators of the way a company commands and implements its strategy of risk taking.

Security and safety have turned out to be a major stake for trust and competitiveness. ■

Operational recommendations

- Promoting the setting up and implementation of a rating scale regarding safety and security assessing the strategies, policies, organisation and action plans and results in this domain seems a very important goal to evaluate the businesses good governance. The CDSE can use the conclusions of its working group "grading and rating commission" to achieve this goal.

- Underscore the importance of security for the benefit of CEOs and the whole business so that Security becomes a vital function. The CDSE plays a unique role in this field and extends it to CEOs and professional organisations that represent them to better assess security strategies.

- Integrating security and safety in the training of future managers is also one of the goals of the club, as is fostering the necessary evolution of laws and regulations in this field, which is made possible through the expertise of its members.

Pascal Crépin

Group AIR LIQUIDE
Group Security Director

Graduate of the ESLSCA Paris, attended business intelligence sessions at IHEDN (French Institute for Advanced Studies On National Defense (military)), he started his career in middle sized enterprises, then at Renault in export functions before joining the AIR LIQUIDE group in 1989. There, he headed diverse regions before taking on a role in HR: internal mobility and professional development. Elected at the Chamber of Commerce and Industry in the county of Vaucluse (South of France) and national President of the network of management and commerce schools until 2010, he is today member of the board of the CDSE.

THE CHIEF SECURITY OFFICER (CSO)

Through his/her role as a scout mentioned by Alain Juillet in his foreword of this White Paper, the CSO helps companies to evolve in uncertain environments, new territories, where they can be confronted with unexpected and unprecedented events. The CSO contributes to the development of commercial activities by helping top managers in their decision making and by securing operations.

THE CSOs ASSIGNEMENTS

The CSO writes and enforces the policies he/she designs to secure their company in all places and countries where it operates. The bulk of his/her strategy aims at protecting stake holders (employees, top management, clients...) and assets (tangible and intangible), which largely represent the real economic value of an enterprise, against all forms of threats and risks.

In this role he/she operates in a timely manner to evaluate and map the risks and threats against the business, analyze the gaps revealing the faults and vulnerabilities and define the priorities in matter of security by attentively scrutinizing cases and consequences.

The CSO always acts according to three possible perspectives:

- **A preventive perspective**

The CSO is consulted beforehand on all main projects. He/she measures the level of needed protection vis a vis the level of risks.

He/she foresees the crisis management process and trains personnel in those domains and in business intelligence.

He/she ensures that Business Continuity Plans (BCP) are enforced and updated/graded. The role is also to serve as an interface with all government services, European or international organisations concerning Security. As a leading actor in duty of care, the CSO implements policies for protecting employees and sites and business travels to and in countries at risk, or during specific major events. He/she ensures protection of all assets, be they tangible, intangible or informational data.

An adviser's perspective

A thorough analysis or feedback on events allows a continuous adaptation of security processes and management. Like Quality, Security must be able to rely on a dedicated reference model. By bringing relevant answers to the risks once they have been identified and weighed, the CSO helps the CEO in making sound decisions.

Therefore a CSO can deal with any subject, even sensitive ones, with anyone, including the highest top management level.

A reactive perspective

In case a security crisis occurs, the CSO stands in first line coordination with an ad hoc crisis cell that proposes solutions to address the problem and ensures they are implemented.

Thus, in this frame, he/she is in charge of activating contacts with all organisations that can help enforce the security policies which have been disseminated. With other involved managers, the CSO sees to the continuity of activities by making sure BCP's are in place and followed.

Beyond his/her usual responsibilities, the CSOs global scope will vary according to the core business of the company, its sector, its being overseas or not, in risky or safe countries, its strategy, its vulnerabilities.

The risk watch can therefore be in the CSOs department. By adding value to the information collected in economic, sectorial and geographic fields, the CSO can be a precious tool for decision making.

Finally, lobbying can also be in the Security hands in some cases. By making its perspectives known by national, European or international organisations, the enterprise is able to act to best protect its interests.

MODUS OPERANDI

The security department is a transversal and support function in the company, just like HR, communication or finance. Naturally the CSO works in close collaboration with all other functional and operational departments. The CSO is intent on selling his/her message through communication, explanations, training and on convincing everyone.

The CSOs organisation is ideally positioned at the highest level of the company, reporting to the President or to a member of the Executive Committee (Excom).

To act, the CSO takes ground on a policy and on texts he/she has disseminated on Security, Governance (key values, good conduct, action principles, code of ethics...).

The CSO also oversees that the resources of his/her organisation are commensurate to the economic stakes and possible threats. He/she can count on internal expertise and dedicated networks in France (D2IE, SGDSN, ANSSI, MAEE, INHESJ, IHEDN, DCRI, DPSD...) to obtain advice and to benefit from their specific trainings and sensitization programs.

D2IE
Interministerial Delegation To Business Intelligence

SGDSN
French General Secretary of Defense and National Security

ANSSI
French National Agency for IT Systems Security

MAEE
French Ministry of Foreign and European Affairs

INHESJ
French National Institute of Advanced Studies On Security and Justice

IHEDN
French Institute for Advanced Studies On National Defense (military)

DCRI
French Central Directorate of Homeland Intelligence

DPSD
French Directorate for the Protection and Security of Defense (military)

THE PROFILES AND TRAJECTORIES

Whatever his/her initial and professional background, the CSO must have very good knowledge of the company's structures and keen expertise in the security and crisis management area. His/her leadership is then naturally acknowledged by everyone, as well as his/her critical view, just as his/her courage to adopt an independent position when necessary. The CSO must in fact show a capacity to deal with complex, paradoxal and sensitive issues.

The CSO will acquire his/her expertise initially, which is continuously developed afterwards at institutes like INHESJ, IHEDN, the ENSP or by participating in professional security clubs. To better disseminate the security culture the DCRI, DPSD or the Gendarmerie can contribute by awareness conferences that they deliver to employees.

The CSO also makes sure travelers or expats have access to training and updated information on the countries they are settled in, especially ones at risk. To do that, The CSO stays permanently informed on geographic zones where the enterprise is operating.

In a context of escalating economic risks, be it to face a prowlers unbelievable boldness or specialized IT tools, or to steer the entity's ground-breaking projects that raise innovative risks on new territories, top managers must be able to rely on the CSO to allow the enterprise to deliver an economic performance in a responsible, sustainable and secure way. ■

Operational recommendations

- The CSO should report directly to a Board member or be a member of the Excom him/herself.
- The expertise necessary for the function is acquired by following a recognized trail where, beyond initial training and personal trajectories, specific training provides updates on new situations, new laws and new dangers abroad.
- Government institutes and colleges can also participate in the continual improvement process by integrating new challenges in their programs.
- In the broader sense, a real management system of security, integrating training in particular, can be formulated by an ad hoc normalization group. This group would comprise CSOs of companies mostly operating abroad.
- Finally there is no doubt that the trust bestowed by other directors or stakeholders upon the CSO will be beneficial to the accomplishment of the CSOs duties. It is therefore crucial that the CSOs performance be regularly assessed and the results of the organisation measured, both internally and externally.

THE SETTING UP OF A SECURITY ORGANISATION WITHIN A CORPORATE BUSINESS

CHRISTIAN AGHROUM

Christian Aghroum

Director of Security,
Group SIPCA

Police Commissaire Divisionnaire, detached from the ministry of the Interior. He is now Director of Security at Group SIPCA, world leader in security inks, based in Lausanne (Switzerland). He has been head of OCLCTIC - Central Office for Cybercrime - for four years and spent thirty years in the National French Police, mostly in terrorism and organized crime units. He is honorary President of the association of top managers of the National Police and author of numerous works and books.

Indispensable in a modern business, the Security Department is still surrounded in mystery. After having seen why one cannot do without such an organisation, we will detail the essential stages to a good setting up of that function so that it benefits the whole business sustainability.

A CHOICE THAT HAS TO BE VALIDATED AND SUPPORTED BY THE TOP EXECUTIVE MANAGEMENT

Creating such a Division addresses an elusive need and therefore it must be supported by the top management.

Increase of crime everywhere, globalisation, developments of business abroad, corruption, travel to risk countries, expanding sophisticated technologies in communication, cybercrime and insecure information systems, are all factors and a reason for a matrix approach. The lack of convergence between physical and IT security/safety typically illustrates the scattering of responsibilities in different types of security management, preventing Top Management from having a comprehensive view and a good notion of how security is addressed within the company. The necessary and wanted reactivity to the treatment of events able to rapidly jeopardize the company's image and/or liabilities,

penal or civil, imposes a smart centralization. All the more that in many instances, providers will be brought into the processes. How to deal with providers and vendors is often a case of how to understand the jargon and mitigate the lack of experience of the novice, although it is easier than one might think. An objective risk mapping, done by the top management, allows the board or any similar body to rapidly understand the benefits of creating a Department to address the issue of Security. This mapping will ensure that beyond the identification of all the risks, are also measured the redundancies and gaps as well as the subjects that are not dealt with. This pre-document will permit to see exactly how to position the Director of Security and it will be submitted to him/her.

The choice of the scope of the structure and who will lead it is crucial. Ethical attitude, legal and technical knowledge, sense of liability, availability, managerial competencies, network capacities, this sounds like a medley tally of qualities but all these are nevertheless relevant to making the right choice. The role must report to a member of the board, it is the only way to obtain the trust and authority which are necessary for the good completion of the job. The profile of the CSO is rather well known today : an abundant literature is available and the advice of a neutral and stable organisation or club like the CDSE may help.

The structure surrounding the CSO must be commensurate to the size of the company. There is no doubt that if in a middle sized company the role may be part time, an international group would not have such thoughts of economy.

A continuous in-house training, a sustained contact with authorities will offer the Security team a real adequacy with the demands of the job. Integration of associates from other directions in the new team will ease the acceptance of the new Security Department by all involved.

TO BE SUSTAINABLE, SECURITY MANAGEMENT MUST BE FULLY INTEGRATED INTO THE CORE BUSINESS

The Security Department can easily be an ivory tower. Some common sense will help avoid this fault. The director and his/her collaborators must understand how the company functions, its complexity, its core business(es). An open program of integration, visits of sites, regular meetings with managers, unions and social groups, will facilitate a demystification of the newly created department and reassure fellow employees.

The discretion that must surround Security management does not exclude communicating about it, both internally and externally. Knowing this department exists and is actually working is not putting it at risk, but on the contrary it will contribute to its legitimacy and will extend its sphere of influence, its networks and will reassure clients and partners in the earnestness of the company.

A clear and transparent introduction to the new Security management is a way of reminding everyone of its main goal : protecting the company and all its assets, personnel first of all. This communication will be relayed by the rolling out of a documentation in which a clear division of duties is explained. The Security department can only be a benefit if, and only if, it works in coordination with other departments, which is facilitated by avoiding too much overlapping of responsibilities.

Time is the ally for this new department. A first year of activity will help determine the fundamental needs of the company and efficiently measure what means are wanted and where action is needed first. For each business there is a specific structure for the security management, according to the size of the business, its internal organisation and its sector of activity.

Three essential functions can be comprised in this department : personnel and tangible assets physical protection ; IT security ; in-house investigations. The management of risks and/ or EHS (in the sense of norms ISO and OHSAS) can also be reporting to this direction or stay aside, so long the information flow is constant between these functions. No one should expect immediate and palpable results from this new direction. It would be unwise and underestimating the human factor plus the fact that KPI's in this domain are difficult to standardize. The choice of dotted or full line reporting collaborators in divisions, departments or subsidiaries will be evaluated according to their number, size and nature of activity. Time will permit the creation down the road of an appropriate cost center, often hard to estimate before the first year of running.

A Security Department cannot do everything on its own. It has to rely on specialized contractors for a good part of its activities. The added value of the Security department definitely is in the mastering of its tasks, in the confrontation of results with the company's specificities and in the qualities of its analyses.

If Security must not slow commerce or industrial development, it is the indispensable side companion of these activities in an ever more globalized and complex world, where risks are on a wide scope, from simple rudeness to organized crime and even terrorism. In this context, specialization allows the governance of the enterprise to make decisions in full awareness while taking advantage of a relevant and legally reliable tool, able to defend its reputation. ■

Operational recommendations

- In the absence of a Security department, top management should launch an audit on its security to shed light on its situation and help make a decision in this domain.
- Then it is necessary to steer both an internal and external information campaign along with the creation of the Security Department.
- Do not forget to avoid isolating the Security department and see to its internal control.

GOVERNMENT/BUSINESS RELATIONS IN SECURITY

MARIE GEROSA - LAURENT MEREYDE

Marie Gerosa

Deputy CSO,
Group THALES

Master in public law, political science and criminology, commissaire divisionnaire, Marie Gerosa is currently detached from the national police. She was chief of several units in the Judiciary Police of Paris in 1994, then head of a section of the national anti-terrorism Department in 1998. In 2004 she was leading the service "Urban violence" at the Intelligence branch of the Police, les Renseignements Généraux. Integrated the Security division of THALES in 2009 as deputy CSO.

Businesses Security needs a tight cooperation with governmental institutions since the protection of the personnel and major and strategic assets imply, directly or not, support from the State.

This approach may vary according to sectors of activity and the degree of internationalization of the Company. However, it does not convey to the State a prime role in the creation and development of an internal Security Division within enterprises. The State can be a privileged partner through at least three main items :

- The awareness of the need to create a Security Division
- The reason of this creation
- Its daily management

THE STATE CONTRIBUTION TO THE CREATION OF A SECURITY DEPARTMENT

A serious incident, or even a severe crisis like abduction, kidnapping, bombing of sites or still the loss or theft of information are elements capable of raising the awareness of a company, leading to a better and efficient organisation concerning security, in order to avoid the reiteration of such situations and mitigate as much as possible the exposure to risk. In this perspective, State institutions can help create a Security Division in three ways :

Laurent Mereyde

Security Vice-President,
Group TECHNIP

Laurent joined TECHNIP as Security VP in 2004. Before that he served in governmental services and in the Security division of AIR FRANCE. Laurent Mereyde is a graduate of Conservatoire National des Arts et Métiers (Master Énergie, Master Économie Internationale) and holds a Master in geopolitics. He attended the Centre des Hautes Études de l'Asie Moderne and l'Institut des Hautes Études de la Sécurité Intérieure (IHESI). He co-authored a book on public politics in the Mediterranean area (Mac Millan and Reading university press). He is currently a member of the board of the CDSE and chairs the joint international security commission CINDEX/CDSE, created in 2004.

- **Initial training**
  Investing in future Security Managers

  Universities and colleges that deal with Security in their programs are still few. It would be beneficial for the State to help raise the awareness of business and management educational schools in this domain so they integrate the subject as one of their mandatory matters. This way, future managers would be made aware of the necessity of having inside their company tools allowing the implementation of business intelligence, crisis management and the setting up of structures to address malevolence to which the business is always confronted.

- **In-house training**
  Investing in the greater number

  A State/professional partnership to organize numerous conferences open to all within companies, facilitates the awareness of all the actors in the field on security matters by upgrading skills and sharing good practices.

- **Specific lectures by heads of governmental administrations**
  Investing in top management

  These conferences meant for the top executives help them raise their level of conscience on Security issues by underscoring the evolution of threats and their possible impact on the business. Upgrading/updating their awareness is often necessary.

CREATION OF A SECURITY DIVISION

The level which makes the decision on the need to set this up is crucial for the general orientation of the new unit. Indeed the "origin" of this act consecrates the importance that the company plans to give to the newly created department. The State, without substituting itself for the internal process, nor interfering in the choice of the persons who will head the Security management, can nevertheless contribute to its success in two different ways :

- **Encouraging the drafting of a code of good practices**

This is essential for the good accomplishment of security missions in terms of quality and transparency vis a vis the employees of the company. This transparency, guarantee of the credibility and sustainability of any Security management, can be fostered by the State by distinguishing where the company acts on its own and where the State can specifically intervene (theft of information by a foreign country, or protection of its employees abroad in case of evacuation).

- **Support an advice and help process**

Through a structure to be defined, the State could detach if needed experts who would support the creation of the Security department. This exceptional action by the government, prompted by and only on the request of a fledgling or restructuring Security department could provide a "general design" defining the global missions and the means and ways to accomplish them.

DAILY MANAGEMENT OF THE SECURITY TEAM

The duty of care for the protection of employees sent abroad to risky areas or simply traveling, also the security of IT systems and of other company assets are crucial for any Security department. Regarding these two matters, the State agencies can help in two directions :

- **A regular exchange of information on country-risks**

The Internet site of the Ministry of Foreign affairs "advice to travelers" does not yet bring all the added value companies and staff may expect from it if you take into consideration the specificity of the means invested. Thus, a dedicated site for corporate businesses or even middle-sized ones, would be a useful and relevant contribution to the daily functioning of corporate Security management departments in that it would help consolidate the sparse bits of information they have. Why not launch such a project in a region first ?

- **Disseminating alerts on information systems or the discovery of new fraud schemes**

Here too, State specialized services, such as those dedicated to enforcing penal law in financial topics for instance, can help protect business interests via their Security department by confidentially communicating the usual elements of the crime or at least the spotted attacks against networks.

Security is one domain in which the State and businesses do share a major common goal : the protection of men and women they employ and the safeguard of their expertise and of the companies assets, often in strategic fields. ■

SECURITY AND TECHNOLOGIES

CHRISTIAN AGHROUM

Christian Aghroum

Director of Security,
Group SIPCA

Police Commissaire Divisionnaire, detached from the ministry of the Interior. He is now Director of Security at Group SIPCA, world leader in security inks, based in Lausanne (Switzerland). He has been head of OCLCTIC - Central Office for Cybercrime - for four years and was in the National French Police for over thirty years, mostly in terrorism and organized crime units. He is honorary President of the association of top managers of the National Police and author of numerous works and books.

Confronted with an ever expanding scope of risks and liability, and mostly on account of the withdrawal of the State from its core ("missions régaliennes" in French) missions, businesses are off on a race to find ever more efficient technologies.

This race is the only way to meet the challenge posed by the increased sophistication of means used by criminals or to to bring tangible evidence before courts in trials, be they penal or civil.

Varied, diverse, complementary to one another and to traditional tools, these technologies are an indispensable trump and asset for Business Security. Continually renewed and upgraded, they want to be fully commandeered and their relevance must be challenged regularly. From this statement we can induce three proposals that can be shared with the public and private sectors.

THE FIELD OF SECURITY TECHNOLOGIES IS BROAD ENOUGH TO SUIT ALL SECURITY NEEDS OF THE BUSINESS

The state itself outsources all or parts of its security to lighten the burdens and chores of the Police or Gendarmerie and help them focus on their core missions. It is not for the state therefore to reinforce its police forces involvement in missions of protection, access control or guarding of private companies. These tasks belong to the private sector. Security technologies evolve consequently and their market is ever expanding in this path. Biometric devices for example have entered this field in the arena of access control for many years. Cctv has also penetrated the public sector when it is already a valued tool tool in the private sector for enhancing peripheral protection ; automatic reading of car plates helps control vehicles in public or private parking lots...

The array of techniques fits the diversity of security needs: peripheral watch, access controls of personnel and vehicles, geo-localization of goods and means of transport, watermarking and detection against counterfeiting, surveillance and protection of communication networks (telephone, Internet...). These advanced technologies however do not replace traditional ones: fences, doors, safes and other coated devices, instruments to enhance physical surveillance (communication, protection equipment...). Of course the means to protect Health and Safety are not forgotten here (a prevention against hazard fires is also a protection against sabotage).

The extension of protective technologies to the world of business Security guarantees the expansion of a market which is boosted by a significant increase of threats. According to the "Atlas 2009-2010" of "*En toute Sécurité* (a security magazine), 22 slots segment this market in France, for a global sales figure of about 19 millions euros in 2008, versus 11 million in 1999 (an increase of 172 % in less than ten years...). The organisation by the private sector of security devices shows which until now were restricted to the public sector is a clear sign of the times.

MASTERING SECURITY TECHNOLOGIES IS ABSOLUTELY NECESSARY BECAUSE IT GUARANTEES AN ETHICAL PROCESS

A non-commandeered or mastered access to protection/security technologies can rapidly open a Pandora's box, the box of amateurism, illegal actions, barbouzerie (para military illegitimate processes). The due protection of privacy and public and individual liberties must remain the absolute rule. It is not a surprise the law maker sees to all or most parts of surveillance and security activities (privacy laws, CNIL, orientation and program law on security) through Parliament Commissions or laws. Security technologies, always evolving, are complementary, interactive and allow crosschecking of behavioral data. An aggressive or too autonomous use of those is a sure way to a court. No doubt all CSOs will find in the penal or labor codes or any other, all the answers they may need to their ethical issues.

The managerial impact of these technologies imposes a proper training and information of users and co-workers alike. The collaboration of the Security management with all departments of the company must be favored at all costs : how indeed to install an access control system based on biometrics if you do not communicate beforehand with associates in order to raise all the legitimate doubts that may appear ? Aided by the legal department, but also by an efficient and competent network outside (like the CDSE), the CSO will eschew all the traps of the security-

obsessed mindset, the paranoiac excessivenesses, or even spying on associates in the business, when not spying illegally one member of the board for the sake of another jealous member...

Anticipation and technological monitoring of new devices and tools are also essential in order to avoid choosing rapidly obsolescent techniques. These qualities of mind prevent succumbing to useless trends, fashions, and wasting money in security ill-controlled and maybe even illegal devices... The cheapest technologies purchased in countries that are careless of social equity or counterfeiting are a guarantee neither for quality nor for the reputation of the buyer. Security has a price. One should accept it. A rational analysis however ensures the correlation between financial capacities, image and the real need for protection. Contracting can be preferred for a rational concern, but trust must be faultless with the partner.

Security technologies and devices have a bright future ahead in an ever more unstable and unpredictable world. These technologies have sense only if they come as a service for the business in particular and society in general in a clearly defined social contract. Internal and external audits, regular reports, transparency towards authorities (government agencies, privacy authorities...) are some of the warranties that good governance must ensure for the business' own security. ■

Operational recommendations

- Associate the private sector with the drafting of laws and regulations related to security technologies. The CDSE, ideal representative of these interests, could be a perfect and regular partner for the public sector in that sense.
- Develop the domains of research and R&D in that field, always in a joint effort of bringing private and public interests closer through various administrations, security firms, universities and clients.
- Launch a study to assess the real cost of security in order to better appreciate the weight of new technologies in the sales figures of security companies and more generally into the State GDP.


MISSEL
contient
l'année, et
MISSION
Fig.

2 THE **ASSIGNEMENTS** OF A SECURITY ORGANISATION

SECURITY ON AN INTERNATIONAL LEVEL

Jérôme Ferrier

CSO TOTAL Group

Jérôme Ferrier is an engineer who has spent his entire career working for ELF and then TOTAL. Prior to his appointment as CSO in 2008, he held a number of senior positions at corporate HQ and foreign subsidiary level including, Director of the Americas and President of Total Gas & Power in Argentina. He is also Vice-President of the International Gas Union.

Events in 2011 have had a considerable impact on the activities of French corporations with international operations, and in particular on the security of those operations. They revealed that security is an issue that must be coordinated on an international level.

These crises were exceptional due to the number of countries affected, the variety of underlying causes, and the resulting political and media exposure.

The threats faced by corporations and their employees vary enormously and require specific analysis. These threats include terrorism (probably the most serious in terms of consequences), socio-political problems and, more generally, crime including kidnap and ransom, maritime piracy and cybercrime. Ten years ago, there was little or no piracy and cybercrime, but today these threats have become more complex and sometimes more violent. It is necessary to develop methods to counter these threats that are in keeping with our corporate ethics, codes of conduct and local legislation.

Three key criteria form the benchmark for effective security operations :

The ability to anticipate

Anticipation relies on the assessments provided by the French Foreign Office and specialist consultants. Recently their authority was dented by a collective failure to anticipate the events of the Arab Spring such as the social uprisings in Tunisia and Egypt and the fighting in Libya. However, they did anticipate the consequences of the elections in certain sub-Saharan countries (Ivory Coast) and Asia (Thailand). Their in-depth analyses and careful interpretation of the smallest signs proved to be correct. Companies must be aware of the importance of this kind of intelligence.

The ability to respond

Response mechanisms will largely depend on the way activities have been structured. In countries where insecurity is endemic and international exposure high, due to the interests at stake, a security operation should be set up at subsidiary level. Comprised of permanent staff or contractors, these operations should report to the Subsidiary Manager, or Group Representative if there is more than one subsidiary in that country. The cardinal rule is to establish a single decision-making centre because action taken at international level could have serious political consequences. But, a flexible approach is required at times particularly when crises take an unexpected turn and don't follow anticipated scenarios. Introducing such mechanisms will help to create the best possible environment for managing crises, particularly if a crisis management team has been identified and given prior training. (X. Graff covers crisis management later in this chapter).

Feedback and post-incident analysis

Feedback and post-incident analysis are essential, regardless of how efficiently a crisis is managed or the expertise of the staff concerned. It is vital to learn lessons from the decisions taken and the actions that resulted. To operate effectively internationally, companies must continually assess the relevance of their internal procedures and establish a security management system capable of handling the unexpected (The return on experience from the incidents that affected the AREVA Group is covered later in this chapter by JM Chéreau).

Once these elements have been taken into consideration, companies active on international markets must set up a corporate security department, reporting directly to the senior management committee, which is responsible for :

- Intelligence and threat assessment to process information in accordance with business priorities. This analysis work, to understand and anticipate events, should be carried out with the support of the relevant Government Departments and in particular the Ministry of Defense, Interior Ministry and Foreign Office.
- Structuring operations into the appropriate number of geographic regions to protect subsidiary infrastructures and employees in the event of a crisis. Personnel protection is a top priority and major obligation. Host States are responsible for protecting personnel and facilities in association with subsidiary security officers. Care must be taken to ensure that military and civil personnel follow best practices in accordance with the company's corporate ethics and codes of conduct.
- Protecting information assets to guarantee the integrity of corporate assets against all forms of cybercrime to maintain the company's competitiveness and protect its long-term interests. This is achieved through collaboration with intelligence networks and Information Systems Departments and a targeted personnel training and awareness policy. ■

Operational recommendations

- Make full use of Government expertise, particularly for intelligence and advice. Government departments are in a position to respond to requests for assistance from corporations.
- Adopt a global approach to personnel management even if separate measures may be applied to local and expatriate personnel particularly in the event of an evacuation.
- Ensure that everyone adheres to corporate ethics and codes of conduct - not just permanent employees and contractors, but also the private or public security forces responsible for the protection of personnel and assets in the countries in which our companies operate.

THE BUSINESS CONFRONTED WITH THE KIDNAPPING OF AN EMPLOYEE

JEAN-MICHEL CHÉREAU

Jean-Michel Chéreau

Protection Director
Group AREVA

Graduated from ENSTA and the École de Guerre (War academy), he participated in the setting up of the Special Operations Command (COS). After various posts, Jean-Michel Chéreau was nominated COS Chief of operations in 1998. He led different brigades, was Deputy Director of Military Intelligence (DRM) before being promoted Général de Corps d'Armée in 2008 when he joined the Army Inspection General. Protection Director of Group AREVA since 2010.

On the night of September 15th 2010 ; an AREVA employee, his wife and five personnel from group VINVI were kidnapped by members of AQMI on the mining site of Arlit in Niger. Both companies were in shock. A quick response was demanded.

Urgent measures were immediately taken : with the help of French authorities, all the expats were first requested to leave all mining sites located in the North of the country.

Most of them were quickly repatriated to France.

Back in France and because AREVA is a national critical infrastructure, most employees were debriefed by an ad hoc team, set up by the Management of the Protection of the group, in order to learn "smoking gun" lessons from what had happened and take first correcting measures right away.

The Group AREVA, should the situation arise again, then took precautionary action to support in times to come :

- hostages' families ;
- employees shocked by these abduction.

There is no miraculous recipe in that domain, but the following actions demonstrated their relevant effectiveness :

- timely internal communication via the enterprise network, with for instance a particular effort on birthday dates, to ensure families have the company's full concern and support and also on another hand, reassure employees : they wanted to know they were still associated in the endeavors to secure the whole company (I will not elaborate here on all the details regarding measures AREVA put in place afterwards) ;
- provide open space on the intranet so the associates who so wish it can express their support to the families ;

- frequent meetings with family members (in addition to information meetings organized by the Ministry of Foreign Affairs) at the group's headquarters, to remind them we are constantly working on a solution and to give them all the answers to their questioning of the situation whenever it is possible.

Simultaneously, it was crucial to take all necessary measures for sending expats back to the mining sites. This in order not to give kidnappers the feeling that the group AREVA had given in, and also to ensure local workers (who, in the absence of expats, contributed to do a great job) that we would not abandon them.

This stage of the process was complex and painful to some of our staff because it was necessarily started by a feedback on the events themselves. This work is indispensable when you consider the severity of the crisis. The quicker it is done, the better.

Hence, we had to :

- put in place all mitigating measures we had identified through consolidated policies and plans drafted with France and Niger authorities ;
- steer communication meetings with employees for explaining them over and over again, as to what had happened and tell them what corrective measures had been decided and how their security would be ensured when they would go back to work, in order to rebuild their trust.

Today, even when four of our employees are still being held as hostages somewhere in the Sahel, a first batch of expats is back on site. They are equipped with security guidelines they have to abide by, documents that will regularly be assessed and upgraded if necessary by internal and external audits every other four months.

Beyond all the procedures, documents, measures that the Direction of the protection of the group disseminated, it is crucial that top management and the most senior employees be made aware of these issues and never forget that as of now, personnel security caps everything and has to be integrated in the very strategy of the company in high risk countries like Niger.

It means a deep change in working as well as living practices which have to be more constraining than before. It is only at this cost that security can be enforced. ■

Operational recommendations

- Undertake, as soon as possible, a full debrief in order to be able to decide corrective procedures without delay.
- Support hostages' families in their endeavors by maintaining regular relations linked with the ministry of Foreign affairs : in such a situation the group must behave as if it was an enlarged family.
- Be close to employees ; show them the commitment of the company in working hard for the liberation of their co-workers.
- Exchange/talk to everyone involved on procedures implemented in order to enhance their physical security.
- If the company takes an active role in the negotiations with kidnappers, it has to be done in very close collaboration with government's services which are the only ones able to avoid the multiplicity of negotiation channels that would be counter-productive, even dangerous.
- In a kidnapping crisis, always favour discretion in your communication so as to not to jeopardize negotiations.

RISK AND CRISIS MANAGEMENT

XAVIER GRAFF

Xavier Graff

Risk Management Director
Group ACCOR

Risk Management Director at group ACCOR. Xavier is also in charge of developing, rolling out and maintaining alive all the risk and crisis management schemes and teams. Prior to this role, he was Security and EHS Director with group CLUB MÉDITERRANÉE where he launched and steered procedures for crisis management after having done a great part of his career in technical management abroad. Xavier Graff is a graduate of the Institut National des Hautes Études de la Sécurité et de la Justice (INHESJ).

Crises in Middle-East countries and the Ivory Coast, tsunami in Japan, earthquake in New-Zealand, world financial crisis, tornado sweeping the East coast in the US, abductions of employees,all these recent events have demonstrated that businesses have to face heterogeneous risks, all being susceptible to impact the security of their clients, their collaborators or still the annual results or their reputation.

RISK MANAGEMENT

The exposure to risks related to security/safety is ever increasing, and demands the setting up of an organisation able to identify and map all the risks of the company according to its activity.

This has to rely first on a culture of risk sensitization which must be inspired by the top executive management and shared by all managers.

Risk mapping is something that will be beneficial to all :

- For actors on the field, it allows them to better identify risks related to the completion of their fixed objectives and improve the steering of their activities
- For the General Management, mapping is a valuable instrument that contributes to strategic planning and the aid to decision making. In fact, it is an internal guidance mechanism.

Once its risks are clearly identified, mapped and sorted, the business still has to implement action plans to mitigate them, reduce their impact, transfer them (insurance), even eliminate them if possible. This will streamline the functioning of the firm in order to obtain planned results thanks to a good anticipation of potential crises.

These stages require a horizontal and heavy workload, involving all the operational units, among which of course, the Security Department in each site and in the HQ. This workload will be eased if people share a common risk culture.

The risk mapping process must take place every year in order to ensure a timely follow up of major risks to which the company may be exposed.

Sharing the results of the mapping with internal audit, guarantees a real follow up of the risks by their owners

The legal environment of companies publicly calling on savings having changed lately in Europe, the due risk management brings specific answers to the following constraints :

- Order of 12/8/2008 (8th directive) : monitoring of the efficiency of crisis management schemes within the company by the audit/risks committee.
- Law of 7/3/2008 (4th and 7th directive) : the report of the CEO must mention risks management procedures implemented by the company.

For a certain number of major and identified risks (sites becoming inaccessible, evacuation of expats, etc) it will be necessary to draft continuity plans (CP) to which the CSO will of course contribute.

CRISIS MANAGEMENT

In a 2010 poll done by the CDSE among its constituents, 78 % of those who answered already had a department or a service dedicated to crisis management and in 48 % of cases, this service had been active for more than 5 years.

In 15 % of the cases, the CSOs owned the crisis management organisation. However, if you consider that 23 companies participate in the CDSE's commission on crisis management and that new demands to adhere to the group are numerous, it is a clear indication of an increased interest from Security organisations in this topic. 63 % of companies said in the same poll they had great expectations regarding the disseminating of good practices and 21 % wished to work on an improvement of the coordination and access with public authorities.

This process, which must obtain the support of the top executive management, is built in several steps:

- creation of basic tools (procedure and guide for crisis management, quick reflex sheets, pocket-memos) ;
- communication and coordination software tools ;
- putting up a 7/7 24/24 watch and telephone answer ;
- identification and training of crisis cell members ;
- drafting the list and map of all concerned actors (internal resources, partners, institutions, media, environment, etc) ;
- real life training.

Within the crisis cell some actors will be indispensible : HR, communication, legal, even insurance, according to each crisis profile.

All along these stages it is highly desirable the company be accompanied by a contractor who will also be able to bring his/her expertise during a real crisis and for the experience feedback.

Due to their complexity, new crises cannot be dealt with by the business alone only. An interaction with other companies (clients, supply chain providers, contractors...) and public authorities is therefore mandatory. This means one has to work, in anticipation and "peace time", links that will be activated in war time... These links are made alive through common exercises on shared procedures.

This public/private sector collaboration is something the CDSE has engaged in since 2008 by actively participating to the drafting of a white document : "command of crises and risks : cross thoughts" under the leadership of INHESJ. One document of this working group, known as "groupe de travail partenarial public-privé, or GT3P", proves the importance of the topic and will continue to be one of the directions the CDSE is exploring. The convention signed in 2009 between the CDSE and the CDS (Crisis Center of the Foreign Affairs ministry) must be more exploited by the partners with other ministries that have a bias on French businesses like Interior, Defense, Environment, Finance, Industry, Health, Transport, etc...).

In order to allow CSOs to exchange freely and confidentially with diverse services of the French administration for accessing more information, it would be ideal to develop an security classification labeled "Business Confidential". This would offer the opportunity to have a head start when a crisis erupts, better deal with it and better protect the business as well as its clients and co-workers. ■

Operational recommendations

- **Help the CSO function evolve upwards by involving it more in crisis and risk management.**
- **Develop new public/private partnerships between the CDSE and the ministries which deal with its members' activities.**
- **Creation by the government of a security classification " Business Confidential " for CSOs.**

COMBATTING FRAUD

NADIA CHELGHOUM

Nadia Chelghoum

Combatting Fraud
Security Director
AXA FRANCE

Nadia Chelghoum attended the National Academy for Commissaires de police in 1989. She was posted in Saint-Étienne, Vaux-en-Velin and Lyon, mostly in community policing roles. In 2001 she joined the Cabinet of the Mayor of Paris, in charge of security issues for the Capital. In 2003 she was recruited as CSO at AXA Insurance.

Our company encounters no risk at all. We are a small family business, we all know one another. With my internal control team anyway, it is impossible for us to be the victim of fraud".

What security manager, as modest his/her role may be, has never heard this from the boss precisely when trying to obtain a budget to combat fraud ? Traditional risks related to fraud though (the most classic being embezzlement), are a reality that many of us have already had to acknowledge. And the economic crisis has definitely increased the impact of this type of criminal behavior in all domains. It is therefore a priority today for any business to invest this field in order to preserve its image and assets.

ADMITTING THE REALITY OF FRAUD

It is quite common for businesses to sway between denial, unawareness, or deliberate choice not to invest funds in a topic that brings no return on investment. Indeed, what good is it to put money in a long term policy to combat fraud when the potential financial losses will always be less than the cost it would demand to set up a counter fraud team ? In fact, to quantify the real impact of losses and of savings done by not investing in an anti fraud policy is always difficult : the right tools to find out are lacking.

Fraud is often a taboo. So that a great number of companies stall at the transparency it entails, because of the consequences in the media (notably if a fraud is committed in financial bodies like banks, etc) and because they do not wish their organisational weaknesses, mostly HR they think,to be publicly exposed.

The origin of fraud may be from outside the company (clients, economic or commercial partners). It can also come from within (criminal behaviors of associates or representatives). We will take a closer look here on internal fraud and make recommendations about this issue specifically because the consequences are far worse for the image of the business.

Acknowledging bluntly the very existence of this type of incidents and accepting responsibility for dealing with them in an open way when they occur is a non negotiable pre-requisite for the implementation of a service dedicated to fraud within a visible and recognized direction. Transparency is also an obligation for drafting and rolling out a policy on this matter, policy that will remain simple and easily understood by everyone. It will integrate the identification of each type of fraud, their mitigation/treatment, how to steer investigations on perpetrators, the ways for triggering internal discipline procedures and reporting to public law enforcement agencies wherever needed.

AN ESSENTIALY DISSUASIVE PROCESS

To us, the "fear of the cop" remains the best deterrent to prevent fraud in businesses. The investigation, the search and the finding of evidence that a fraud has really taken place, the identification of person responsible, all this must be realized in a strictly legal and objective way. Thus, the gathering of public financial and freely accessible information, the analysis of transactions, of financial flows in the general frame of a fraud can be valuable sources of information, in compliance with labor laws and those of the company which is the data owner.

A general monitoring, as much on the networks as on the Internet or still by checking information on different data bases, open and accessible to all, is the first step of a general surveillance. Then the regular use of performing IT devices by internal control and the detection of frauds by analysis of targeted items allows anticipating the risk upstream.

The rolling out of fast investigations, both to prove or disprove the innocence of the suspected persons or prove the existence of criminal facts, will help gather the evidence and identify the authors so as to attain the overture of a disciplinary procedure or eventually of a judiciary one. To do just that, co-associates of the unit will be trained in investigative techniques: how to steer them in the strict respect of codes of conduct and/or of ethics, or public codes (like labor and penal codes). However the service in charge of the investigation is not the last one to have a say: HR and legal are stakeholders in these procedures in the very interest of the company and its employees.

Among rolled out tools, the publication of a code of conduct (or ethics) is a good means to protect the business against the risk of fraud but also against any behavior contrary to the law. This code, or chart, must be accompanied by a system of professional alert or reporting mechanism, also called whistle blowing, adapted to the local law. It will allow anyone to report any incident which looks fraudulent. Once again the more upstream you are, the less you will lose and the smaller the impact on personnel and assets is.

Such a chart must go along with an awareness program for all the managers. An appropriate communication about the policy is necessary to build a risk culture shared by all, a culture that will be realistic to be beneficial. For example, the fact of telling employees what sanctions they incur, or to inform them of the systematic implementation of a disciplinary procedure that can lead to a firing of the concerned personnel or still a reporting to the judiciary authorities is undoubtedly dissuasive and preventive.

Lodging a complaint is not only dissuasive, it also has, if made public, a value of setting an example. It is also necessary to protect in the long term the economic market that would suffer from unpunished crimes. This proceeding finally gives companies the opportunity to benefit from the expertise of professional investigators and from the power, might and legal rights of a judicial inquiry. On the other hand the recourse to private investigators is always a possibility too of course, but it needs to be strictly monitored in order not to breach ethical rules and laws.

Combatting fraud is everyone's business. It requires the support of all the teams that belong to the company, i.e. HR, legal, communication, finance, risk management, etc. It also requires a true collaboration with governments' agencies, in the best interest of public and private executives.

Finally the building up of a corporate library of ethical documentation enforced by the right amount of personnel commensurate to the size of the company is not costly for the business. It is a useful defense in the long term against all risks of fraud. ■

INFORMATION PROTECTION

CYRIL NGUYEN - JEAN-PIERRE VUILLERME

Cyril Nguyen

Security/Safety Director,
Loss Prevention
Group CREDIT AGRICOLE

42 years old, is a member of the board of CDSE. Attended the 21st session of INHESJ. Master's Degree in information technologies and security from the university of Marne-la-Vallée. Prior to being Security/Safety Director, loss prevention at group CREDIT AGRICOLE, he was Security head for NESTLÉ FRANCE and before that Loss prevention head for TECH DATA FRANCE. He spent 14 years in a special service at the ministry of Defense.

If the protection of strategic information is still a topic unknown to many people, the real operational efficiency of means of protection in this domain mostly relies on the understanding of security stakes by all the actors of the business, whatever their level is. The human factor indeed appears to always be the most determining one when you analyse the causes for a loss of information (often not-intentional): the human factor must therefore retain all the attention as soon as information protection is at stake.

INTERVENTIONIST OR NAIVE APPROACH ?

Having made this statement, the temptation would consequently be to establish and impose a body of constraining internal rules (information security classification, protection, length of archive retention, shredding...) the breaching of which being heavily sanctioned. This "interventionist" approach will not however be efficient in time if the personnel do not buy into this way of thinking, which passes by a good understanding of the stakes. We will also note here that this domain is not covered, or very little, by laws and regulations (and moreover that the jurisprudence is generally not in favor of the business in this field). Clear legislative texts regarding the protection of confidential business information are awaited here (project of the law maker Bernard Carayon)

Another approach, certainly less directive and possibly more naive, is to trust each employee to behave correctly in this area by making their own decisions on the need for information security.
This would require that each and every one has the capacity to identify the security importance of all the documents one is using and to protect them consequently, even if most of those documents today are "virtual". But the result is uncertain, all the more that the employees sense of loyalty to the business is less and less certain !

Jean-Pierre Vuillerme

Risk Management Director, ADIT

Doctor in engineering. Started his career as researcher-professor during 4 years. Joined group MICHELIN in 1972, where he assumed several roles (industrialization Manager, Communication and Public Affairs Director and finally Environment, Safety and Risk Prevention Head before retiring in 2009). Joined ADIT in January 2010 to launch the French Business Center in Baghdad from scratch and took the position of Risk Manager Director.

An effective answer to that challenge is probably seeking out a right balance between these two separate policies. But even then, the involvement of the top executive management remains to be clearly demonstrated by showing its support and its belief in a true security culture and by setting the example itself. We are still a long way from it. The losses of information (leading very often to losses of markets or damage to the reputation, on the products or on the executives' image) like other sensitive issues like fraud are still taboos and this does not help Security organisations.

AN APPROPRIATE ANSWER TO SECURITY ISSUES

Because they feel comfortable behind their codes of conduct or ethical rules, some managers also believe that what they think to be criminal behaviors they forbid to themselves will not be used against them by their competitors.

What's more, top managers have not always realized that the organisation of the industrial networks (most of the competitors being in the same channel are in fact intertwined and connected by the same tight fabric of contractors, providers, for raw materials in particular) and the mobility of information systems (laptops, smartphones...etc, which entitle them to stay connected to the business permanently) leap over both borders of the enterprise and those between private and professional life. Private laptops are often used for professional use and reverse, the former able to contain sensitive information belonging to the business... without much appropriate protection.

As for social networks, they are sources of many breaches : it is not uncommon to hear conversations about confidential subjects in buses and trains, or even in the bar facing the headquarters. Social networks on the internet are equally extremely dangerous in that they give the illusion to belong to a private sphere when in fact they are public.

As it is easy to see, the causes for loss of information can take many forms and the channels are numerous.

This being said, a very clear message, avoiding technical jargons and focusing on the consequences of a loss of strategic information, has to be sent to all employees, associates, co-workers :

it is the jobs of the enterprise itself, and in some cases its very sustainability, which are threatened by those losses. This message must be carried out by the top executives whose behavior, once more, must be exemplary in this domain.

Thus and only thus, can the CSOs role be legitimate : he is not only the one who lays down rules, often constraining, regarding protection processes, he is also the main actor of sensitization actions that will take place and will induce the development of necessary motivation to enforce the rules among all the personnel.

In this domain, resorting to governmental organisations like the DCRI or the Gendarmerie, according to their zone of competency, is extremely efficient for two reasons. First a message is all more heard when it originates from an external expert who, moreover, represents the State. Secondly, these awareness campaigns do not limit themselves to giving useful advice for professional life. They also broach on the risks of wrong behavior and their consequences in private life. Operations of "social engineering", embezzlements, sexual assaults... have been facilitated by open talks on social Internet networks (address, hobbies, visited sites...). The sensitization becomes then very efficient by the echoes it finds in the private lives of everyone. These trainings are as of now much appreciated by businesses which have to be patient to benefit from them so much they are sought after. The recent project of the D2IE and INHESJ (project Euclès) to give a "label" to some lecturers on this subject will provide an alternative solution. Without chauvinism, let us note here that apparently these types of trainings from State authorities for the benefit of the private sector do not exist elsewhere!

Internal training sessions have to be regularly organized as a second step, centered on specific risks and taking ground on real life examples if possible. Trainings should be interactive and will aim at showing the pertinence of means of protection installed in the company (like providing dedicated information to travelers, data shredding devices or deletion of copier disks before their maintenance or disposal). Role games (defending or attacking in turns) are also good pedagogical ways to show how easy it is to capture strategic information too often involuntarily forwarded to public addresses, either by simple techniques of social engineering or by false call for recruitment or tenders.

Finally, a documentary report recalling the main principles (very often based on common sense), along with on line e-trainings allows to complement the sensitization procedure. Naturally, let's not forget some controls (clean desk policy for example), which are necessary to maintain the collective awareness of all these issues. ■

THE PROTECTION OF CRITICAL INFRASTRUCTURES

JEAN-MARC SABATHÉ

Jean-Marc Sabathé

Safety Director
Group EDF

Received his initial training at the commissariat de la Marine nationale (Navy), worked in several ministerial cabinets and occupied various roles in local communities where he was elected as representative. General Secretary of a political party in the 90's, Jean-Marc Sabathé set up the role of Spokesperson at the Ministry of Defense before being promoted Sous-préfet in 1999. He was posted at home and overseas, and then became administrateur civil at the Ministry of the Interior where he headed the bureau for officers at the Directorate of Police Administration (DAPN) between 2004 and 2007. He is now detached as Safety Director at EDF.

The protection of critical infrastructures is at the very heart of governmental and major public and private utility concerns. The content of that protection covers a large scope, from preventing malevolence and terrorism to a multi-risks approach for enhancing the resilience capacities of the nation in case of a major crisis.

In a context where threats of all sorts increase every day, primarily terrorist ones the early 2000, France created in 2006 a procedure regarding the "sectors of activity of vital importance" (SAIV), incorporated in the Code of Defense. The State committed itself to a setting up structures in this domain, associating in its working proceedings all the utilities on which new obligations would be placed.

Thus, "operators of utilities have to cooperate at their own cost to the protection of said sites"as said in the Code of Defense (L 1332-1 of the code).

Activities of vital importance are divided up among 12 sectors (transport, energy, health, etc). Each coordinating Ministry sets the targeted objectives of protection and probable scenarii in a national directive of security (DNS). Each company, designated as Operator of Vital Importance (OIV) is mandated to draft and finalize an "operator's security plan" (PSO in French), unique document that is the operator's answer to the State's request.

Each OIV proposes within its PSO a list of Sites of Vital Importance (PIV) which are in fact the sites, buildings, sub-locations that need to be particularly protected.

Finally each PVI is provided by corporate Security with appropriate security procedures (PPP, plan de protection particulier) approved by the local préfet who, in his own turn, has to prepare a plan for the county called PPE (Plan Externe de Protection).

A STRONG INVOLVEMENT FROM THE SECURITY DIRECTOR

All the workload will rest on the CSOs shoulders: site coordination, drafting of PSO's and PPP's. It demands a great capacity to assimilate the government's requirements, regular meetings with all the concerned co-directions, a mobilization of engineering capacities, a thorough reassessment of the risk analyses, an overhaul of organisational schemes, notably for crisis network, thinking about size and relevance of security procedures and devices, checking the implementation of Vigipirate plan (an anti terrorism scheme, put in place in the 1990's to better control public spaces against bombings) and lastly studying the interdependencies with other operators to bring coordinated answers targeting resilience in time.

Constraints are relatively heavy. Threats and scenarii are always susceptible to being reviewed for an increase of planned measures, pushing foward the upgrading of all the devices.

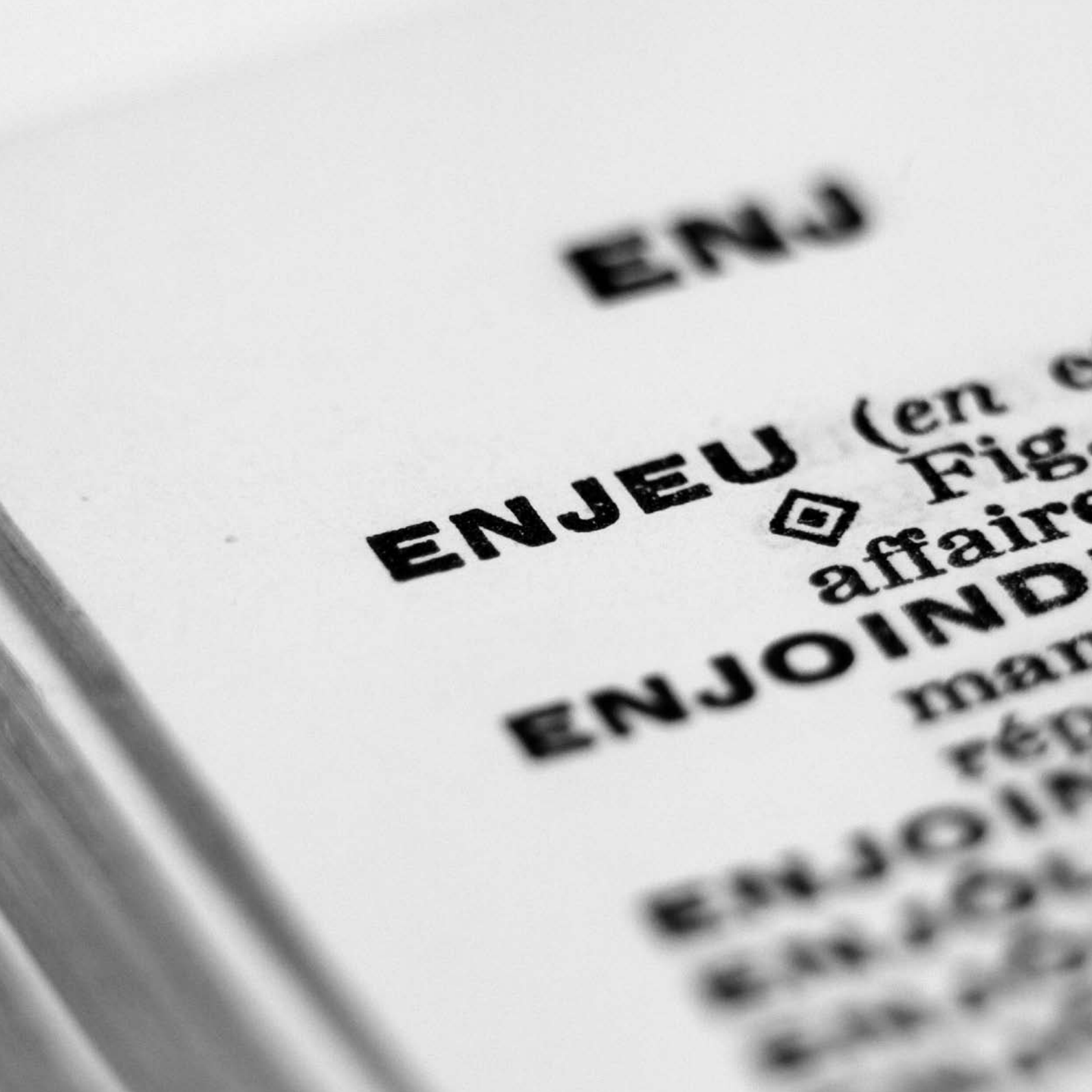
AN APPROACH WHICH IS EVER MORE INTERNATIONAL AND MULTI-RISK

Two trends are currently at work. If states are the appropriate level to assess threats by themselves and adopt the nationwide measures they deem appropriate, international authorities and most of all the European Union tend to take hold of the issue too. The EU directive of December 2008, for example which deals with the Security of Critical Infrastructures, stipulates measures that have to be implemented on cross border sites. The EU undoubtedly desires to go even further (European regulation, common referentials, crisis management...),

Finally, with the frequent occurrence of climatic disasters, and the nuclear incident in Japan in 2011 in particular, states wish to see their plans evolve from anti-terrorism targets to multi-risk ones, with the will to ensure the resilience of administrations and main economic activities. Planning has still interesting days ahead ! ■

Operational recommendations

- The government must improve its inter-ministerial approach to better understand inter-dependencies between economic sectors and commit itself to continue its efforts in this sense to give enterprises more visibility.
- The CSO must have a corporate positioning of his action to obtain support from his General Management and collect all the energies to overcome the hurdles.
- The CSO must also undertake financial analyses and weigh the impacts of the process to ensure its success and its acceptance by all.


ENJ
ENJEU
ENJOIND

3 NEW **STAKES** FOR SECURITY

PROTECTION OF SENSITIVE INFORMATION

GUILLAUME CAPOIS - PHILIPPE DULUC

Guillaume Capois

Director of Security
Group EADS

Graduate of the École Spéciale Militaire, Saint-Cyr, he spent his career in special operations, parachute units, special forces and military intelligence. After being posted to an embassy, he came back to France to head the DSIRP (Direction of industrial security in Paris area). He then became a member of the Groupe Permanent d'Intelligence Économique (GPIE) of the "Haut Responsable à l'Intelligence Économique" Alain Juillet. In 2007 he joined EADS as Chief Security Officer.

The environment in which companies thrive has considerably changed these past years. Information management, timely sharing of it within extended and global companies in a context of imperative reactivity has imposed the intensive use of IT systems. At the same time, the increased capacities of systems, tools and devices have transformed working methods, down to the most current daily actions, all this leading to a blurring, even a permeability of the frontiers between private and professional lives.

In this environment of very high competitiveness where codes of conduct and laws are sometimes forgotten, threats on the integrity of information are all the more serious and numerous that technologies and methodologies that support and facilitate information theft are permanently evolving, some of them being easily accessible on the Internet.

TYPOLOGY OF THREATS

Most hackers or attackers can be divided into three groups that sometimes interact :

- Organisations supported by state structures or agencies.
- Competitors acting directly or through "specialized" firms that can in some cases can be in relation with organized crime.
- Pure hackers in quest of fame, motivated by an ideology or acting through simple serendipity.

Attacks have evolved in danger, complexity and size, and, without trying to be exhaustive, generally have for consequences :

- Theft of personal data (number of bank cards...) motivated by greed (deceiving, fraud, spam, blackmail...) ;
- targeted attacks on the availability or integrity of systems (defacement or denial of service...) with an ideological motivation ("Anonymous" phenomenom) ;
- sophisticated attacks aiming at stealing sensitive information (Advanced Persistent Threats) motivated by industrial or strategic espionage ;
- cyber attacks attempting to damage equipment or disrupt, even close down production lines or services (attacks on Iranian nuclear centrifuges in 2009 by the use of the Stuxnet worm).

These latter months, news has demonstrated the large scope and frequency of these types of attacks, even if reality is certainly even more dreadful, many victims avoiding to make public their own case, or still worse, unaware they are being attacked.

WHAT SOLUTIONS ?

To mitigate threats, some directions can be followed by Security organisations. What is at stake is replacing information security at the heart of all the actors' concerns, preoccupations or projects, at all levels of the enterprise, and to give the Security department the means that are needed to implement its policies.

First of all, a global and comprehensive approach of IT must be favored. It means a clear governance, warranting a freedom of appreciation and judgment on proposals and prefered solutions in order to help maintain consistency in the protection of business information. IT Security should report to the Security Department in order to attain this goal. The Security Department is not in charge of IT architecture or specific security operations which still must be conducted by the Chief Information Officer. But the CSO is tasked with stipulating specifications and constraints to be enforced, with the validation of chosen solutions and finally the steering

Philippe Duluc

Director of the Security/Safety Commercial Pole, Group BULL

Graduate of the École Polytechnique, engineer in armament, he held roles in operational cryptology, then became head of this department in the Ministry of Defense until 1999 when he was designated to be special adviser to the General Secretary of National Defense, in charge of scientific and technical affairs. In 2003 he set up the Security Department at FRANCE TELECOM ORANGE that he headed until 2011. Today Director of the Security and Safety commercial activities at BULL, he is the CSO of the group at the same time. He chairs the permanent group Cybersecurity at Alliance pour la Confiance Numérique (ACN - Alliance for Digital Trust)

of compliance audits. The CSOs organisation ensures a better consistency of all security issues (physical, human and digital ones) and allows avoiding conflicts of interest. In order to be efficient, Security budgets must not depend on the possibilities of the Directorate of Information : recent attacks have amply shown what the results of successful attacks could be.

Secondly, in front of these multiform and permanent threats, a security organisation based on peripheral protection only is obsolete. It must be replaced by an in-depth security, seconded by a capacity of detection and treatment of any sophisticated attack. No one can rely on a "Chinese wall" any more. One has to segregate, crypt, strongly authentify, safeguard evidence... by an ability to detect and analyze a penetration of the systems to better manage and ensure it does not happen again. The creation of a Security Operation Center and of a Computer Emergency Reaction Team (CERT) are imperative to improve the reactivity and the expertise in these domains, capitalize on lessons learnt, maintain a network of experts, inside and outside the company, confront ideas and solutions, exchange on those and finally collaborate with dedicated state agencies like ANSSI (National agency for IT security) in France.

Finally, the human factor-individuals and users, has to be replaced at the core of the process because man is the main actor in the security of information. The rolling out of a targeted sensitization plan, often updated and personalized, allows prompting a motivation and a sufficient awareness to avoid most traps and most frequent careless behaviors (phishing, identity theft, social networks), provoking reports of first impressions on a job and a reactivity to the feedback of incidents. A clear policy for the commitment of all must also be implemented (public charts, objectives, assessment). Any new project or modification of IT systems (tools, devices, architecture, software, contracting, off shoring) must be accompanied by the appropriate procedure including the advice of the Security department.

There is no perfect protection and modesty, vigilance and a permanent capacity to re-evaluate chosen solutions must predominate. The permanent quest for improving the current situation and adapt it to the ever moving evolution of threats can be facilitated by the implementation of virtuous cycles like PCDA (Plan, Do, Check, Act) and pluri-annual security budgetary planning, assessed every year, implying all the actors (Security, IT, HR, Finance) and legitimated at the highest levels of the corporate ladder. ■

BUSINESSES' ECONOMIC SECURITY

Bernard Galéa

Security and Strategic
Intelligence Director
Group FM LOGISTIC

Master in Global Risk and Crisis Management (Paris1-Sorbonne) and holder of other degrees from the ESSEC business school in Operational Management of Ffinancial Analyses, Bernard Galéa did the first part of his career in the aero-naval forces, then was detached 17 years to the Ministries of Defense and Foreign affairs. He served in many countries abroad along with his positions in Paris. He joined FM LOGISTIC in January 2008 as CSO. After his setting up of the function, he enlarged his scope to Strategic Intelligence. He was awarded Security Director of the year in 2010 in the latest private security awards ceremony and became chair of the French chapter of ASIS in the same year.

The world is experiencing a dramatic change. We are confronted at the same time with armed conflicts, an "Arab spring" the spreading and consequences of which being still unpredictable, a tsunami in Japan that shattered all certainties in matter of nuclear safety and security, stopped supply chains and still threatens public health in the region, maybe even further than Japan, and a financial crisis ever rebounding that modifies relations and forces between nations.

The world economy evolution and globalization have had (and still do) geo-political and strategic economic consequences that strengthen commercial competitiveness on each continent. As Bernard Carayon, MP of the Tarn county, rightly underlined, paraphrasing Diderot during the ambassadors' conference in Paris on August 26th 2004 : *"without man's corruption we would not have to fear an economic war, this compulsive and violent illness of the economic body and we could achieve our natural state and enjoy an economic peace instead..."*. The daily news shows every day that nothing has changed.

In these circumstances, companies have to continue seizing all opportunities of development and most especially understand threats against their economic assets: classic threats (industrial espionage, technological theft etc...) or newer forms (cybercrime, disinformation, etc). A focus on business intelligence allows this

approach : *"business intelligence is mastering and protecting strategic information for any economic player. It has a triple goal : the competitiveness of the industrial fabric, the security of the economy and of businesses, and the strengthening of our country"* adds Alain Juillet in his reference book on economic intelligence training. On an operational level, this approach will not separate economic security, research and sharing of information (monitoring of all information, networks of experts and common good practices) from lobbying (influence practices with public and private executives).

The evolution of the threats and their management entail the imperative adaptation of Security organisations in businesses. If it is now well understood that the CSO must be positioned at the highest level of organisations, better still be a member of the board, efficient CSOs must also collaborate to the commercial success of their company. Our friends from the US have already integrated this dimension in their charts by calling this "security man" "VP insight", which connotes with strategic intelligence director. The issue for this person is not to define the strategy of the company but to accompany it, shed light on the dangers it will encounter in its activities and protect it (see the works of Pr. Jonathan Calof, from the university of Ottawa).

Beyond classic stakes such as securing sites and personnel abroad, this function must also fully participate in the economic security to protect the company from :

- industrial espionage and technological thefts ;
- risks to information assets (rumors, disinformation, attacks on the image of the company, e-reputation) ;
- commercial and competitive risks (counterfeiting, risks with clients, competition dangers, poaching of employees who have a special expertise or detain key-information, etc.) ;
- economic organized crime (laundering, corruption, off shoring, criminal gangs...). In that respect, the implementation of an ethical chart backed by a whistle blower system reinforces the security of the organisation ;
- cybercrime (piracy, worms, virus, etc.) ;
- geopolitical and societal risks (technological evolutions) ;
- economic impacts of terrorism ;
- risks stemming from mergers, acquisitions : i.e. the need to have an in-depth analysis of country-risks (to know where I am treading) acquire reliable information - convincing, cross checked and valid - on a future partner (to know who really is

this person I am dealing with), identify a local network (not act alone without reliable support). The interest of it all is to bring, during the due diligence process, all relevant elements that contribute to bringing light to decision making. ■

Operational recommendations

- **Have the parliament vote and publish a law on "business secrets" and impose - in an appendix - the existence of the "security classification confidential".**
- **Take this law to the European level in order to harmonize/ regulate business practices.**
- **Encourage the public/private collaboration with a better commitment of state agencies in the support of the economic development of enterprises. This necessarily goes by an equality of treatment of enterprises in the access to economic information with state agencies.**
- **Foster the development of the CDSE at the European level, on the model of associations like ISMA in the US (International Security Management Association) or still ASIS (American Society for Industrial Security).**

BUSINESS LIABILITY AND "SECURITY"

Régis Poincelet

Corporate Security
Department GDF SUEZ

Trained at Aix en Provence University of Law and Economic Science. Graduated from the Insurance Institute. After a career in insurance and risk management with foreign companies, he joined the insurance company MARSH as manager for big accounts. Insurance and Risk Director of LYONNAISE DES EAUX, then SUEZ. Security Director of Group GDF SUEZ where he created an Economic Strategic Intelligence Department. He is a member of the board of the CDSE.

FROM CLASSIC LIABILITY TO A FORM OF CORPORATE SOCIAL RESPONSIBILITY

Up until some years ago, the notion of business liability was essentially perceived as the result of a legal concept, the application of which could entail civil and penal sanctions.

That is the reason why businesses have imperfectly sought to transfer to insurance companies the consequences of their responsibility, because the issue was (through financial compensation of a prejudice) to mitigate a possible increase of liabilities in the balance sheet.

Moral liability was sometimes mentioned in law books, but only in the margin, and it was to better keep it to one side it since the sanction was only in the inner conscience of everyone and thus stood out of the financial arena.

Things have changed drastically. If the classic notions of penal and civil liability of course still exist and are even reinforced (if not perverted by the vicious game of what is commonly called "judicialization" - where courts are diverted to rule on petty disputes), we have to acknowledge, through the emergence of the CSR (Corporate Social Responsibility) concept, a new form of "moral" liability that calls on ethics (even if ethics and liability do not completely overlap). CSR is, according to the definition given by the European Commission *"a concept that designates the voluntary integration by enterprises of social and environmental concerns into their commercial activities and their relations with stakeholders"*.

The sanction of a breach of CSR by the enterprise is of a very specific nature in that it impacts most of all the reputation of the business, i.e. its image, even before having the dire and catastrophic financial consequences we have seen, which are not susceptible to be covered by insurances.

THE START OF A NEW FUNCTION : FROM SAFETY TO SECURITY

In this broadening of the liability concept and of the aggravation of its consequences, we witness the beginning of a novel way of understanding the contents of the mission achieved by security professionals and the goals attached to it. This is an evolution prompted and supported by these very professionals when they write every day their doctrine in circles like the CDSE.

To illustrate this thesis, suffice it to take the example of the due protection of personnel, either travelers or expats. The judicial decision in the 'Karachi' case that goes back to January 15th 2004, drastically reminded businesses they were liable for the security of their employees, that it was an absolute obligation, and that their responsibility could be engaged on the ground of the "inexcusable fault", even in the event of a terrorist bombing that each and everyone until then thought, maybe candidly, to be part of the exempting case of absolute necessity.

Professionals have reacted to this trend by taking "standard" measures of prevention and protection aiming at ensuring and reinforcing personnel security. In a second stage, they also understood that this mission could not be accomplished without calling upon people specialized in the monitoring of risky countries whose expertise had been neglected too long.

One can therefore think that multinationals are going to opt for new ways of setting up in risky countries, taking into account the new CSR principles which are to live "with" and not "in" a country, or still by wondering not what can be produced there but what can be done with its inhabitants who are more often than not our employees too.

CSOs will have to integrate that new approach of their remit if they do not wish to continue to "react only to non-conventional situations by the all too classic "evacuation" of expats. With the exception of some justified, because extreme, cases, everybody knows that the real motivation for an evacuation is certainly the laudable concern for protecting the personnel, travelers or expatriated, but also the illusory concern not to engage one's liability (or at least to dilute it) by the adoption of a comfortable, if gregarious, behavior.

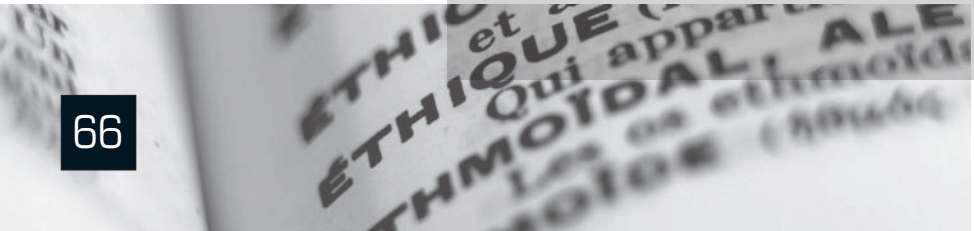
This is the reason why an ethical behavior from the CSOs will lead to the adoption of appropriate measures for the personnel who are not expats and for whom an evacuation would be meaningless. Neglecting this issue will most certainly be considered as a discrimination in years to come.

NEW PERSPECTIVES...

This example demonstrates that security professionals will have to broaden their scope in order to be perceived, within their business, as able to accompany its development by taking calculated risks but also by abiding by other imperatives than security only, like ethics.

Our goals are of course to win new markets and ensure business continuity (even when circumstances make them hazardous), but these goals will have to do with the imperatives we have just mentioned.

To get there from here, CSOs will have to use their imagination and accept their responsibility in this process. ■



TOWARD A CO-PRODUCTION OF SAFETY/SECURITY

Charles Yvinec

Security Director, CSO
Group AIR FRANCE

After the École Nationale Supérieure de Police in Saint-Cyr au Mont-d'Or in 1982, he was posted in judicial, border and community police forces, and then joined the cabinet of the General Director of National Police. After another post as regional border Director in the French Antilles, he went to the General Secretary for National Security at the Presidence of the Republic where he was promoted Contrôleur Général.
AIR FRANCE Security Director since 2004 and member of the board of the CDSE.

ENFORCING A LEGAL AND REGULATORY FRAME

Whenever the CSOs functions are mentioned, one immediately thinks that the CSO would mainly have to deal with "confidential" matters, in relation with public authorities, sensitive remit which management of would be restricted to specialists only. This image does not really fit the reality of this job, made of ever more numerous regulations, that are strictly monitored and progressively submitted to the same norms as those that rule the activities of any business.

This evolution finally resulted in that today the CSO is more concerned with compliance than anything else.

Under these circumstances, the nature of the relation that the Security Director has with public authorities is more like the one the average citizen has vis-à-vis the public services than those, a lot more blurred and secret, that our ancient colleagues, the "old boys", had with their privileged correspondents inside specialized civil or military services.

This new relationship, purely administrative, is certainly more constraining and it imposes exchanges with relevant authorities at each stage of the implementation of a Security Department, whatever the enterprise.

- When drafting the procedures that will be put in place, the CSO will first seek to obtain advice or counsels on applicable texts especially when there is legal uncertainty from relevant public services.
- When implementing measures afterward he/she will continue to exchange with them, notably when and where security programs have to be vetted by a public authority.
- Finally the same contact will be sustained in the phase of monitoring and controlling by state agencies of eventual non-compliance cases

A JOINT MANAGEMENT OF SECURITY

This type of relation that seems to be a form of "subordination" because the enterprise is largely dependent on decisions made by public services is leaving place to a more and more joint relationship.

Ministries and state agencies have indeed realized by and by the necessity of working in partnership with the professionals who are concerned with security processes and regulations in order to avoid drafting and publishing ill-adapted or even inapplicable texts.

Corporate security managers and heads are thus invited, individually or collectively, face to face or in commissions, to contribute to a shared management of security issues between public and private partners. This job of reflexion and conceptualization undoubtedly participates to the valorisation of the CSOs function.

Once the procedures are elaborated and published, the enterprise expects the CSO to have consequently an efficient management of the risks, which demands a great capacity of anticipation, reaction and permanent adaptation to reality by taking into account the feedback of previous crises.

Whatever the performance or the qualities of private security firms, one has to admit that the contribution and advice of public services have no match in the implementation of a security policy within a private company. Indeed the state plays a unique role for the validation, treatment and assessment of sensitive information.

INFORMATION AT THE HEART OF THE CO-PRODUCTION OF SECURITY

If main corporate businesses have long since attempted on their side to obtain information, stamped with the seal of the state, giving this mission to their Security Officer, the State, on its side has long shied away from engaging into a collaboration which it perceived negatively as perilous, fearing breaches of sensitive information.

This feeling however has evolved lately and following the much cited example of Anglo-Saxon countries, French authorities now associate the private sector, multinationals interests among them, with their regulatory activities.

Ministries, Foreign Affairs first of all but also some specialized agencies progressively set up mechanisms to improve an essential communication toward enterprises through seminars, commissions joining public and private sectors.

The International Commission created by the Foreign Affairs Ministry and the Cindex (Inter-enterprises Center for Expatriation) and the CDSE is a perfect illustration of this partnership destined to ease information sharing and assessment of the situation in risk-countries.

If the exchange of information is not an issue when it is about domains where confidentiality is not very high, it goes otherwise when the communication is about highly sensitive matters.

Specialized services, which are legitimately cautious, are intent on giving away information only to entrusted correspondents, either on account of their professional background, or because they had the opportunity to assess their capacity to deal with this type of information, in particular under the security classification of an official authorization "confidential" or "defense secret".

In order to facilitate these exchanges when time urges and even in sensitive domains, it is highly recommended to organize beforehand this public/private relationship through protocols and to designate or accredit correspondents within the security department in charge of maintaining the contacts.

It is also important to determine the objectives of this sharing of information in order to avoid possible confusions or conflicts of interest between the two sectors, the interest of the state being sometimes different than the enterprise's one, especially in the social and economic fields.

Safety and security within an enterprise pass by a new way of thinking our relationship with the government to streamline and optimize our reciprocal capacity of reaction. ■

COMPLIANCE : AN OPPORTUNITY FOR SECURITY DEPARTMENTS

XAVIER GUIZOT

Xavier Guizot

Head of Risk and Compliance Management of the CARREFOUR Group

Head of Risk and Compliance Management of the CARREFOUR Group, Xavier Guizot is in charge of Risk Management, Business Intelligence, Crisis Management, Compliance, Ethics and Security. Trained in financial schools, he was Risk Prevention Director prior to his current functions, and before that Projects Manager for the Secretary General of the Group.

COMPLIANCE ?

The French often use the term "compliance" from the English language, when they should say "conformité". It is probably because compliance is a rather new field in Europe whereas it took a crucial importance in the US long ago, but especially now after the financial scandals like Enron of the years 2000.

Compliance mostly is the result of a great increase in norms and texts outside the usual legal domain - what is currently called "soft law", of more numerous controls and a significant hardening of sanctions. Through these practices, compliance aims at enhancing the enforcement of procedures and processes and also at strengthening resilience of organisations by a greater prevention.

All this is implemented through "compliance programs" that apply to all domains of risks to which the business is exposed (law abiding, corruption, confidentiality)

As any other prevention policy, the "compliance program" must be as closely as possible adapted to the realities of the company, to its culture, organisation and issues. It also depends on the core business of the firm, with a pressure and regulatory obligations that are more or less constraining according to sectors of activity. For example, compliance is more developed and sensitive in financial sectors.

Compliance is also one key element of the internal control process, a sort of call to the law reminding everyone that sustainable performance and good results can only be attained through a total respect of regulations. Consequently, intelligence monitoring, information and training are crucial in the mechanism, especially in a de-compartmentalized approach of the business.

Whereas the direct or indirect cost of these programs can be perceived as a hurdle, the success of the process will mostly depend on the operational and pedagogical character of the approach.

COMPLIANCE AND SECURITY

For the CSO, compliance takes two dimensions: compliance programs of the security function proper, i.e. monitoring security processes and procedures, but it is also getting involved, as CSO, into the global compliance of the business regarding all its activities.

- For the security function per se, global standards are just fledgling and hardly developed even if by nature some sectors are submitted to regulations or specific constraints (defense, energy, aeronautics) with a recently reinforced focus on critical/vital infrastructures. If compliance varies according to the sector of activity, it also does according to the domains in which the security department will intervene because these fields are submitted to regulatory obligations more or less constraining : CCTV, confidentiality, fraud prevention, PCA, private security, travelers and expats protection... If several specific ISO norms do directly concern the CSO (27001 for IT security, supply chain), the peripheral protecton, organisation and compliance aspects of the function can also be inspired by a broader risk management approach like the one found in the ISO 26 000 and the COSO.
- Because of his positioning and his role in internal control, the CSO is also a major player in supporting the global compliance policy of the enterprise.

With an exemplary behavior and leadership, actions to service the business and a transversal and de-compartmentalized vision, the CSO can be an adviser, a counsel, a facilitator/monitor for all compliance issues other functions have to cope with on their side.

Compliance is a real opportunity for CSOs for overseeing the general conduct of the business in an evolving regulatory context. It is also a positive way for improving the image of the function through the demonstration of its capacity to apprehend the whole enterprise with a global view and an expert's perspective ready to help everyone. Compliance however is not the alpha and omega of security. It is just a means to reinforce mechanisms without forgetting common sense, vigilance and intelligence that enable to identify issues and anticipate them in a time of increasing uncertainties where rules of tomorrow are not drafted yet. ■


nationaux. Droits
tecteurs. Un ton,
PROTECTION (lat. *pr*
du mal. La protec
de lettres a rendu
sa protection, prer

Operational recommendations

- According to the core business of the enterprise and his/her scope, the CSO will undoubtedly benefit from building one or several *"compliance programs"* regarding security. To do that the CSO will indentify regulations and references to which most of the people working for security are submitted in their daily tasks, assess the compliance issues they have, help them in drafting action plans to address these and eventually choose items to be controlled by Internal Control.

- A *"compliance program"* could for example be drafted for travelers' security since all the elements needed for creating such a program are here : regulation (labor laws), jurisprudence, references, available training and sensitization programs, and KPIs.

- The efficacy of compliance programs will also depend on the *"normative intensity and dynamics"*, i.e. the creation of a working group mixing public and private partners and ministries to study applicable norms regarding security, with both a European and international perspective. Being intent on simplifying and making existing norms more efficient, this process would improve the visibility and coherence of all the references.

THE CHALLENGE OF COMMUNICATION FOR SECURITY ORGANISATIONS

ALAIN BELLEFACE

Alain Belleface

Deputy CSO
Group VINCI

Master in risk management and graduate of INHESJ. Has worked fifteen years at the Ministry of Defense, then two years in a firm specialized in international security and crisis management. Joined Group VINCI in 2008 as Deputy CSO.

The business is an open world made of information exchanges, sharing and communication. Therefore, the legitimacy of Security organisations and their embedding in the business as support functions is as indispensible as more traditional ones, and to be effective requires excellent means of communication.

"Say what you do and do what you say" along with a transparency, ethics and job streamlining concern, is a necessity to embed the Security function and provide it with real broader scope. On the contrary, silence will only entail interpretations, suspicions, rumors, fantasies, all of which do a disservice to Security.

Communication of Security organisations should be turned inward so that they be clearly identified to facilitate feedback of information and to demonstrate their expertise and capacity to address problems for the benefit of all company levels, from top management to field managers. It is also turned outward for easing and helping exchanges with public and private sector stakeholders, with whom dialogue must be sustained and enhanced.

AN INDISPENSABLE FOCUS ON IMAGE

The absence of communication as much as the professional background of most CSOs and their teams (mostly from State specialized services) encourage isolation, stigmatization if not fear. One has to admit that the image of Security organisations is often negative. In the company they are perceived as center costs, hindering the business, secretly investigating and even stepping into private matters. Externally they are seen as structures designed to recycle retiring civil servants. Because these images are wrong, communication on the structure is essential.

On account of their professional background, CSOs are technicians who primarily benefit from a multi disciplinary expertise. They are apt to deal with urgencies, crises, all sorts of events where time for communication and for action do not match.

Thus communication is a skill ill-mastered by most CSOs, all the more that they have served in State structures where everything is codified or preplanned and where discretion, reserve and confidentiality are often crucial.

As for CSOs coming from the internal business ranks, many have technical or scientific backgrounds that have no more prepared them to communication than their colleagues from the public sector.

Without going so far as to position itself on the opposite side of corporate communication, the Security organisation must stand out through the building up of an image and identity that are visible, legible and attractive. All available tools and professional techniques should be used toward that goal. Mottos, work on image, the creation of a visual identity, use of Internet, drafting and disseminating of good practice booklets, participation in internal newsletters, theme campaigns, employees' testimonies are perfect examples of what can be utilized to reach out to all categories of personnel.

PREVENTION AND COMMUNICATION : AN INDISPENSABLE TEAM TO CONVINCE

An efficient Security policy takes ground on three general pillars : technical, organisational and behavioral measures. If the first former two are predictable and measurable, the third pillar is random, unstable and hard to master. To mitigate this risk, an effort will inevitably be placed on anticipation, preparation and prevention. This goal will be attained through communication with the employees and by rolling out a consistent security policy.

The efficacy of specific or general security policies mainly relies on the fact that personnel adhere to them. Indeed neglect creates an opportunity for the malevolent one and vigilance is maintained when certitudes are forgotten.

Security often comes as a troublemaker for most employees' peace of mind. Procedures can be perceived as constraining and unjustified because an employee is also a responsible citizen who, in his/her private life, will claim to already have the right behaviors and comportments.

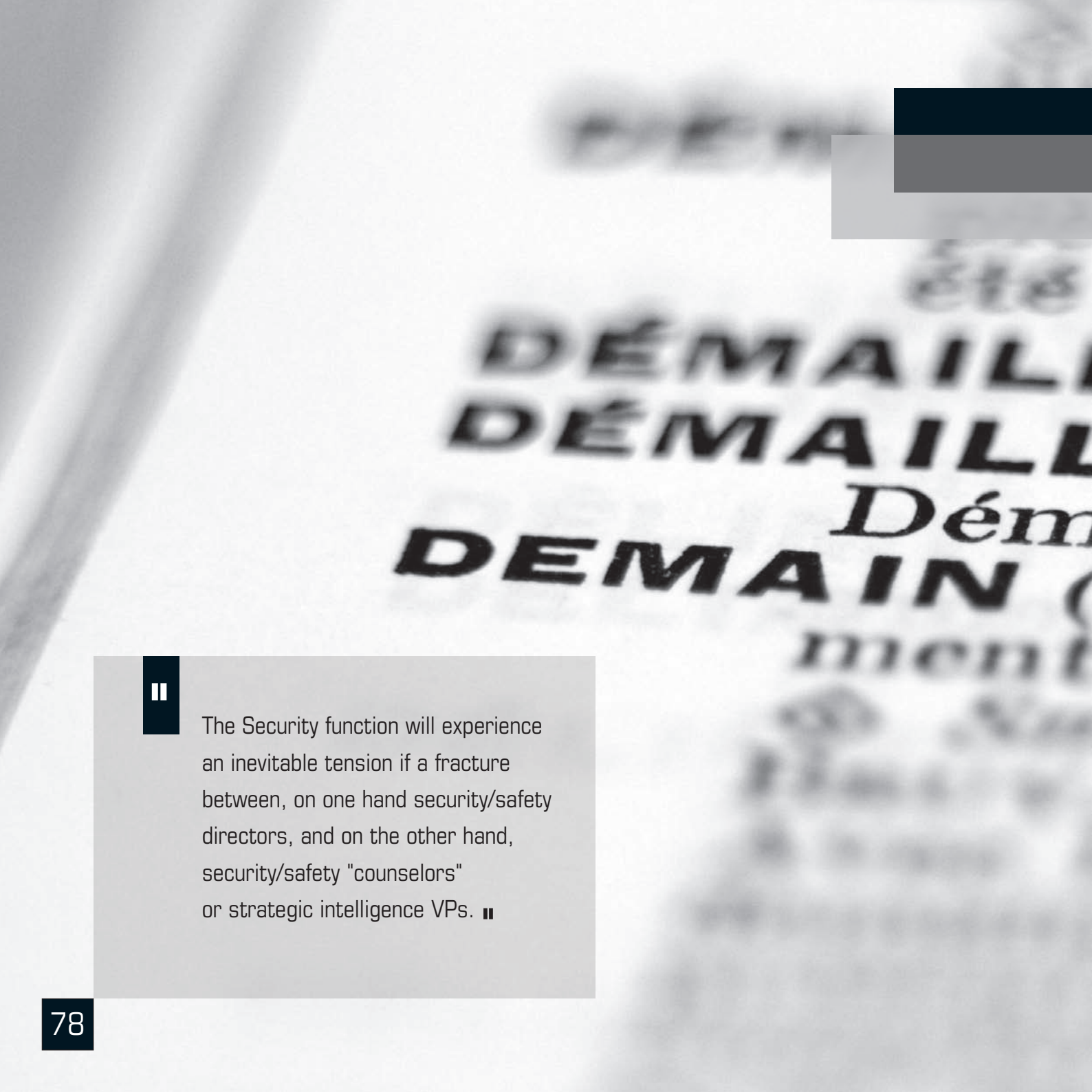
Because the margin to convince is narrow, Security organisations have to learn how to pass the right messages to obtain a natural adherence to good practices and rules. The right message must also be aligned with the reality of the enterprise, its core businesses, environment, market, and its competitive and regulatory surroundings.

ANSWERING TRANSPARENCY'S DEMANDS

Finally, beyond the image and the prevention reasons, Security organisations must prepare to communicate on their proper activity at the request of senior management.

Social liability regarding physical protection of employees, the possibility of seeing breaches of secrecy prosecuted or still ever more comprehensive risks analyses, the trend is toward more empowered Security organisations. Add to that that executive or all forms of boards will be brought in the future to request detailed information on actions driven by Security organisations. In a general frame of enlarged social liability that demands always more communication and transparency from businesses, it is highly probable these will have to address security issues in their annual reports. And then it will have to be completely mastered after what is already being done for financial communication for instance.

Developing internally, training specific personnel, hiring contractors to help, taking ground on corporate communication services' capacities, all means are available for CSOs to successfully address this challenge that will allow to address the other topics mentioned in this White Paper. ■



The Security function will experience an inevitable tension if a fracture between, on one hand security/safety directors, and on the other hand, security/safety "counselors" or strategic intelligence VPs.

CONCLUSION

OLIVIER HASSID

CDSE Managing Director

Olivier Hassid

Managing Director
of the Club des Directeurs
de Sécurité des Entreprises
(Club of Business Security Directors)

PHd in Economy, Managing Director of the CDSE, he was Security Director in a municipal team in 2003 before joining the Prime minister services for security issues. He was then assistant to the General Manager at BRINKS before being joining the CDSE. He authored numerous books on security and risk management. He also edits the CDSE review " *Sécurité & Stratégie* ".

What profile for tomorrow's CSO ? What will his/her missions be ? To whom will the CSO report?

Our words of conclusion are not to suggest there is an ideal profile simply because there is no such thing. According to the history of the business, of the personality of its CEO, of the nature of the threats to which the enterprise is confronted, the profile of the CSO and the contents of the role will considerably evolve. Having said that, some trends are visible.

To start with, the function will grow within businesses in coming years.

In spite of recent cases that may weigh on the reputation of Security departments, businesses will increasingly need teams focused on safety/security.

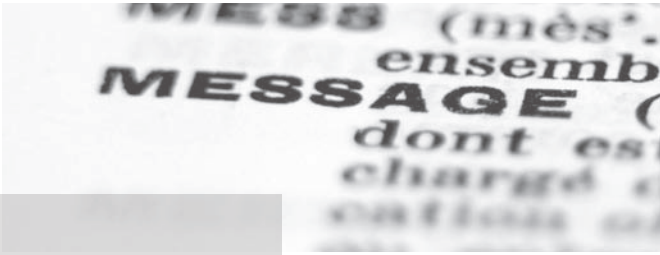
The expanding of most businesses abroad, what is referred to as globalization, along with the virtualization of the economy, put more and more company assets at risk. Let's name for example kidnap, data loss, fraud or even pressures on employees... To mitigate those dangers in high risk countries where the business is in search or growth, there will be no other choice than to integrate security from scratch in any investment project.

Secondly, the Security function will experience an inevitable tension or even a fracture between, on one hand Security/safety directors, and on the other hand, security/safety counselors or strategic intelligence VPs (or VP insight 1). Indeed it is quite possible that businesses will call upon two sorts of expertise. First a CSO proper, in charge of ensuring (in) tangible assets and employees' security. Then a security advisor tasked with the supporting all international projects. It is not necessarily the same person that would play the two roles. The former is more operational and focused on organisations while the latter is closer to the very strategy of the group and of its top executives, bringing a global vision. One is safety oriented and focused on management while the other is more on securing strategies, somewhat similar to that which was said by the President in his opening words of this White Paper. The former would deal with audits, sensitization programs for travelers where the latter would be on due diligences business intelligence, negotiations, acquisitions and mergers. Unless the equation is solved thanks to hybrid personalities at ease in both economic and security matters. Those two sides of a function could also be articulated into one same direction, with the caveat that a well organized "bi-cephalic" management would be a benefit to the business while an ill coordinated one would be source of rifts, loss of managerial efficacy, incomprehension and friction.

Thirdly, will the function be staffed with personnel coming straight from the business or former law agencies officers or even military ? In a recent study published in *Security and Strategy*, the researcher Frédéric Ocqueteau observed that the function in fact is *"militarizing" itself, military officers taking advantage of the credit they have "to dispose of an unvarnished reputation for knowing how and where to timely collect the right information at the right sources 2"*. But the dice is not cast yet. Indeed we soon could see the arrival in these functions of people who have a very different background like IT, engineers or still financial executives. It is almost certain for example that with the development of the digital society IT security experts will be called to exert these roles. Likewise, the "financialization" of economy may entail that CSOs could originate from the banking or insurance sectors. One should not forget profiles from the core

1. See Bernard Galea's assertions in "Economic security" page 59 in this White Paper

2. Ocqueteau, "CSOs'Profiles and Trajectories Security and Strategy, March 2011- June 2011.



business : there are people out there who have already been confronted with security risks and have found how to mitigate them. To some top executives, the expertise in "comprehension of business mechanisms" might very well prime over any other knowledge, even security ones.

Lastly, the function will largely depend on university training. In France some thirty or so of those are available. CSOs of the future will undoubtedly emerge for the most part from these educational programs which precisely combine security management, criminology and law. These new profiles will then maybe address the need of hybrid personalities we mentioned, both savvy in ROI issues and untouchable in matters of situational prevention. ■

1 rue de Stockholm
75008 Paris - France
Tél. +33(0)1 44 70 70 85
Fax +33(0)1 44 70 72 13
contact@cdse.fr
www.cdse.fr