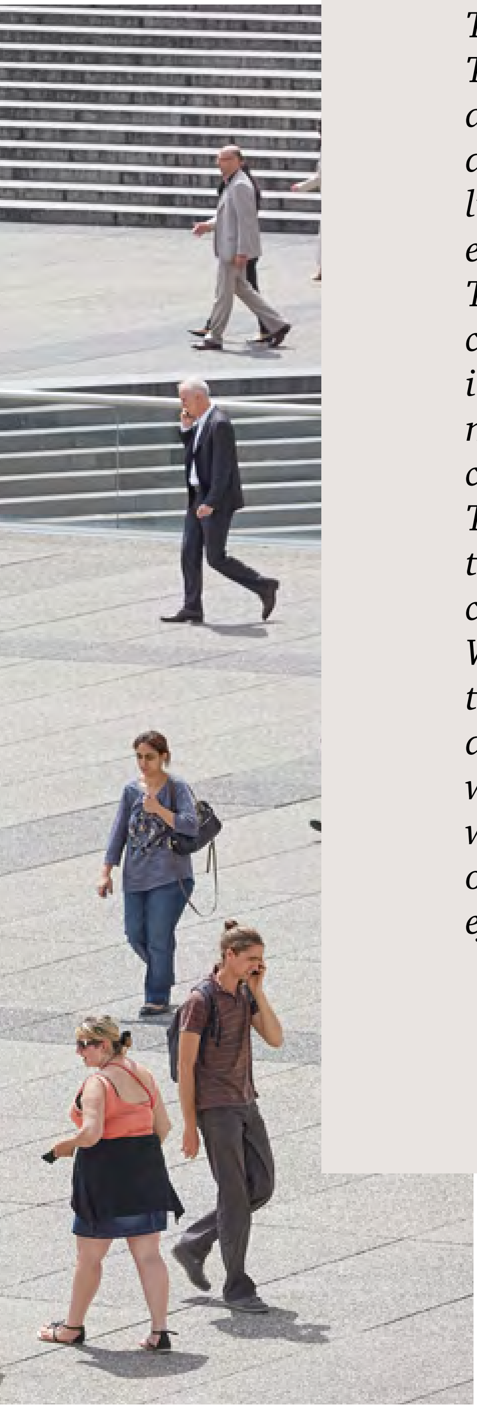
The transformation of the Security sector: towards a new paradigm

Feedback on company practices on a global scale

pwc

Table of contents

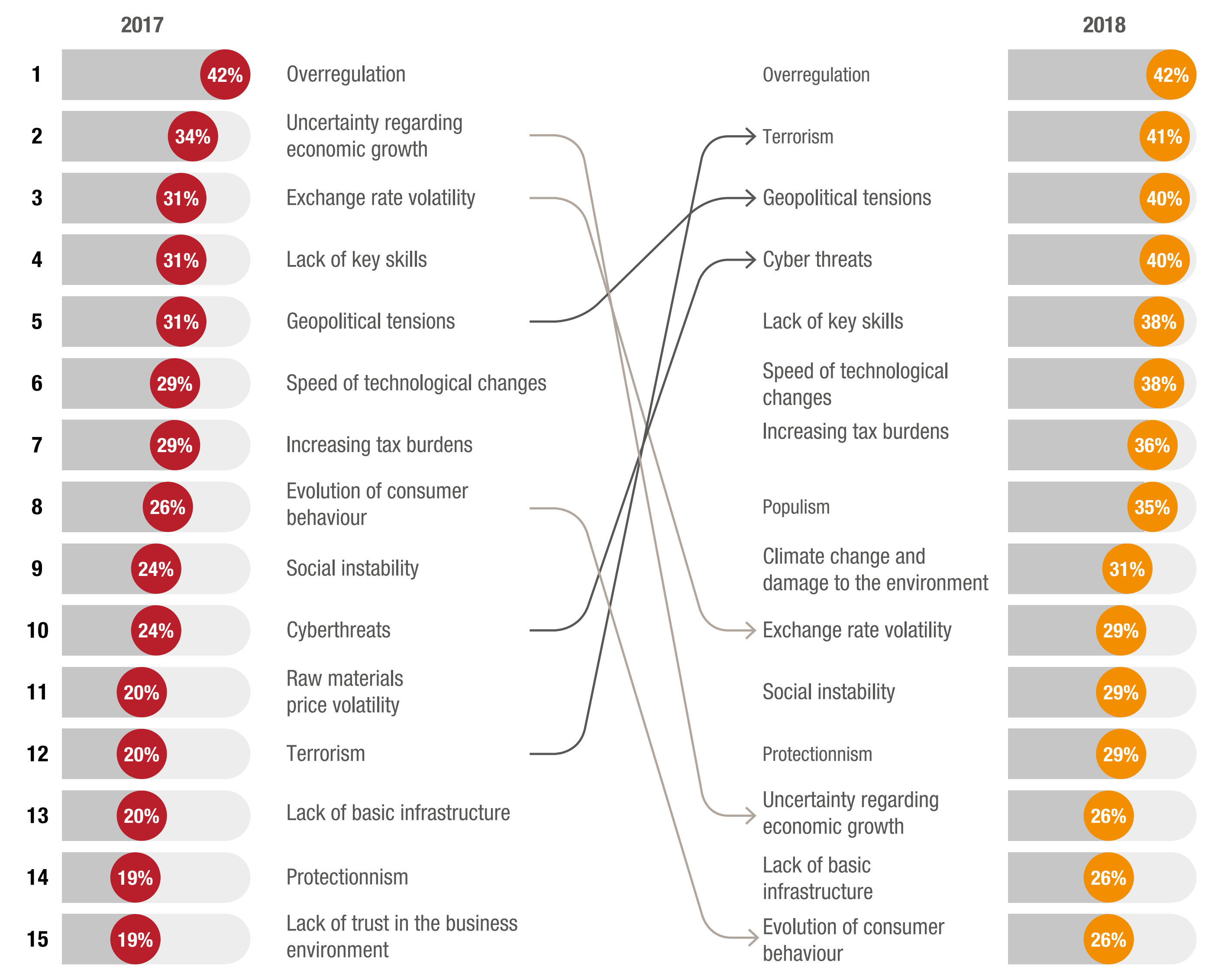


The security sector is in full transformation.
The organisational structure of security departments, their director's affiliation as well as the scope of their responsibilities are undergoing deep changes. These changes are particularly linked to the strategic evolution of companies, with the emergence of new risks and increased vulnerability.
The PwC annual global study regarding the priorities of company leaders- the "CEO Survey"- reveals the growing importance of terrorist threats on companies- threats that moved from 12th place in 2017 to 2nd place in 2018 (refer to the chart on page 2).
The study also highlights their growing fear of geopolitical tensions, now ranked as the 3rd most important concern for companies, whereas cyber threats are now ranked in 4th place. While the perception of these threats varies from one country to another, terrorism, cyberattacks and geopolitical upheavals are at the heart of business executives' concerns throughout the world. In this context, it is recommended that leaders study which best market practices could be implemented by their organisations to not only deal with current risks more effectively, but also better anticipate those to come.

Evolution of risks: Terrorism and cybersecurity threats at the centre of leaders' concerns

Among the following risks, which do you find most concerning with regard to your company's growth perspectives?

Percentage of respondents "extremely concerned"



Source: PwC, 21st annual barometer CEO Survey
Basis: all respondents (2018=1293; 2017=1379)

Source : PwC, 21st Annual Global CEO Survey https://www.pwc.fr/fr/assets/files/pdf/2018/01/pwc-ceo-survey-report-2018.pdf

Presentation of the study

This purpose of this study is to highlight the key trends identified during research conducted by PwC. It consists of three main parts: part one explains the new organisation of the security department, notably with regard to its position within the company, the growing involvement of security in the field of cybersecurity, and the collaboration between security and cybersecurity teams. The second part of this study is concerned with the resources available to the security department: in a context where mastering information is at the heart of a security policy's success, the use of Data analytics has been identified as a key resource. Other resources identified include measures allowing the deployment of a security culture within the company. Finally, the third part of this study is devoted to developing a new frame of reference based on a model involving three lines of defence.

Methodology of the study

The results of the present study are based on feedback received from the field, most notably from inquiries and interviews carried out from January 2018 with twenty international companies in various sectors.

Main goals

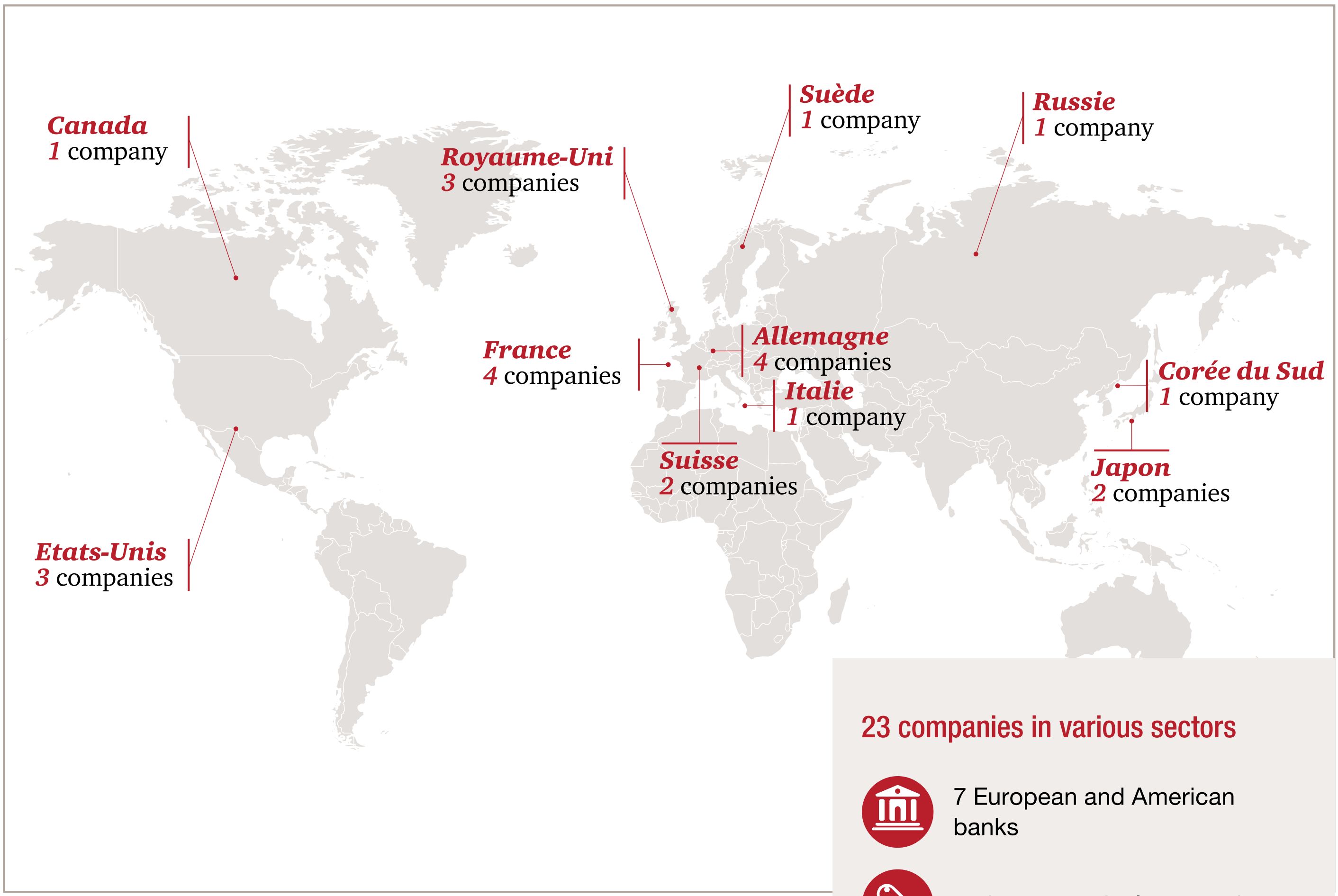
- Analyse and reveal the main trends of security services of international groups
- Understand how international companies have modified their practices and adapted their strategy to respond to the development of threats;
- Identify the methods used by such companies to modify and adapt their practices and strategies, as well as gain an understanding of best organisational practices.

Key figures

- **23 companies surveyed,**
  20 of which are international companies that generate a turnover of **20 billion dollars** and are present in a total of more than 60 countries.

- **50 interviews carried** out with Chief Safety/Security Officers or Chief Information Security Officers.

More than 10 countries represented



23 companies in various sectors

- 7 European and American banks
- 4 pharmaceutical companies
- 3 companies in the luxury sector
- 2 aeronautical and defence companies
- 2 telecommunication companies
- 5 companies in other sectors of activity (engineering, insurance, materials, etc.)

A new departmental organisation

Most of the international companies on the panel are reflecting on the position and organisation of their security department. A significant number of surveyed companies are currently changing or have recently modified the organisational structure of their security department. In most cases, these changes are explained by the arrival of a new Chief Security Officer or by the transformation of the company's strategy (for example: merger/acquisition). Today, departments are evolving and becoming increasingly structured, centralised, visible and open to diverse profiles. Furthermore, security departments are becoming increasingly concerned with the issue of cybersecurity and companies are attempting to strengthen collaboration between their security and cybersecurity teams.

Position of the department within the company

The position of the Security department within the company is currently undergoing a complete transformation. As part of the study carried out by PwC, three important trends have been identified: centralisation, structuring, and professionalization of the department.

Centralising the department

More than 50% of surveyed companies tend to centralise their security program through the creation of a sole department at the company level which is responsible for piloting its governance and operations.

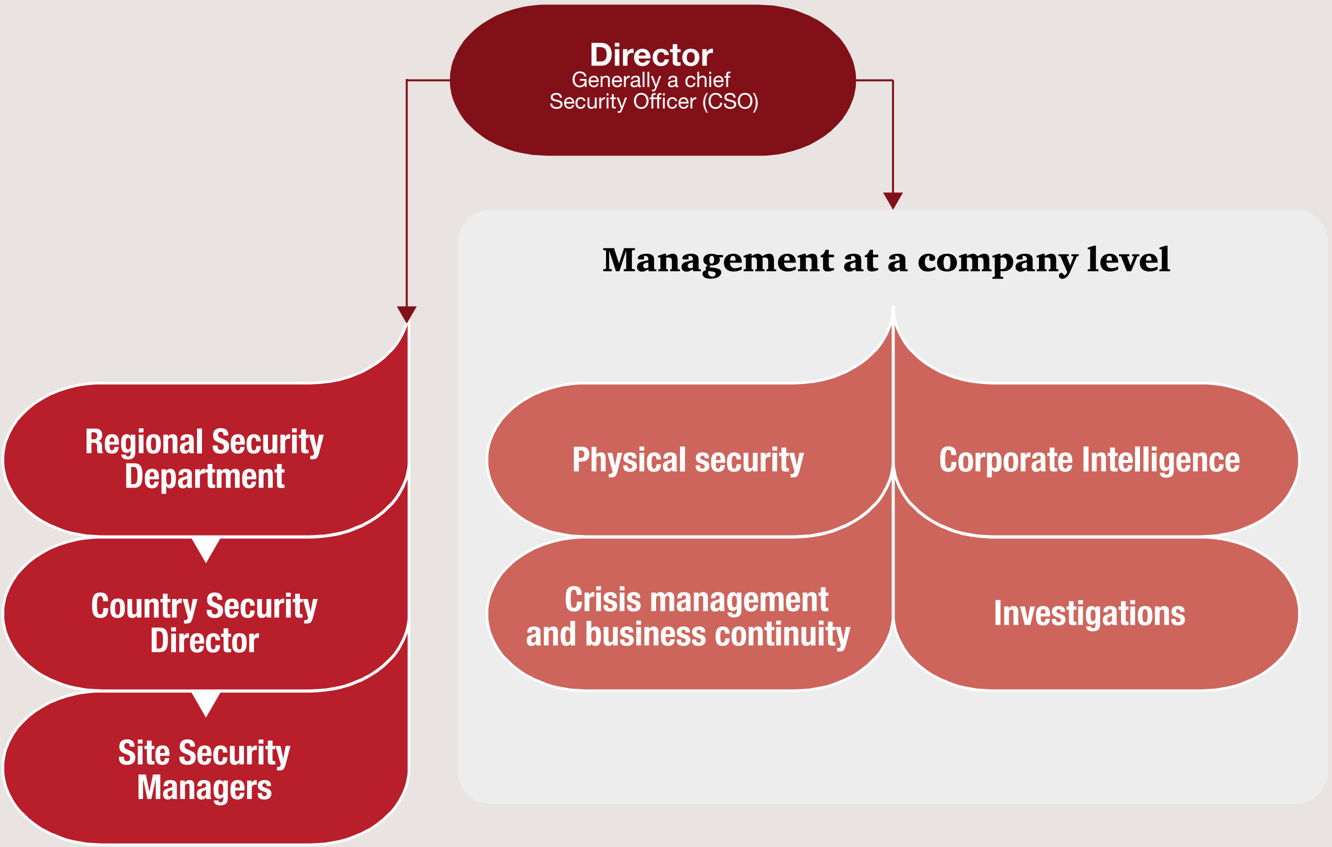
The centralised model implies:

- A significant workforce at the company level (more than 30 professionals);
- A central department as a main decision maker with regard to security management (definition of policies and directives, writing of standards, reporting and indicators, etc…)
- An operational role at a global level (studies, corporate intelligence, etc.);
- Control of security activities at a local level.

The main benefits of centralising the department mentioned by the surveyed companies

1. Centralisation facilitates information feedback as well as the consolidation of data reporting and therefore allows for better management (rationalisation of means and actions);
2. The centralised model ensures the application of the same standards in all regions, consequently reducing the differences in maturity levels of different regions;
3. This model is more visible and more legible for stakeholders, and is capable of being audited more easily.

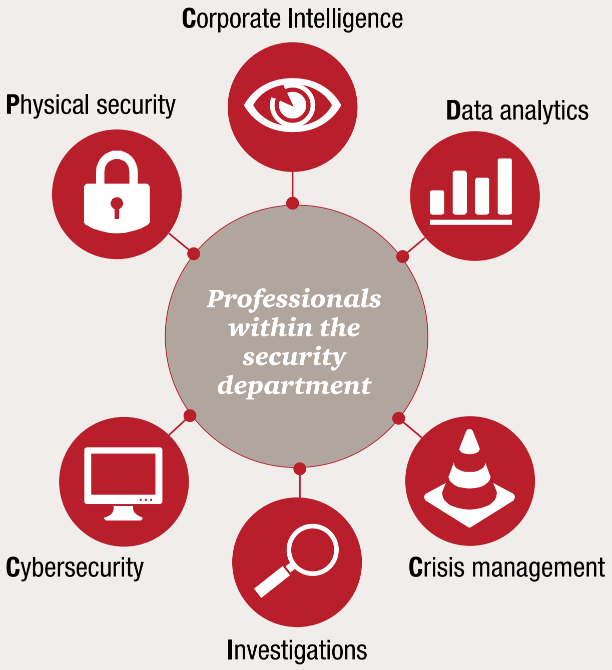
Example of an organizational model found in several large sample companies


Director
Generally a chief Security Officer (CSO)
Management at a company level
Regional Security Department
Country Security Director
Site Security Managers
Physical security
Corporate Intelligence
Crisis management and business continuity
Investigations

The links between the central and regional levels can be hierarchical or functional

Structuring and professionalising the department

The Security Departments of companies surveyed are structured around specific areas of expertise and are staffed with experts in physical security, information protection, crisis management, corporate intelligence, investigations and cybersecurity.
Recent years have been marked by a diversification of talents and the recruitment of new profiles such as data analysts (specialists of data analytics) and corporate intelligence specialists.



Legitimising the department

Considered for a long time as being limited to ensuring the physical security of buildings and travellers, Security leaders have seen their role evolve. Today, most Security leaders report directly to a member of the executive committee, thereby improving the Security Department's credibility and legitimacy. The Chief Security Officer can be considered as the leader of physical security, information security, and crisis management at the same time.

Involvement of the Security department in cybersecurity issues

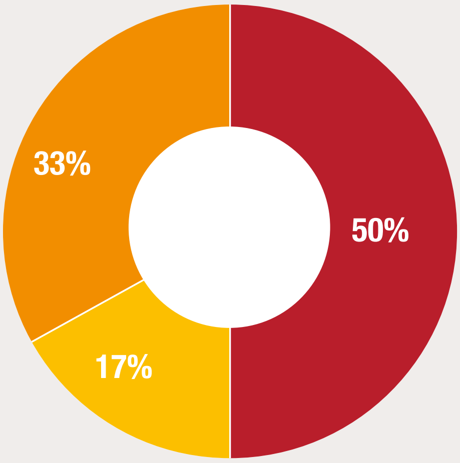
While reporting by the Chief Information Security Officer (CISO) to the Security department remains somewhat rare, this is nevertheless the case in 17% of companies.

The decision to have the Chief Information Security Officer report to the Chief Security officers is often linked to the CSO's background: he may also be a former CISO or have experience in cybersecurity within a public administration (intelligence services or technical services).

In general, for all of the companies in the present study, their Security departments are involved in:

- Protecting information (governance, awareness raising actions, etc.);
- Participating in crisis management and incident response;
- Managing cyber-enabled crimes, i.e. traditional crimes (fraud, harassment) amplified by the use of information and communication technologies (ICT).

To whom does the CISO in your company report?



🟥 Reports to the Chief Information Officer or Information Technology (IT) director

🟨 Reports to the Chief Security Officer

🟧 Reports to the Chief Innovation Officer, Chief Operating Officer or Chief Risk Officer

According to the results of the study, approximately one in two companies states:

- Not entrusting the technical department with the management of all cybersecurity issues;
- Resorting to versatile profiles (for example, persons with experience in both management and cybersecurity);
- Drawing on the expertise of the Security department in discussions and strategic decisions linked to cybersecurity issues;
- Ensuring the close involvement of the Chief Security Officer in the management of cybersecurity crises.

> *Criminals cooperate more efficiently than us .*
>
> Chief Security Officer of an international bank

Towards better cooperation between security and cybersecurity

Until recently, there was little communication between the security department and the information systems security department. Interviews carried out with surveyed companies highlight the necessity of de-compartmentalising and ensuring the sharing of skill sets between these two fields.

What are the fields of cooperation identified between security and cybersecurity teams?

- Strengthened interaction between security and cybersecurity experts through frequent exchanges regarding tests, procedures and tools;
- Collaboration between cybersecurity, corporate intelligence and physical security specialists within the Security Operations Centre (SOC);
- Common efforts aimed at better understanding the forms, characteristics and typologies of cybercrimes;
- Exchanging information through "data fusion cells" (see page 12);
- Common actions in case of crisis or emergency (participation in the crisis unit, etc.);
- Collaborating on internal threat issues ("insider threats");
- Joint crisis management exercises;
- Raising professionals' awareness of the issues linked to cybersecurity/security;
- Cooperative work on security directives (policy of information protection, etc.).

The questions to ask yourself

- What changes to the organisational structure of your security department would be required in order to improve its performance?
- Does the security centralisation/decentralisation strategy implemented in your organisation allow risk to be managed conveniently?
- What role does the Security department play in terms of cybersecurity?
- What measures have been implemented to de-compartmentalise departments and ensure better collaboration between security and cybersecurity teams?
- Who is responsible for crisis management? How is it organised?
- Are the risks of information leakage well covered by your company?

New means of action

In an effort to improve proactivity and efficiency, the Security department is making use of new technical and organisational tools. The increase in new technologies, combined with the emergence of new methods for collecting and analysing data, allow the Security department to better understand its risks and anticipate potential hazards. In a continually evolving and increasingly complex environment, the means of monitoring and analysis are the key to a resilient organisation.

The efficiency of the Security department is also based on the commitment of each of the company's employees- today, company employees are becoming real security ambassadors and actors and it is for this reason that companies are seeking concrete solutions to strengthen their security culture.

The value of information at the heart of security and Corporate Intelligence

In an environment where the quantity of available data is rising in an exponential way, the production of relevant knowledge is becoming a key issue for security and corporate intelligence (CI) teams. Corporate intelligence can be defined as the research, processing and exploitation of useful information for economic actors.

This awareness, clearly observed in the financial and industrial sectors, translates into the increasing importance of Corporate Intelligence teams, which are adopting new tools and methods, as well as the creation of "Security Operations Centres" (centres of risk and reaction analysis) and transversal units of data consolidation and processing ("fusion cells").

More than 80% of surveyed companies have services dedicated to Corporate Intelligence

What are the activities implemented by the CI teams for the benefit of the Security department?

- Systematic support for every strategic decision (for example: merger/acquisition)
- Developing an information collection plan
- Identifying and prioritising information sources in order to have a general idea of the quality and accessibility of information likely to be of interest for the company
- Using several databases in order to intersect and verify every element of information
- Implementation of specific "Open Source Intelligence" tools (web crawling, specific databases, etc.).

Concrete examples of projects carried out by CI teams

- Identifying and analysing security risks
- dentifying vulnerabilities
- Verifying the trustworthiness of third parties
- Verifying a person's background (for example of a candidate during a recruitment process) in full respect of the laws in effect in the country
- Legal, economic, reputational and technological monitoring
- Collecting information during investigations
- Informational support for crisis management
- Identifying reliable partners in new markets

All surveyed companies reported having resorted to a subcontractor at least once for the carrying out of due diligence on third parties and/or in-depth investigations. The main reasons for engaging subcontractors are the following:

- The type of engagement is remote from the companies' primary skills;
- The engagement requires strong technical expertise;
- The engagement may turn out to be time-consuming or require greater resources than those available within the company;
- The need to obtain a critical analysis from an independent entity.

Corporate intelligence teams

According to the study carried out, more than 80% of surveyed companies have services dedicated to CI. Corporate intelligence teams report to the security department or to the strategy department and are in charge of identifying and minimising risks while at the same time favouring the development of the company and acting as a support for the leaders in their decision-making. To that extent, the CI service often works like an in-house consulting firm responding to the requirements of different actors. In most observed cases, the Corporate Intelligence service is comprised of five to twenty professionals, several of whom possess prior experience in intelligence or police services.

Security Operations Centres (SOC)

Given the permanent need for monitoring linked to security issues, large international corporations in the financial and the industrial sectors set up risk and security analysis centres ("Security Operations Centres") to ensure the monitoring of operational situations 24/7.

This practice is already well-developed in the field of cybersecurity (dedicated SOC). It tends to be more widespread via the deployment of management and security risk analysis centres whose goal is to:

- Collect alerts raised by the company's employees;
- Collect, analyse and process information relating to threats and security risks;
- Ensure a fast and easy exchange of in-house information in the context of a crisis;
- Oversee the link between the company and law enforcement agencies;
- Bring informational support to regional and local security teams in times of crisis;
- Populate security risk and threat databases.

« Fusion cells »

Fusion cells are a new trend within Security departments. They aim to take advantage of new technologies (big data, artificial intelligence...) and machine learning in order to:

- Aggregate a wide variety of data within a single tool in order to transform it into useful information;
- Create and sustain risk and threat databases (criminality, etc.);
- Process the information in order to offer a "user friendly" visualisation (dashboards, etc.);
- Organise the in-house sharing of information in order to transmit information to the appropriate actors;
- Provide analytical elements that facilitate decision-making, particularly by improving the ability to anticipate.

The implementation of fusion cells was only observed in 10% of surveyed companies. These organisations share similar characteristics: their Security departments employed at least one hundred professionals, including four to six data specialists ("Data Analysts and Data Scientists"). Moreover, these cells are systematically integrated in Security Departments whose scope also covers cybersecurity.

Deploying a security culture

An efficient system of security within the company requires a regular training course that goes beyond elementary e-learning. Several examples of concrete measures set up by the surveyed companies are provided below. The totality of these companies have begun to consider the best way to favour the incorporation of a security culture in the workplace.

Individualised training courses for persons with significant responsibilities

Several companies in the sample have set up training courses or "face to face" meetings with their executive officers for the purposes of raising awareness. During this dialogue, security professionals inform key leaders and their families of risks as well as best practices to follow. Particular attention is drawn to the use of social media and to different social engineering techniques used by wrongdoers. To ensure the development of appropriate reflexes, security and cybersecurity teams frequently send false emails (similar to phishing and spear phishing emails) to employees occupying sensitive positions.

Bootcamp security

Each year, groups of employees spend two to three days in a training camp ("bootcamp") where security experts provide them immersive training courses on how to behave in relation to malevolent acts. The employees learn more about their responsibilities and thus familiarise themselves with best practices.

Security correspondents

The designation of a security correspondent at the subsidiary/ business unit level is becoming an increasingly widespread practice. The correspondent is responsible for awareness raising matters, as well as for liaison with the central department.

"Serious game"

The use of learning and innovative awareness-raising methods is a frequently observed trend. Therefore, the use of "serious games", based on the principle of learning by doing, allows for the integration of key information by placing participants in close-to-reality situations in order to instil useful notions in them.

Did you know it ?

PwC has launched its first "serious game" dedicated to cybersecurity: Game of threats TM. This game is a realistic simulation involving real time decision-making in light of cybersecurity threats, and includes simulations from both the attacker's and from the company's point of view.

To learn more www.pwc.fr/fr/expertises/conseil/cybersecurite/game-of-threats.html

The questions to ask yourself

- Which specialised software do you use to collect, analyse and process security information?
- Which employee projects are devoted to Corporate Intelligence within your teams?
- Do you have monitoring teams devoted to security issues allowing operational responses to incidents?
- Which measures do you implement in order to build a security culture within your company?
- Do you possess the relevant means for analysing data necessary to the carrying out of your projects? Do you rely on data scientists within your security department or do you plan to recruit any?

A new frame of reference

Developments in risk management practices are leading Security departments to progressively transform their model in order to ensure conformity with the best organisational practices in this area. The studies carried out, particularly with the Security departments of financial sector companies, show that this willingness to optimise organisation often translates into the implementation of a model revolving around three lines of defence ("3 LoD model").

The three lines of defence model

The three lines of defence approach relies on the clear and prior definition of specific departmental roles and responsibilities. First, it is important to recall the objectives of this approach:

Le modèle des trois lignes de défense permet de :

- Ensure that responsibilities are defined and positioned at the appropriate organisational level;
- Establish a situational analysis in order to ensure that all of the organisation's risks are properly taken into account (existence of procedures at a relevant level, absence of useless redundancy...);
- Obtain a global vision of security issues, completely integrated within the risk management program;
- Demonstrate effective governance over time and ensure the avoidance of ethical dysfunctions.

The first line of defence

The first line of defence is responsible for the security of its perimeter, and its action falls within the framework of the company's security policies and procedures.

Generally, the first line is comprised of local, regional as well as central security units in charge of operational activities (investigations, traveller's security...).

The first line of defence is also represented by the totality of the company's professionals, who, through the implementation of good practices promoted by the company (sensitive information management procedures, suspicious event reporting, etc.), play a crucial role in their protection.

The second line of defence

The second line of defence is responsible for security governance. For this reason, the second line of defence is at the core of the strategy's definition and articulation, of policies and of security standards. It carries out the evaluation of global risks and vulnerabilities and analyses such risks and vulnerabilities with regards to the organisation's risk appetite. The second line of defence is also responsible for the training of professionals, business continuity planning, and for evaluating third-party relationships.

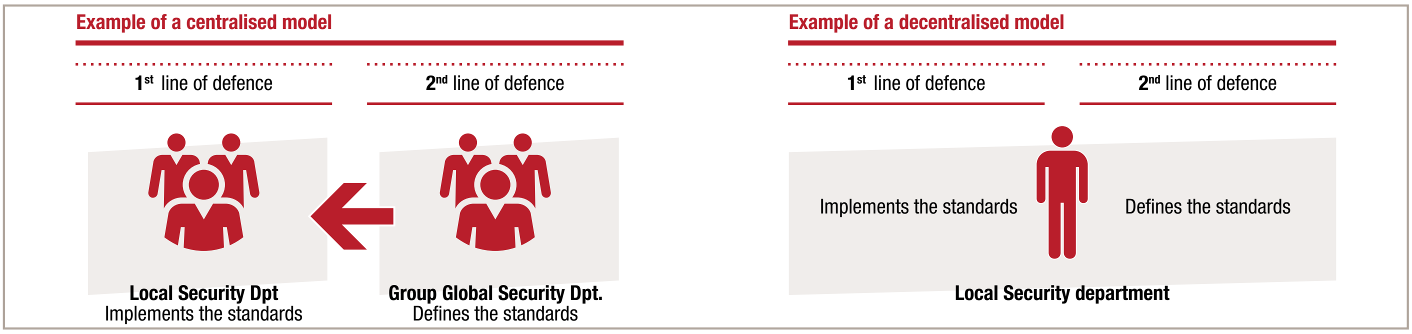
In addition, the second line of defence collects information coming from operational teams (KPI, self-evaluation, etc.) and regularly carries out control activities (evaluation, department review, etc.). It determines the level of risk thanks to key indicators and adjusts the means of control to be deployed by the first line of defence.

Generally, the second line of defence is comprised of a security and risk analysis governance department that is located at the company's headquarters. This approach favours the implementation of globally shared standards.

With regards to international companies, however, this role may also be carried out at the regional level. This choice is often explained by networking and territorial stakes requiring a specific local department or a governance strategy based upon organisational entities with a high degree of autonomy (regional BU, national department...). This approach favours taking into account local stakes but poses the risk of unequal development from one department to another.

Thus the frontier between the first and the second lines of defence is sometimes narrow: in the case of centralised governance, the separation between the first and the second line is strongly marked. On the other hand, decentralised governance very often implies that some second line of defence actors may be required to ensure the implementation of measures that they themselves defined (see the chart below).

Simplified illustration of the link between the first and the second lines of defence according to the chosen type of governance.



The third line of defence

The third line of defence develops and implements an audit program allowing executive management to ensure the organisation's capacity to master risks by controlling the implementation of standards on a regular basis. For this reason, it actively contributes to the continuous improvement of methods and procedures in order to improve the quality of the Security department's activities.

In order to guarantee its objectivity, the third line of defence is generally carried out by a department which is independent to the first and the second lines of defence and is only held accountable to executive management.

Therefore this line should ideally be represented by a department other than Security.

It appears that audit departments do not always have the skills to audit security departments and consequently leave the latter to carry out this work by themselves. However, this practice does not correspond to the philosophy of the three lines of defence model.

Less than 1/3 of surveyed companies have a third independent line of defence for security

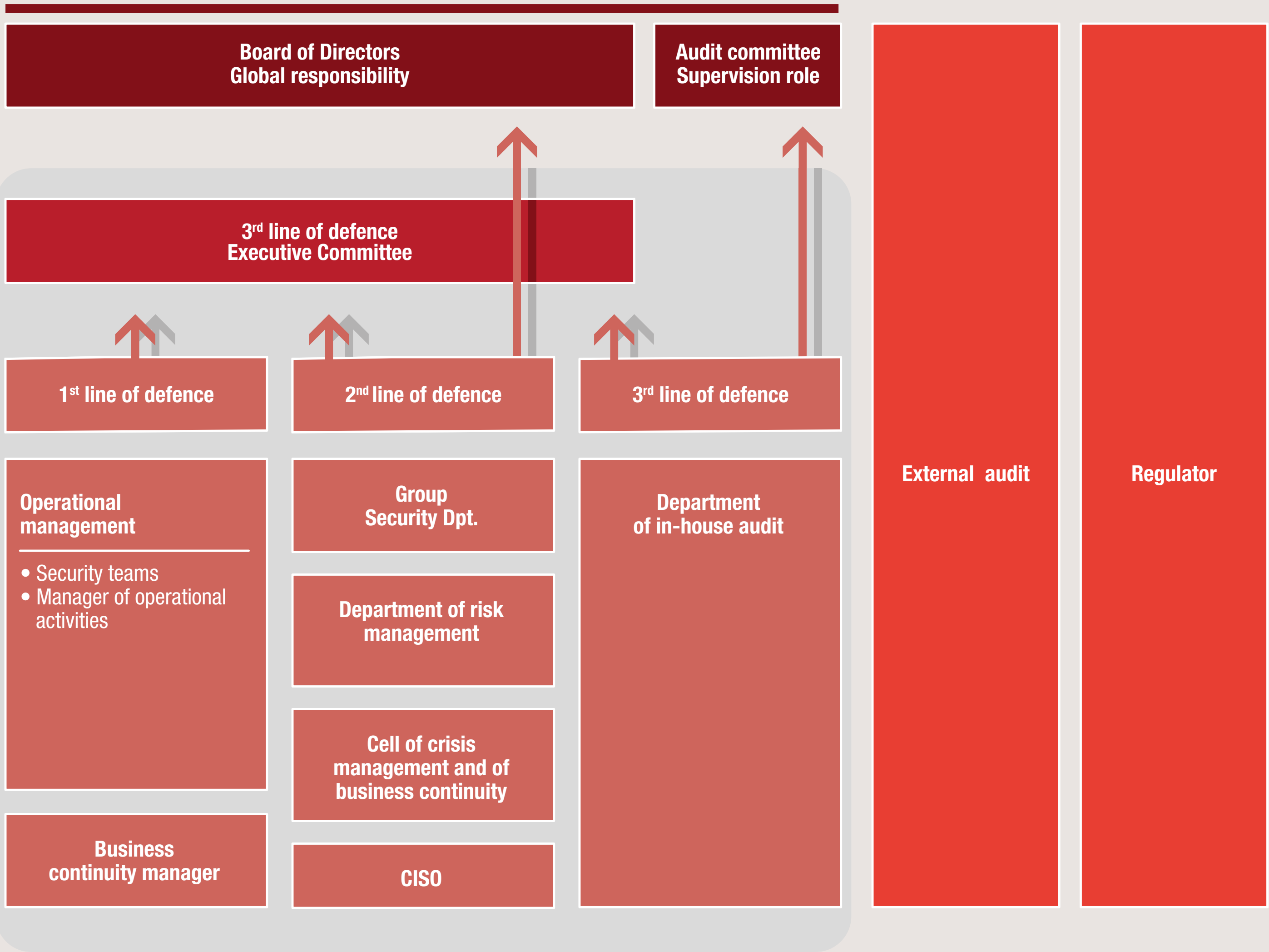
Companies following the above best practices in relation to the third line of defence generally entrust their in-house audit department or general inspection team with their auditing tasks. However, audits may also be conducted by external auditors. We recommend that the entity commissioning the audits be independent from the Security department and at a sufficient hierarchical level, in order to limit potential risks linked to a lack of independence.

The activities led by the third line of defence must not be mixed up with the diagnostics, the self-evaluations and other continuous improvement procedures implemented by the first and second lines of defence. Even though they are indispensable, these activities do not allow executive management to benefit from an independent look at the situation. Reviewing what has already been implemented via the three defence line model allows the company to detect inconsistencies (unnecessary duplication...) which may turn out to be very complicated to remedy given the potential obstacles (reluctance of some services which can consider that change will diminish their role within the organisation, etc.).

“We adopted a three-lines-of-defence approach two years ago. In spite of some difficulties encountered, I consider that this approach is a model to follow.”

Chief Security Officer of a pharmaceutical sector leader

Example of a model based on the three lines of defence



Board of Directors
Global responsibility

Audit committee
Supervision role

3rd line of defence
Executive Committee

1st line of defence

2nd line of defence

3rd line of defence

Operational management

- Security teams
- Manager of operational activities

Business continuity manager

Group Security Dpt.

Department of risk management

Cell of crisis management and of business continuity

CISO

Department of in-house audit

External audit

Regulator

The questions to ask yourself

- How do security teams at an operational level distinguish themselves from those at a strategic level?
- Do you have a security governance department within your organisation?
- How are local and regional security teams and headquarters' services interlinked?
- Is your Security department audited by the in-house audit department?
- Does the Security department show respect for general data and personal data protection rules?

Conclusion

The constant changes in the risk environment and the ever-growing demands in relation to security matters are compelling Security departments to evolve. In their search for the ideal organisational model, companies are centralising their security programs and structuring their Security department around areas of expertise staffed with multi-skilled experts. As their duties are no longer restricted to physical security issues, we have observed that Security departments may also intervene in relation to cybersecurity and crisis management matters, and that they are developing a close collaboration with technical teams.

In addition, Security departments are fully taking advantage of the digital revolution and Big Data by integrating new tools and means of monitoring and information analysis. This integration allows companies to better understand threats and their own vulnerabilities. In order to mitigate risks, they are also striving to develop a culture of security by training professionals in the best practices.

Finally, in order to optimise security management and to demonstrate good governance, some companies are opting to implement a model revolving around the three lines of defence.

We thank all of those whose contributions allowed us to carry out this study. Moreover, the interviews conducted with security departments show that today, large corporations are more inclined to share information about their organisation and the innovative practices they have put in place to manage security risks. This attitude reflects the desire of security departments to demonstrate that security issues are being taken into account at the highest corporate level and that adequate human and technical resources are being mobilised. This communication strategy allows companies to reassure their clients and investors about the organisation in place.

For further reading...

Today, the security of companies is more than ever a strategic matter. Facing a context where internal and external threats appear to be multiplying, Security departments must strengthen their systems with management tools. PwC offers a practical guide to implementing sustainable solutions.

To learn more, see pwc.fr/securite-surete

The indicators and dashboards in terms of security
Transforming security departments by harnessing data

Les indicateurs et tableaux de bord en matière de sûreté
Transformer la fonction sûreté avec l'exploitation des données

pwc

Contacts

Staff security, information systems security, information security... our approach covers your organisation's full spectrum of security concerns everywhere in the world.

Our experts will assist you with all of the security components necessary to help protect you and your business and to allow you to work calmly and efficiently.

Olivier Hassid

Security, Infrastructure Security and Corporate Intelligence Director

PwC France

olivier.hassid@pwc.com
01 56 57 75 16

Thierry Delville

Cyber Intelligence Partner

PwC France

thierry.delville@pwc.com
01 56 57 41 56

"Cyber Intelligence", the new platform launched by PwC to prevent, manage and anticipate the cybersecurity and security risks of companies

PwC has created a new "Cyber Intelligence" entity operationally headed by Philippe Trouchaud, expert in cybersecurity and Partner at PwC. Within the firm, the Cyber Intelligence entity now gathers more than 150 people in order to respond to strategic challenges and cybersecurity priorities and, more widely, to challenges and priorities concerning security, safety, corporate intelligence, crisis management and investigation.

The information contained in this present document has an exclusively general goal and must not be used in any way as a substitute for professional advice. In any event, in no case will the responsibility of PricewaterhouseCoopers Audit and/or of any of the member entities of the PwC network be engaged due to or following a decision taken on the basis of the information contained in the present document.

www.pwc.fr