Claudia Kestermann, Martin Langer & Arthur Hartmann


# Corporate Security at the **TOP100 Companies** Germany Austria Switzerland

## Legal Notice

This publication was jointly written and published by the University of Applied Sciences for Public Administration Bremen and the University of Applied Sciences FH Campus Wien. Authors responsible for its content: Prof. Dr. Claudia Kestermann (University of Applied Sciences for Public Administration Bremen), FH-Prof. DI Martin Langer (University of Applied Sciences FH Campus Wien), Prof. Dr. Arthur Hartmann (University of Applied Sciences for Public Administration Bremen). Editor: DI (FH) Mag. Thomas Goiser MA; Copy-editor: Mag.a Verena Brinda www.verenabrinda.at; Graphic Designer: Doris Grussmann (www.dggd.at).


Vienna, Bremen; November 2014

# Contents

# Foreword

FH Campus Wien

Prof.in Dr.in Luise Greuel
Rector, University of Applied Sciences for Public Administration Bremen

ao. Univ.-Prof. Mag. Dr. Arthur Mettinger
Rector, University of Applied Sciences FH Campus Wien

## Pioneers Offer Orientation

Security is a basic need, and it affects us all. Today most people take it for granted. On the one hand, that is the result of the fortunate situation in which we, in our community at the heart of Europe, have found ourselves for the last several decades: the rule of law, functioning institutions, social and political peace, as well as (for the most part) shared values. That hasn‘t always been the case here, and it is hardly the case everywhere. On the other hand, high security standards and a high subjective feeling of security are also the result of the daily commitment of public authorities, courageous individuals, civil society and business.

Companies—especially internationally competitive ones—know that they possess valuable resources and protect them accordingly: ideas and information, processes and methods, patents and rights, raw materials, buildings and machines, and last but not least, employees. The threats and challenges are numerous, highly diverse, and are constantly evolving.

The security of the TOP 100 companies in Germany, Austria and Switzerland, and the accompanying implementation and organisation of corporate security, as well as the role of those responsible for it is, in this regard, an especially important research topic, as security is part of those companies‘ economic success. At the same time, those responsible for the security of large companies are pioneers and pacesetters for new developments; they set an example for other businesses through their innovation as well as through their organisational and security issues.

The work of the chief security officers at those companies is thus of particular importance. We are pleased that at both of our universities this topic was taken up as a research project, and it reinforces our stance of attributing particular importance to research on security and of paying particular scholarly attention to the work of CSOs in German-speaking countries.

The issue of corporate security will increase in relevance. Therefore, we hope for all of those involved that this study and the publication below from our universities contributes to a gain in insight and to a more in-depth discussion of the current questions that surround it.

Luise Greuel, Arthur Mettinger

# Vorwort und Danksagung

Prof.in Dr.in Claudia Kestermann
University of Applied Sciences for Public Administration Bremen

FH-Prof. Martin Langer
University of Applied Sciences FH Campus Wien

Prof. Dr. Arthur Hartmann
University of Applied Sciences for Public Administration Bremen

## At the Cutting Edge

Both of our universities connect science, security and business. This is the only way to success—precisely in the area of risk and security management—due to things becoming increasingly connected and complex. This interdisciplinary approach is demonstrated in the curricula of our programs of study, in our various collaborations in teaching and research, and last but not least in our research topics. At our schools it has been and still is our goal to offer as many practice-oriented degree programs as possible, so that the engagement of our graduates, with their knowledge and skills, will benefit companies. In order to meet this goal and continue developing our course content, it is important to know which skills are necessary today and which will be needed for the future.

In this study, which is of particular importance to all of us and our universities, we address security issues from various perspectives. The Institute for Police and Security Research (IPOS), for example, is located at the Hochschule für Öffentliche Verwaltung Bremen. In the project presented here, for the first time, we have joined our resources and are growing the partnership that began with the founding by our institutes of the Cooperation Network for Risk, Safety and Security Studies (CONRIS).

On the following pages we present the project Corporate Security TOP 100 and its results in more detail. For this study, we did not just pursue our own research interests, but also met requests from the business community. We were in turn supported by companies with their participation in our survey. To all of the participants, the chief security officers of the largest German, Austrian and Swiss companies, a hearty thanks!

We were able to convince pivotal people and organisations that represent, in particular, security in the participating countries of our research project, notably:

- Jörg Ziercke, President, German Federal Criminal Police Office
- General Franz Lang, Director, Austrian Criminal Intelligence Service, Austrian Ministry of the Interior
- Dr. Jean-Luc Vez, Director, Federal Office of Police (Switzerland) until August of this year.

We would also like to offer our hearty thanks on this occasion for the trust shown and for the support received. With the results of this research project, our goal was to offer those involved and anyone interested in the topic current insights as well as an impetus for thought and discussion for their field of activity.

We hope we were successful at this and look forward to your feedback.

Claudia Kestermann, Martin Langer, Arthur Hartmann

# 1. Introduction


In the winter of 2013/2014 a survey of important businesses in Germany, Austria and Switzerland (the D-A-CH Region) was carried out by the University of Applied Sciences for Public Administration Bremen and the University of Applied Sciences FH Campus Wien regarding security aspects. The goal of the study Corporate Security CSO TOP 100 was to gain information on the establishment and structure of security, on the security culture at leading businesses all across Germany, Austria and Switzerland, as well as on the impact of crime.

The study is intended to offer insights into the organisation of security in the D-A-CH Region and to facilitate an in-depth analysis of different integrative factors whose results can in turn be of use.

The results presented here represent select parts of the overall study. In the following sections, general topics are first descriptively presented and examined in relation to central factors. Differentiated analyses of specific questions are to be examined in more detail and published elsewhere.

# 2. Research Methods

## 2.1 Content and Operationsalisation of Research Questions

The questionnaire is divided into three main sections, to be described below: Organisational and Security Structure, Company and Security Culture, Crime Rates, as well as Task Areas and Partnerships.

### Organisation and Security Structure

In investigating structural aspects, of particular interest were the leading positions in security departments (or those responsible for security), especially their connection to the board of directors, their realm of responsibility, their potential authority to act and their strategic potential to influence the repair of structural aspects relating to organisation and security at companies.

### Company and Security Culture

Various attitudes, behaviours and measures fall into this section. The following table offers an overview of these individual aspects.

Questions on the topic of company culture were addressed using, among others, a standardised instrument, Jöns, Hodapp and Weiss's short scale for the assessment of company culture (2006). The scale covers aspects of company strategy, company culture, leadership behaviour and cooperation.[1]

***Table 1: Aspects of security culture***

- Aspects of company culture which affect security
- Behavioural guidelines, codes of conduct, evaluation of effects and quality control
- Whistleblowing systems, how whistleblowing is handled
- Measures for awareness, sensitivisation to security issues
- How mistakes are handled at companies

In this section, besides the involvement of staff in the development of behavioural guidelines, particularly the way in which employees are informed thereof, and the implementation of those guidelines, as well as the monitoring of their effects are also explored. Questions on access to and presentation of codes of conduct, as well as the obligation to adhere to behavioural guidelines were carried out based on Erwin's findings (2011).

Next, the topics of whistleblowing, the implementation of a whistleblowing system, and the assessment thereof by those surveyed were examined. Lastly, this section examines measures aimed at sensitivisation to security issues and their relevance in increasing security awareness within organisations. This section ends with questions about company culture when it comes to mistakes, and the management of mistakes at companies.[2]

1 From a methodological point of view, here the interpretation of individual aspects of company and security culture is limited, as the target group surveyed consists of individuals belonging to companies, and thus only their individual perspectives were surveyed. For general statements on company and security culture, a survey of a larger sample of employees and management at the individual companies would be necessary.

2 according to Hudson (2007), Fahlbruch, Schöbel & Domeinski (2008); Weick & Sutcliffe (2003), Buerschaper (2008).

**Crime Rates**

In the third section, businesses were surveyed on their experiences as victims of various crimes. In addition to prevalence (instances within the last twenty-four months), the extent of damage was also surveyed. Additionally, the amount of time spent on preventive and reactive crime-fighting measures were examined. On top of that, of interest was to what extent businesses systematically record issues that emerge, and if so, the extent of information gathered, and how and how often reporting and analysis of insights gleaned from that information are carried out.

In addition to those questions on experience with cooperation, questions as to the assessment of future challenges and of personal satisfaction with working conditions concluded the survey.

***Table 2: Crime rates***

- Types of crimes: property crimes, corporate crimes, other white-collar crimes, blackmail and sabotage
- Preventive and reactive measures
- Reporting of instances that emerge, reporting systems

## 2.2 Conducting the Survey, and Comments on Sampling

In the participating countries, Germany, Austria and Switzerland, various numbers of companies were selected depending on their size and density. The basis for inclusion of companies was their published sales figures. Moreover, the largest insurance companies and banks were addressed separately. In Germany, a total of N=180 questionnaires were sent by mail, in Austria, N=99, and in Switzerland, N=62. Participation was possible either by filling out a paper questionnaire or the online version.

A total of N=72 questionnaires were sent back, correlating to a rate of 21.1%. After subtracting questionnaires that were insufficiently completed and thus not taken into account, a net sample of N=54 questionnaires (response rate: 15.8%) remained. Given not only the distinctiveness of the sampling but also, especially, the survey's subject matter, this level of participation is to be considered highly acceptable.

The N=54 participants are distributed over the countries involved as follows: N=32 participants are from German companies, N=13 are from Austrian ones and N=9 are from Swiss companies. In light of the small size of the sampling, the results (especially those based on country) are primarily of a heuristic nature. For this reason, in terms of good practice, the findings are to be used as examples and correlations are to be identified which act as guides for practical experience as well as for further research.

The participating companies, banks and/or insurance companies are in large part transnationally-active firms which are represented, on average, in forty-two countries (median: thirty countries). Almost two-thirds of them (64.5%) are active on at least four continents.

# 3. Primary Results

In the following section, primary select results are presented; the focus here lies on a descriptive account. In addition to information on the frequency of occurrence, bivariate correlations or group differences are examined.

## 3.1 Organisation of Security, and Satisfaction of Those Responsible for it

### Separate Corporate Security Departments: Germany far ahead of Austria and Switzerland

Nearly three out of four (74%) participating companies have a corporate security department. Of the German companies surveyed, the percentage thereof with their own corporate security department (87.5%) is much higher than that of Swiss (66.7%) and Austrian companies (46.2%).

56% of participants agree that the topic of security is a function explicitly allocated to the board. While this is indicated by half of the participants in Germany and Switzerland (DE 48.3%, CH 50%), the percentage in Austria is over three-quarters (AT 76.9%).

This is also demonstrated by the location within the company's hierarchy of the head of the corporate security department or the person in charge of security (see Fig. 1).

In Austria, three quarters of security management jobs are located, in terms of organisation, at the top two levels; in both Germany and Switzerland, around 44% are located within the top two levels.

### The Greater the Authority, the Higher the Satisfaction

The hierarchical level which the corporate security department has correlates significantly positively with the level of satisfaction with one's own position. [3]

### Conditions and Resources: Very Different Ratings

Some specific questions dealt with the satisfaction of those responsible for security along with conditions at companies, their positions, and the resources at their disposal (see Fig. 2).

Satisfaction with one's own position is relatively high (87.5%: "strongly agree"/"somewhat agree"). Almost as marked is a positive assessment of the board's support (83.4%: "strongly agree"/"somewhat agree") and a functional link to the board (73%: "strongly agree"/"somewhat agree"). Nevertheless, a not insignificant percentage of those surveyed is dissatisfied with the current situation.

A large portion of those surveyed is at least relatively satisfied with their responsibility for the budget (90.7% having a budget available to them). In regards to the amount of budget available to them, a relatively high level of satisfaction can be assumed—only around one in five (20.9%) indicates being "rather dissatisfied" or "very dissatisfied". At 41.7%, dissatisfaction with personnel situations is, in contrast, substantially higher.

3 Spearman rho=.505, p<.01

***Figure 1: Management level of corporate security department or of person in charge of security***

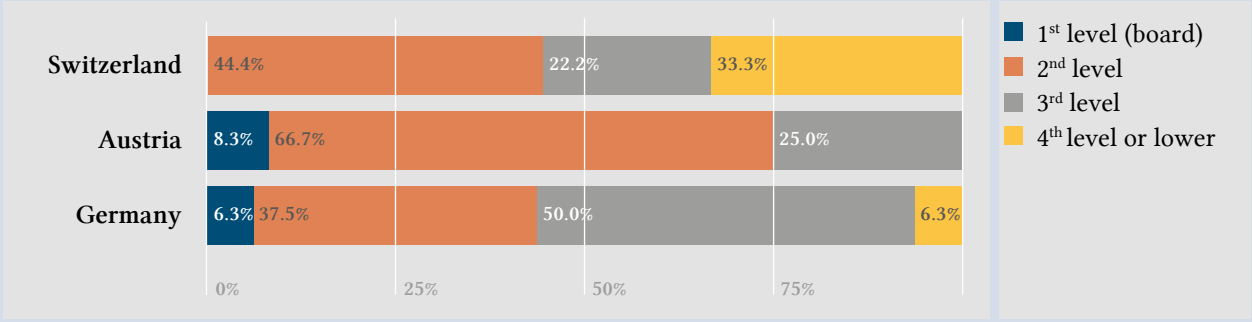
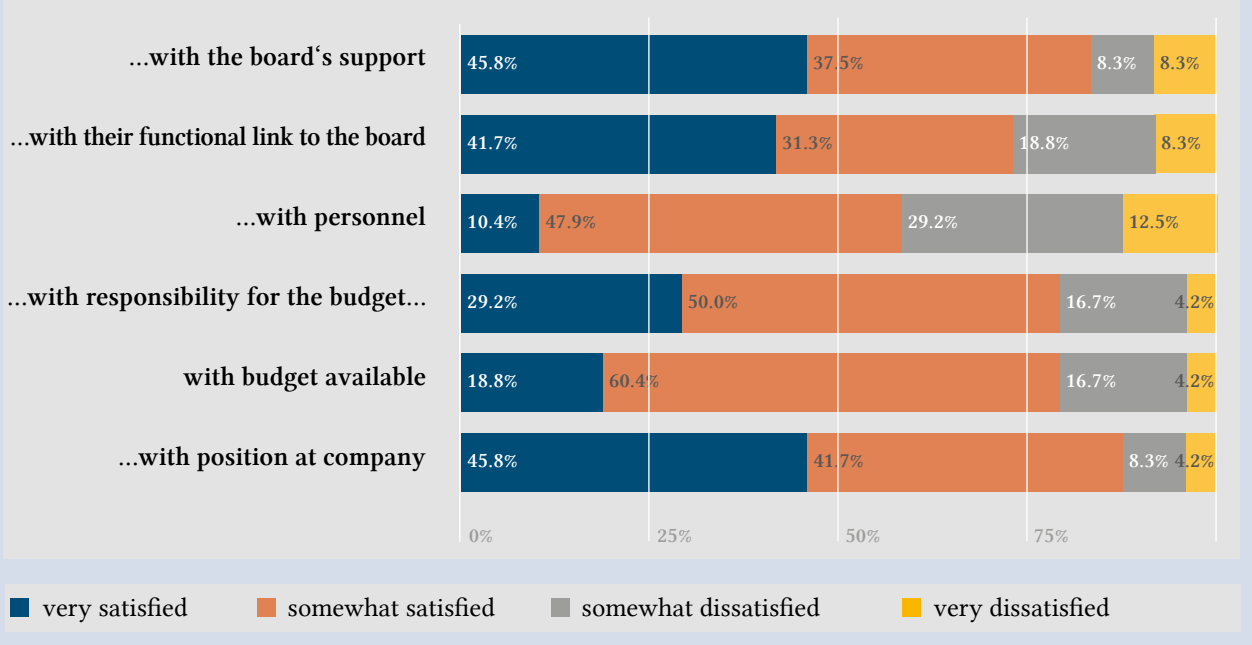



***Figure 2: Satisfaction of those surveyed***



## Satisfaction Ranking: Switzerland behind Austria and Germany

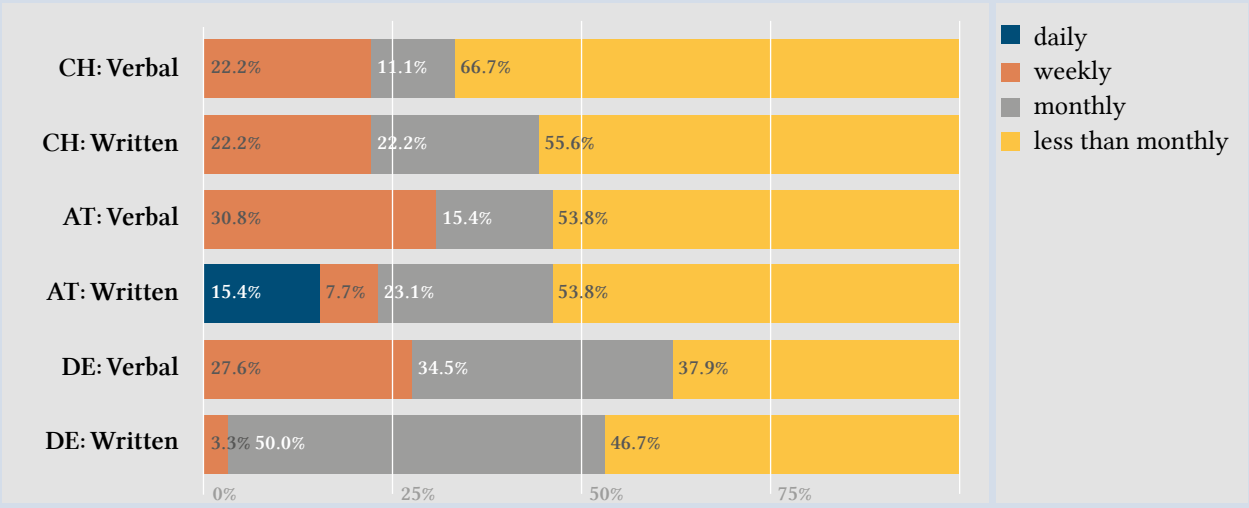
With a mean value of 2.5 in an average ranking of aspects of satisfaction (scale: 1= "very satisfied" to 4= "very dissatisfied"), the Swiss surveyed are considerably less satisfied with the current situation than the Germans (M=1.9) and the Austrians surveyed (M=1.8).

## Correlation Between Involvement and Satisfaction

To what extent satisfaction with the aforementioned structural aspects is correlated to frequency of verbal or written contact to the board is examined in the following section. To begin with, frequency of and opportunities for contact at the companies (according to country) are presented.

Whereas in Germany the board is reported to much less frequently in writing than in other countries, verbal reports are much more frequent there. Furthermore, 80.6% of Germans surveyed indicated being able to contact the board as needed. 69.2% of those surveyed from Austria indicate having such an additional avenue of communication, while of those from Switzerland, only 44.4% do. The frequency of written reporting has no correlation to aspects of satisfaction, as does more frequent verbal (and thus personal) contact: this correlates significantly to satisfaction with one's own position as well as satisfaction with the amount of budget available.[4]

***Figure 3: Frequency of reporting to the board***



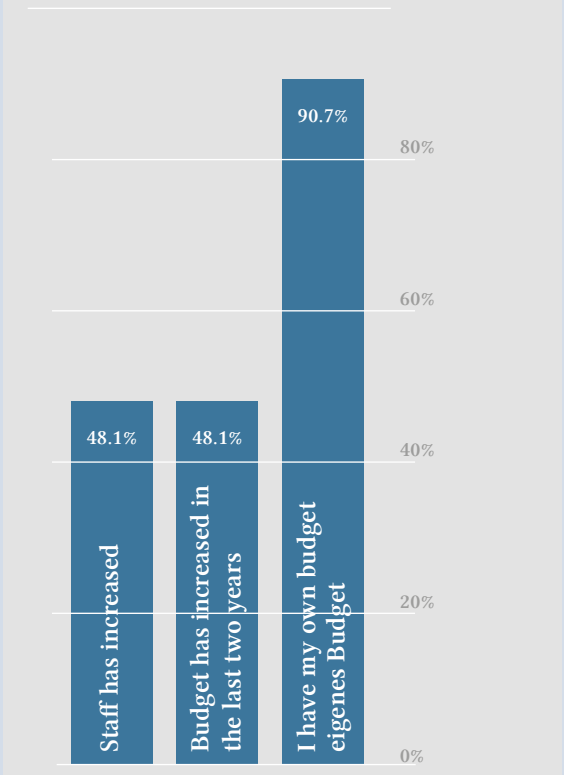

4 Spearman rho=.472, p<.001; Spearman rho=.307, p<.05

## 3.2 Financial and Human Resources

In regards to budget responsibility, there are slight differences among those surveyed from the three countries: the percentage of participants from Germany who have their own budget is the highest, at 96.9%, whereas in Austria 84.6% indicate such, and in Switzerland, 77.8%. Those with their own budgets demonstrate significantly more positive values in regards to all of the aspects of satisfaction surveyed than those who have no budget responsibilities. This is valid regardless of actual financial or human resources. An increase in budget or staff is reported by around 50% of Germans and Austrians surveyed, whereas this is affirmed by only 35% of Swiss participants.

When those who were able to report a budget increase in the last two years are compared with those whose budgets did not increase, there is an effect, in regards to aspects of satisfaction surveyed, on their perception of the board: in the latter group, satisfaction with their functional link to the board as well as with support from the board is significantly lower.[5] In addition, in regards to personnel changes, a correlation to perceived support from the board is evident; frequency of contact with the board is exceedingly significant here. [6]

***Figure 4: Financial and human resources***




5 T=-2.318; p<.05; T=-2.108; p<.05
6 T=-2.429; p<.05; T=-2.895; p<.01

***Table 3: Budget and personnel increases in connection with aspects of satisfaction***

| | **Budget has increased in the last two years** | **Mean value** |
|---|---|---|
| Satisfaction with functional link to board | Budget has increased<br>Budget has not increased | 1.55<br>2.15 |
| Satisfaction with support of boarda | Budget has increased<br>Budget has not increased | 1.45<br>1.96 |
| | **Staff has increased in the last two years** | **Mean value** |
| Satisfaction with support of board | Staff has increased<br>Staff has not increased | 1.43<br>2.04 |
| Frequency with which board is verbally addressed | Staff has increased<br>Staff has not increased | 2.83<br>3.48 |

Skalen: Zufriedenheit – 1=„sehr zufrieden“ bis 4=„sehr unzufrieden“;
Häufigkeit - 1=„täglich“ bis 4=„seltener als monatlich“

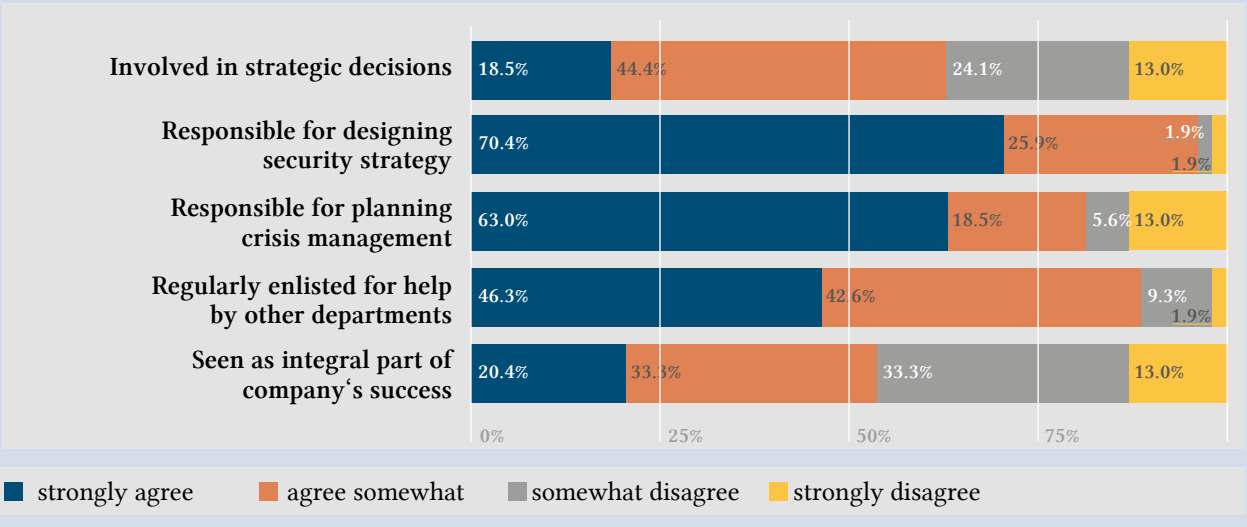
## 3.3 Strategic Decision-Making at Companies

To what extent those surveyed are involved in strategic decisions or trusted with related tasks and/or vested with related competences is shown in Figure 5.

### “Yes” to Responsibility and Involvement, but More Likely “No” to Sharing in Success?

63% of those surveyed are at least partly involved in decisions of strategic importance for the company (options: “strongly agree” and “agree somewhat”). In regards to design of security strategy, the percentage rises to 96.3%.

***Figure 5: Importance and strategic involvement***
*of corporate security department and/or those responsible for security*



81.5% see themselves as (jointly) responsible for designing and planning a crisis management concept; a somewhat higher percentage, at 88.9%, is enlisted for help or consulted by other departments of the company, illustrating their significance to the company.

If one looks, however, at assessment of whether the corporate security department or those responsible for security and their work is seen as an integral part of the company's success, this is considerably less positive. While 53.7% believe with some reservations that this perception prevails, a not insignificant percentage of the participants takes a more or less markedly pessimistic standpoint. Evident here is the oft-cited discrepancy between, on the one hand, the importance of one's own work and the issue of security, and on the other hand, others' evaluation of security and/or security's image at the company.[7]

## Competences: Governance Function in Normal Cases and Crisis Management Unit in Special Cases

More than three quarters (75.9%) of those responsible for security are authorised to issue directives to other departments in certain situations. In Germany and Austria, the percentage is somewhat higher; in Switzerland, in contrast, only two-thirds of those surveyed are endowed with such powers.

Besides fundamental competences and capacities for security matters, security management possesses a certain amount of authority in various areas and situations. The most frequently named aspects are listed by example in the following table.

***Table 4: Conditions for authority to issue directives***

**Fundamental capacities**

- "Corporate security has a governance function in many tasks."
- "CSO has the authority to give directives regarding all security matters regulated by law."
- "Policies, standards and guidelines on all matters relating to security."
- Functional responsibility, setting guidelines and functional authority

**Specific capacities**

- Emergency and crisis situations, evacuations (incident and crisis management)
- Travel safety
- Investigations, incident reporting
- Data protection
- Event and personnel protection
- Asset protection, fire safety, hazardous materials
- Environmental protection
- Violations of safety regulations

Among the individual countries, there is a considerable difference regarding the question of the corporate security department or the person responsible for security's potentially leading a crisis management team: only around every second person surveyed from Austria and Switzerland (55% and 55.6%, respectively) indicated that they lead crisis teams in certain situations or events; in Germany, in contrast, four out of five (78.1%) do.

7 Differences among the countries are statistically irrelevant: mean values: DE 2.4; AT 2.2; CH 2.8 (scale: 1 = "strongly agree" to 4 = "strongly disagree")

## 3.4 Functional Responsibilities

As expected, the areas of responsibility of participating companies' security departments and of those in charge of security vary widely, their particular areas of responsibility depending on human resources, company structure and the industry they are involved in.

Form of organisation, its accompanying complexity and distinctions in areas of responsibility are to be taken into account here. Thus, before too large a significance to any differences among the countries involved, it is more important to compare companies with corporate security departments with those who have organised security differently. To begin with, below there is an overview of those fields that—as a function of security organisation—most or least frequently fall within the areas of responsibility of those surveyed.

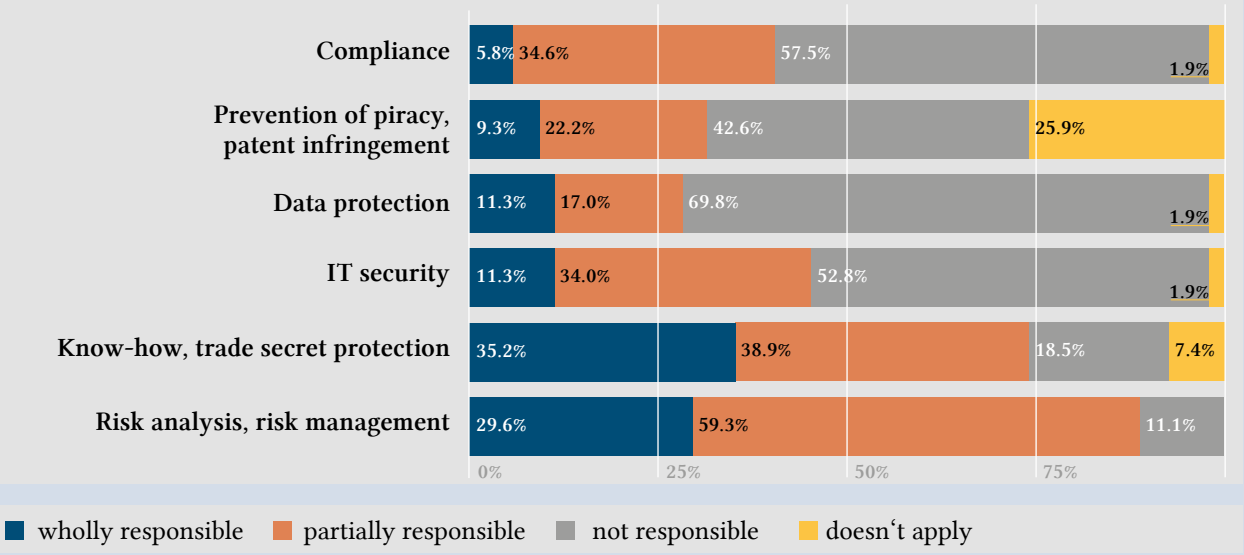
Data on the individual areas of responsibility (predefined by the questionnaire) are first presented in the figures on the overall sampling (across all forms of organisation and countries). Afterwards, the areas which demonstrated

***Table 5: Areas of responsibility according to organisation of security***

| **Corporate security department (n=40) within company** | **Companies with a different organisation of security (n=14)** |
|---|---|
| **High level of responsibility**<br>(sum of "wholly responsible" and "partially responsible" ≥ 80%) | **High level of responsibility**<br>(sum of "wholly responsible" and "partially responsible" ≥ 60%) |
| 1. Company-wide security strategy (100%)<br>2. Emergency and crisis management (100%)*<br>3. Internal investigations (95%)**<br>4. Risk analysis, risk management (92.5%)<br>5. Plant safety and security (92.5%)<br>6. Event security (92.5%)<br>7. Travel safety (90%)<br>8. Know-how protection, trade secret protection (87.5%)**<br>9. Prevention of property and economic crimes (87.5%)*<br>10. Executive protection (87.5%)**<br>11. Workplace safety (workplace violence) (82.5%)<br>12. Business continuity management (80%) | 1. Company-wide security strategy (100%)<br>2. Emergency and crisis management (85.7%)*<br>3. Plant safety and security (85.7%)<br>4. Occupational health and safety, fire safety (78.6%)<br>5. Risk analysis, risk management (78.6%)<br>6. Event security (71.4%)<br>7. Travel safety (71.4%)<br>8. Workplace safety (workplace violence) (71.4%)<br>9. Internal investigations (69.2%)** |
| **Low level of responsibility**<br>(sum of "wholly responsible" and "partially responsible" ≤50%) | **Low level of responsibility**<br>(sum of "wholly responsible" and "partially responsible" ≤50%) |
| 1. Data protection (25%)<br>2. Prevention of piracy, patent infringement (35%)<br>3. Compliance (37.5%)<br>4. IT security (46.2%)<br>5. Occupational health and safety, fire safety (50%) | 1. Prevention of piracy, patent infringement (21.4%)<br>2. Know-how protection, trade secret protection (35.7%)**<br>3. Data protection (38.5%)<br>4. IT security (42.8%)<br>5. Compliance (50%) |

Statistically significant differences are identified as follows: * p<.05, ** p<.01

*Figure 6: Areas of responsibility and competences*




considerable differences according to country are examined more closely.

## In Part, Considerable Differences Among Countries

When focus is placed on the individual countries, a more nuanced picture emerges—especially when one looks at the areas outside of those employees' realm of responsibility for or the (presumed) lack of relevance of certain topics.

### Information Security

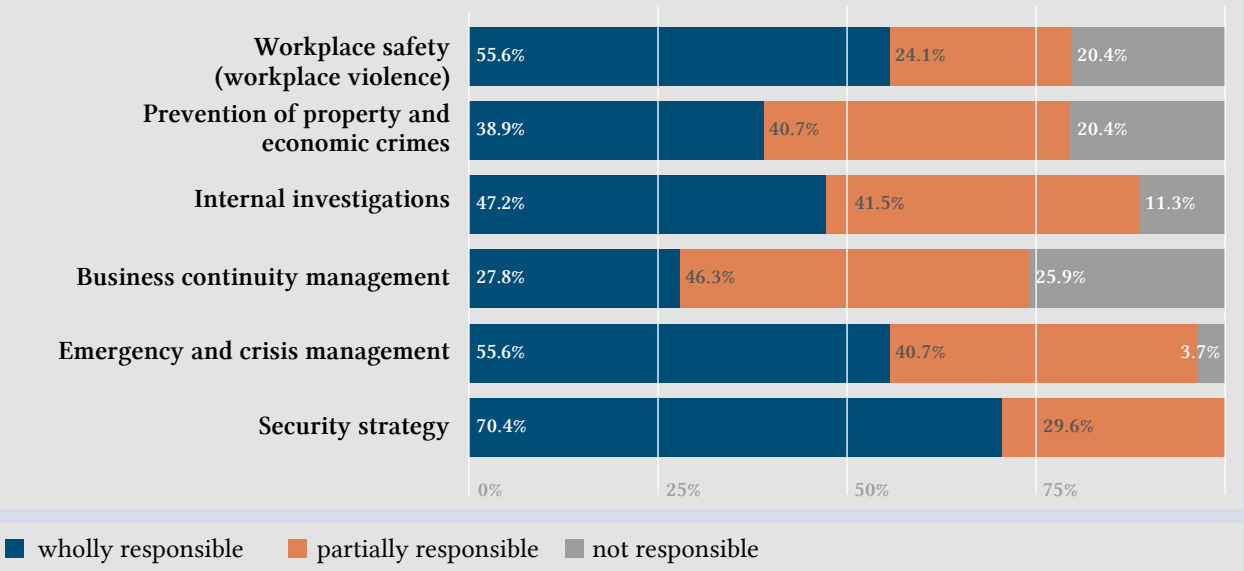
For example, 15.4% of Austrians surveyed indicate that protection of know-how and trade secrets is not relevant in their countries (DE 3.1%, CH 11.1%). The matter is thus rated as less important in Austria than in most companies of their neighbours. 30.8% assert that they are not in charge of this area of responsibility (DE 15.6%, CH 11.1%).[8] Whereas in Germany and Switzerland, all of the corporate security departments are responsible for these matters, in Austria that is not the case.

Another interesting area is data protection: whereas 87.5% of those surveyed from German companies describe themselves as not responsible for it, at 58.3%, a much lower percentage of Austria's participants describe themselves as thus. On the other hand, two-thirds of those surveyed in Switzerland are at least partially responsible for data protection (DE 12.5%, AT 41.7%). This area appears not to play a pivotal role in security for a multitude of companies.

In contrast, two out of three participants from Switzerland (66.7%) are not responsible for IT security. The percentage at Austrian companies is 58.3%, and from Germany, 46.9%. At more than half of German companies—and thus to a greater extent than in Austria and Switzerland—there is (at least in part) a functional competence for this matter.

8 It is to be noted here, however, in critique of the methods used, that not to be ruled out is the possibility that the lumping-together of protection of know-how and trade secrets might have led to confusion.

*Figure 7: Areas of responsibility and competences*




### Business Security: Differences According to Country

Upon observation of risk analysis and risk management, the results from Austria are surprising: a total of 61.6% see themselves as responsible (15.4% "wholly responsible; 46.2% "partially responsible"); in Germany and Switzerland, almost all of the respondents see themselves as such ("wholly responsible": DE 37.5%, CH 22.2%; "partially responsible" DE 59.4%, CH 77.8%).

A similar picture emerges from an analysis by country of perception of responsibility for prevention of property and economic crimes. In the German and Swiss companies surveyed, the percentage of those responsible for this area ("wholly responsible"; "partially responsible"), at, respectively, 84.4% and 88.9% (with 44% each responding "wholly responsible"), is relatively high, whereas in companies from Austria, only 61.5% describe themselves as responsible for it (with only 23.1% being "wholly responsible").

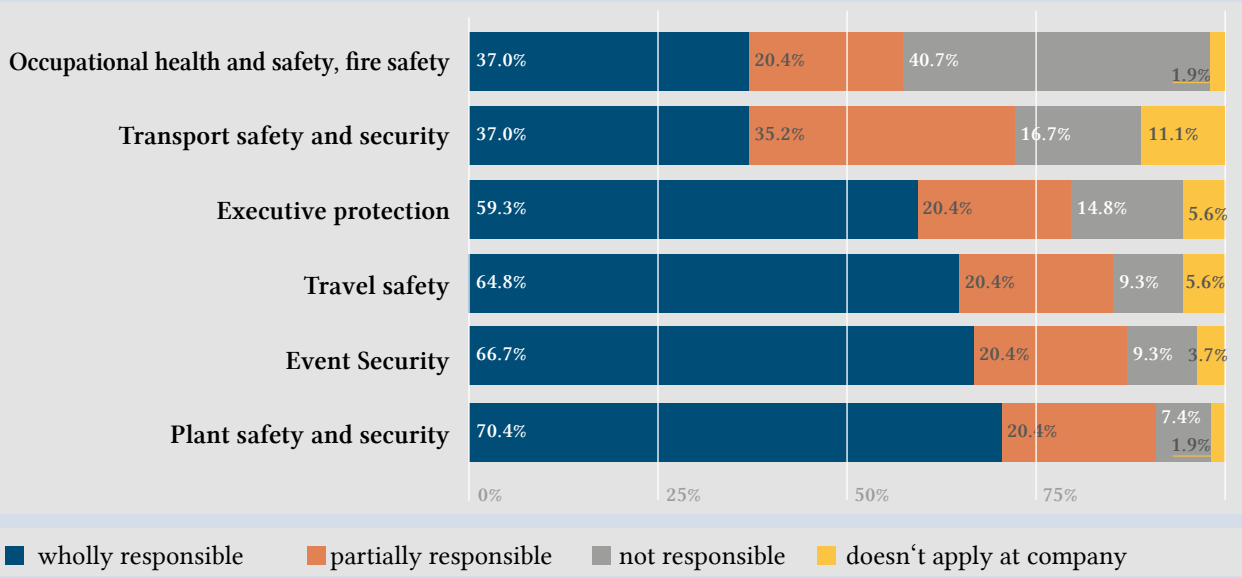
### Physical Security: Differences According to Country

Various fields of responsibility are included in this category; answers provide few clear differences according to country (rather according to companies' security structure, see above).

In the following areas, however, the pattern of responsibility described above repeats, with a low percentage of respondents from Austrian firms responsible (sums of "wholly responsible" and "partially responsible" responses are shown): event security (AT 61.5%, DE 93.8%, CH 100%), travel safety (AT 46.2%, DE 96.9%, CH 100%), executive protection (AT 46.2%, DE 90.6%, CH 88.9%).

A different picture presents itself, however, in regards to the areas of workplace safety (workplace violence) as well as to occupational health and safety and to fire safety. Whereas occupational health and safety, and fire safety fall within the realm of responsibility of those responsible

***Figure 8: Areas of responsibility and competences***




for security in Austrian and Swiss companies (CH 88.9%, AT 84.6%), only 37.5% of German respondents indicate responsibility for them. 92.3% of Austrian respondents and 100% of Swiss respondents are responsible for workplace security. For two-thirds of those responsible for security in Germany, it falls within their realm of responsibility. Especially in German countries with corporate security departments, that area of responsibility lies with other staff (with the fire protection officer or the occupational health and safety officer, for example).

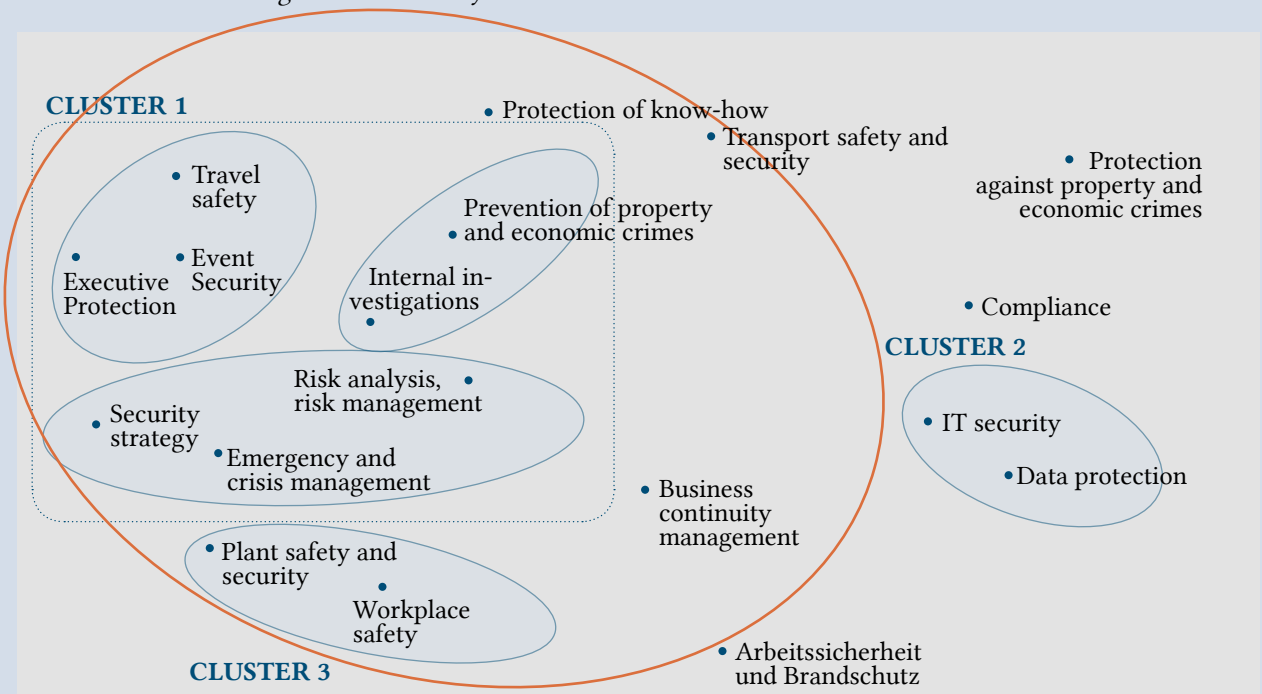
## A Function Dominated by Three Clusters of Responsibility

The connections among individual areas of responsibility will be examined below.

To these ends, using a multidimensional scale based on respondents‘ answers, the relative position of areas of responsibility are analysed in a multidimensional space in order to uncover any particular similarities and/or dissimilarities through the resulting configuration. Through a similarly-executed cluster analysis, homogenous groups of items can also be identified.

The areas of responsibility in Cluster 1 fall most frequently within the respondents‘ realms of responsibility, and thus represent, in practice, the core areas of those responsible for security at large companies.

***Figure 9: Areas of responsibility and competences***
*Multidimensional scaling and cluster analysis*




The further to the left an item is located, the more often (and more completely) those matters tend to fall within respondents‘ realms of responsibility. The percentage of respondents who indicated that items do not apply at their companies is somewhat higher for those topics located at the top edge of the figure than for others. The closer that topics are to one another, the more frequently was responsibility for them similarly rated. Items in a cluster appear together frequently (or, in contrast, are similarly absent). If a person indicated being responsible for an item in a cluster, in many cases, they were also responsible for the other topics located in that cluster. If they weren‘t responsible for something, then the other topics in that cluster seldom fell within their area of responsibility.

The commonality of the items in Cluster 2 (IT security and data protection) particularly lies—besides in their content and/or the importance of IT for data protection—in the relative rarity of responsibility for them by CSO's. The particularly close proximity of the items in Cluster 3, responsibility for plant safety and security, and workplace safety (prevention of workplace violence), may be due to the fact that responsibility in the production industry for prevention of workplace violence is vital and also falls within the scope of duties there.

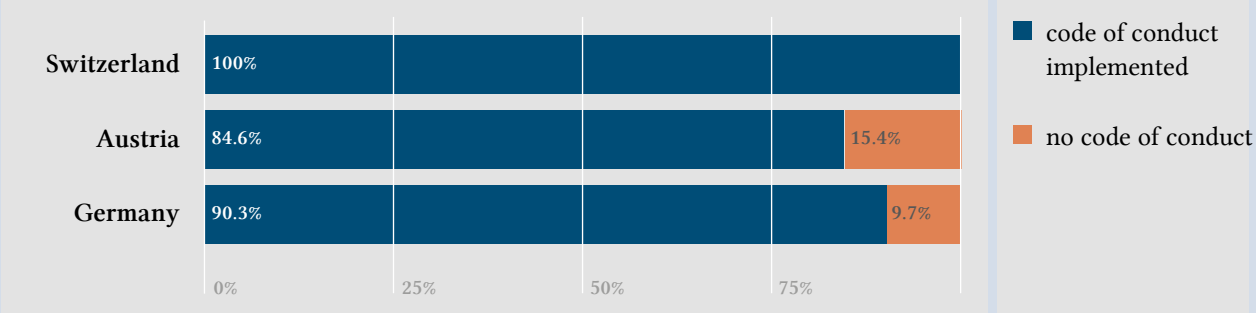
For the subgroup of companies with corporate security departments, the primary realm of responsibilities includes, besides Clusters 1 and 3, the items know-how protection and business continuity management, as well as, when applicable, transport safety and security, and/or supply chain security.

## 3.5 Codes of Conduct, Policies and Whistleblower Systems

A further focus of this study is enquiry into the status of the implementation of codes of conduct at companies. Below, codes of conduct[9] will be discussed; in doing so, however, only individual aspects of overriding importance from this area will be included. How companies deal with whistleblowing and systems for whistleblowing were at the heart of this enquiry.

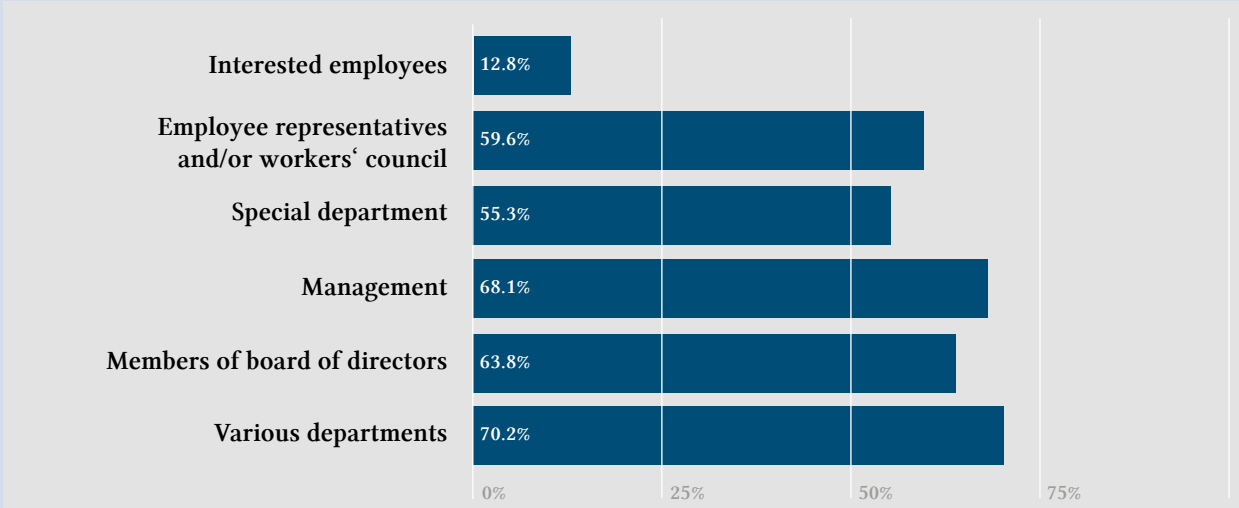
A total of 90.6% of those surveyed indicate that a code of conduct offering employees orientation does exist at their company. In Switzerland, all of the respondents said that a code of conduct has been implemented at their company; in Germany, 90.3%; and in Austria, the number is the lowest, at 84.6%.

***Figure 10: Code of conduct***




9 In many cases, this is used as a tool for measurement of company ethics (Kaptein & Schwarz 2008), as an integral element of compliance systems (Wecker & van Laak 2009), or even called a company "constitution" (Hoffmann 2008).

***Figure 11: People involved in the development of codes of conduct***




Who was consulted in the development and drafting of codes of conduct? Were various departments and groups involved? Data here corresponds to companies that do have a code of conduct. In some cases (3.4%), codes of conduct were not developed within respondents‘ own companies. In those cases, the companies are only from Germany. In Figure 11, involvement in the writing of a code of conduct is depicted, whereby multiple responses were allowed. To begin with, it is clear that ultimately a multitude of people from companies were involved in the development of their codes of conduct.

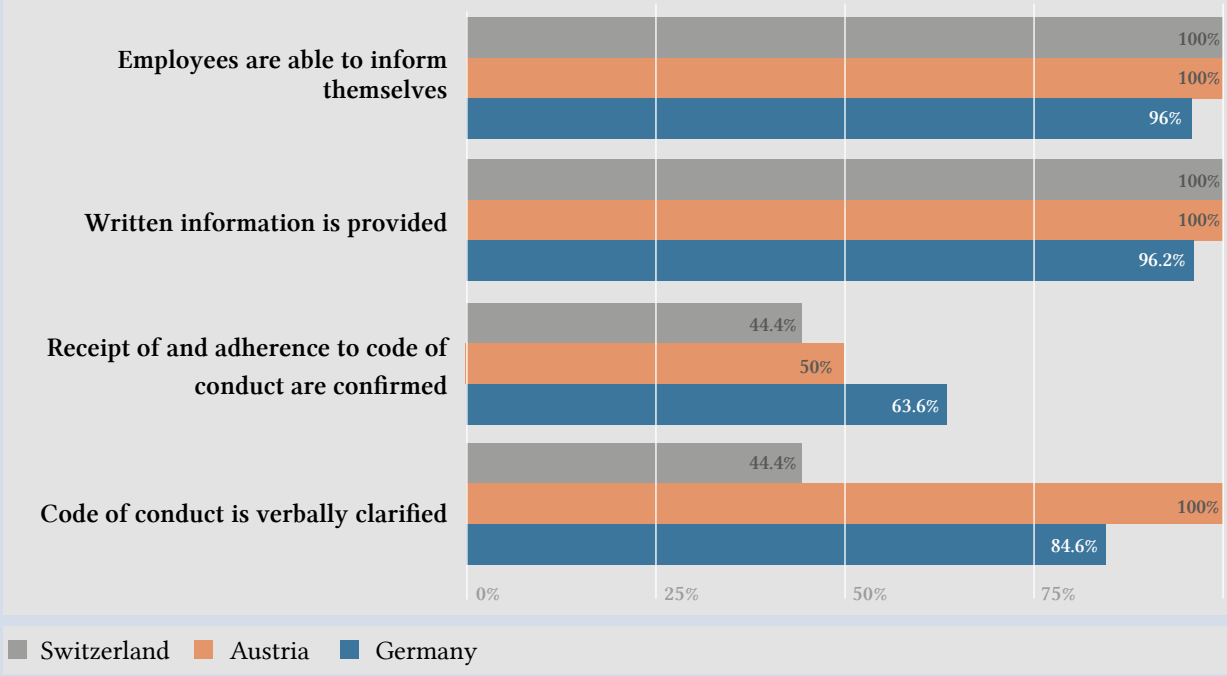
Initially, the high percentage of board involvement stands out. In both Germany and Switzerland, two-thirds of respondents indicated its collaboration, and in Austria, still 54.5%. Involvement of the management at Swiss companies is noticeably higher at 77.8% (DE 66.7%, AT 63.6%). Participation of employee representatives was, at 44.4%, not as high at Swiss companies as at those in neighbouring countries (DE 63%, AT 63.6%). This is relativised, however, by a glance at interested employees‘ opportunities for participation: whereas the percentage was 3.7% in German and 9.1% in Austrian companies, a percentage of 44% of Swiss respondents indicated thus.

In order to achieve the binding nature necessary as well as the personal obligation of each member of the organisation, the method of promulgation is essential to the implementation of companies‘ codes of conduct.

Employees are generally able to inform themselves of company codes of conduct, and in addition, they receive written information on it. On the whole, though, only somewhat over half of the companies surveyed (56.1%) confirm receipt of the document and attest in writing to their adherence to the behavioral guidelines laid down in it.

At four out of five companies (80.4%), codes of conduct are verbally addressed in order to increase understan-

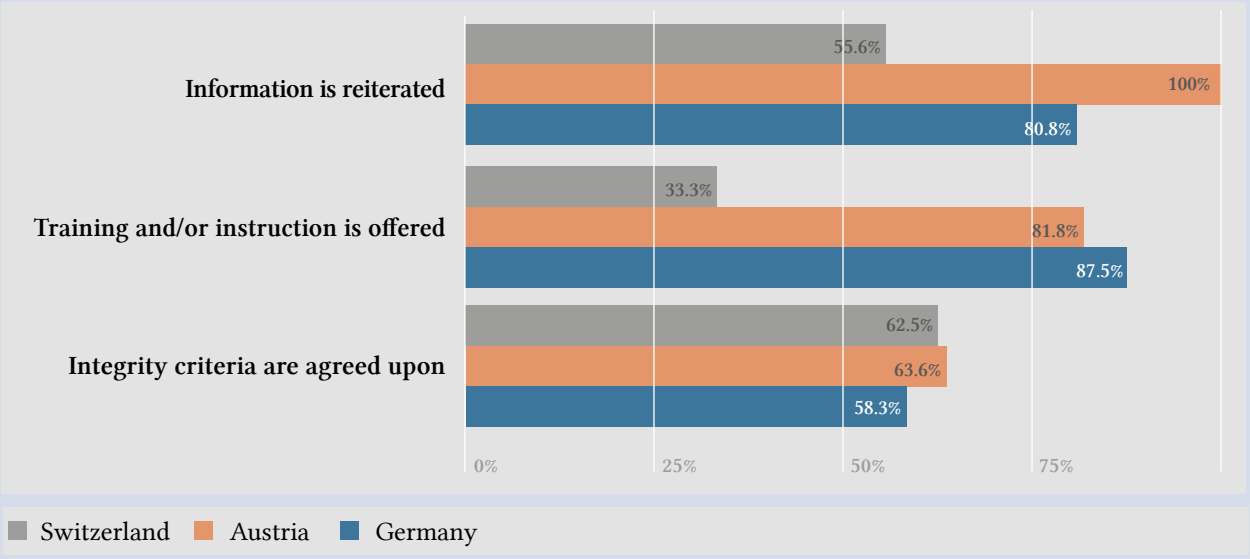
***Figure 12: Information for employees***




ding and plausibility. It is worth noting that only 44.4% of participating Swiss companies use either of the last two measures mentioned.

Reiterated information in the form of change notifications or content review is carried out across the group to the same extent as the communication of codes of conduct (80.4%); it is less common at Swiss companies. An even lower percentage of ethics training or instruction is offered at those companies. There are only minor differences among the three countries in regards to inclusion of integrity criteria in target agreements with managers.

***Figure 13: Information for employees***




In this survey, the availability of further guidelines and/or policies at companies was examined: at all of the companies surveyed, there are data protection guidelines; there is an anti-corruption policy at (only) 83% of them. The latter is most commonly implemented at participating companies from Germany and Austria.

***Figure 14: Availability of select policies***

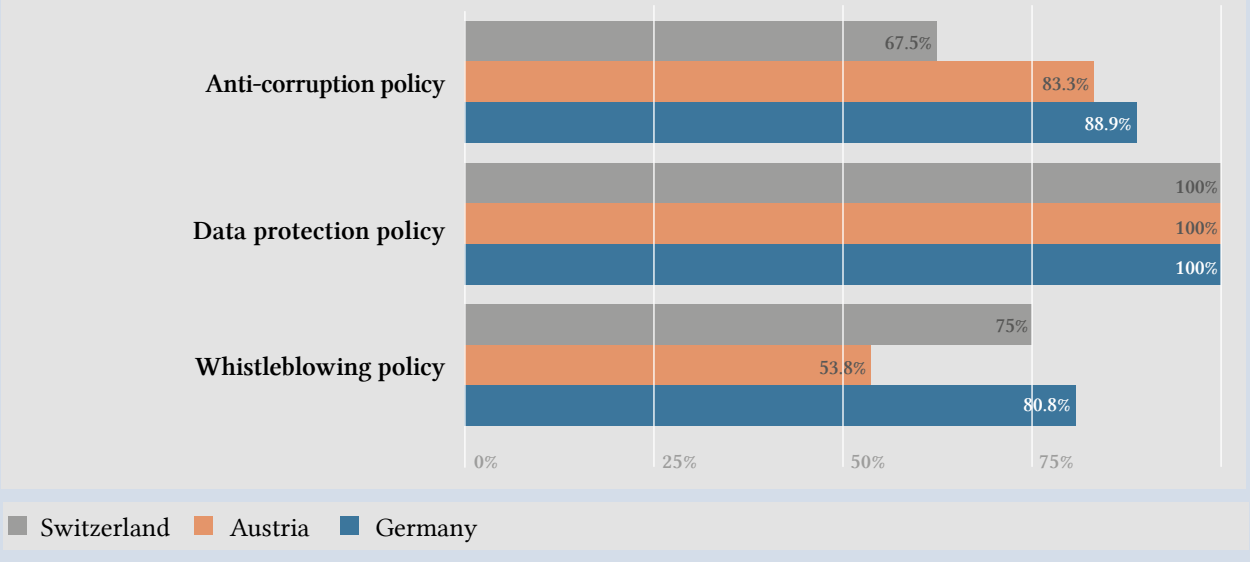
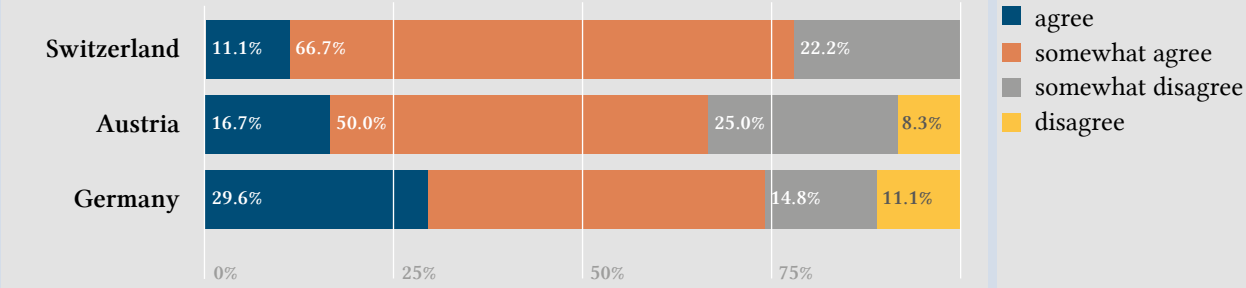


***Figure 15: Our company encourages internal whistleblowing***




The situation regarding whistleblowing policies varies greatly: they have been implemented at four-fifths of German, three-quarters of Swiss, and only a bit more than half of Austrian companies. Moreover, there is a multitude of further (security) policies at companies.

### Whistleblowing Systems: Room for Improvement in Austria

73.1% of companies surveyed indicate that, besides a whistleblowing policy, a whistleblowing system has been implemented; at a further 5.8% of the companies, one is being set up. In this area, as well, the differences among the individual countries is considerable: whereas only 6.7% of the German and 22.2% of the Swiss companies have no whistleblowing system (none planned, at least), at 53.8%, the percentage in Austria is considerably higher.

There is definitely a need for it, though: if one takes a look at the assessments by those surveyed of the encouragement of internal disclosure of employee behaviour which is damaging to the company, two-thirds of Austrians surveyed are in favor of such an aid to internal whistleblowing ("agree" and "somewhat agree"). In light of the results shown above, though, in many cases the availability of a whistleblowing system does not necessarily imply encouragement of it by the company.

Across the countries, about three-quarters of the companies surveyed (72.9% "agree" and "somewhat agree") encourage internal whistleblowing at least to some extent. To a similar extent, the assertion that at their own companies, whistleblowers do not matter is disputed (75.5% "somewhat disagree" and "disagree").

German companies surveyed are in large part convinced of a (relatively) high level of protection for whistleblowers; protection for whistleblowers is not as positively assessed in Austria and Switzerland.

Over a third of those surveyed says that (rather) excessive importance is placed on whistleblowing. Those from Swiss companies surveyed constitute the exception, 88.9% of whom regard the statement as (rather) not applicable at their firms.

***Figure 16: Whistleblowers do not matter at our company***

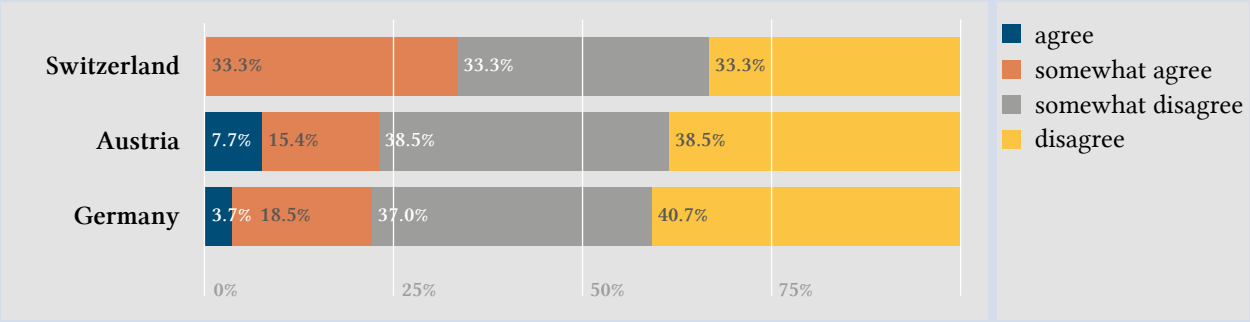



***Figure 17: We offer whistleblowers great protection***

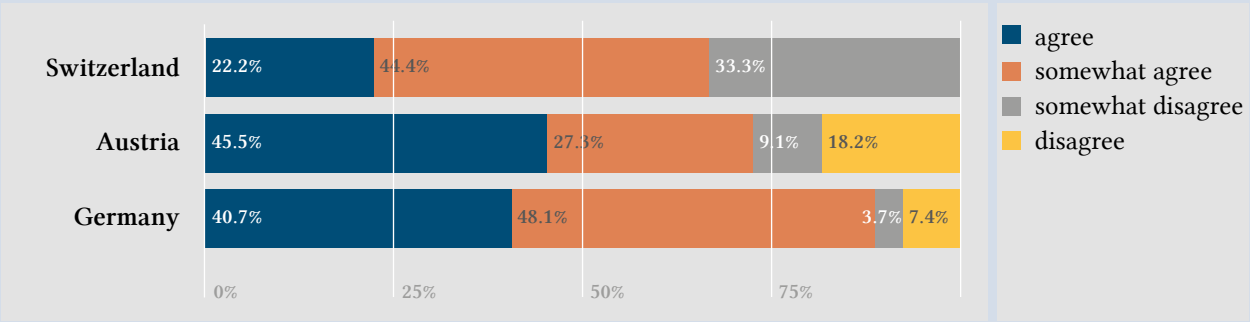
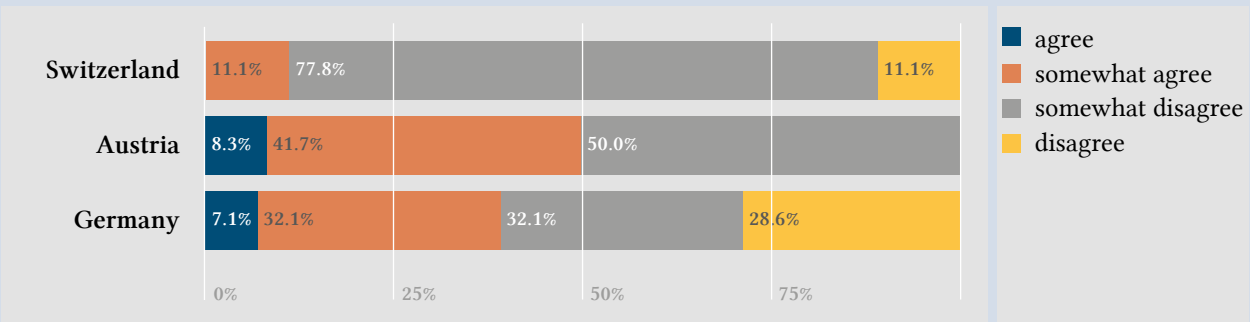



***Figure 18: Too much focus is placed on whistleblowing***



## 3.6 Crime Rate and Detection

Any company can be affected by crime. Large companies, in particular, are often targeted, and many potential crimes are not at all recognised as such or reported to the authorities. The survey data here always refers to a reference period of twenty-four months. Response options, besides the explicit ruling-out of having been victim of an offense, included the possibility of indicating one-time or numerous occurrences, or of admitting any uncertainty ("not to be ruled out").

Below, the overall results are presented first, and then the differences among the countries and in particular any differences relating to security organisation (whether or not there is a corporate security department), with a focus on company size, are highlighted.

### Property Crimes: Clear Differences

Of all the aforementioned crimes, property crimes occur with the most frequency. Theft and embezzlement had a two-year prevalence of 83% at the companies surveyed. The next most frequent offense is fraud, with a prevalence rate of 58.3%, followed by breach of trust, at 49%.

A unique picture emerges upon examination of the countries according to the last two offenses mentioned. Austrian companies indicated having been affected to a far lesser extent: by fraud, only 18.2% (compared to DE 71.5% and CH 66.7%), by breach of trust, 36.4% (DE 55.6%, CH 51.8%).

### Corporate Crimes: Counterfeiting More Common than Data Loss; High Uncertainty

The highest occurrence of corporate crimes appears to be product piracy, at 21.2% (at the same time, a high percentage of companies have not been affected, at 57.4%), followed by theft of confidential company data (and thus loss of know-how) at 19.5%, theft of confidential customer information, at 15.5%, and the occurrence of industrial and/or economic espionage, at 13%. In regards to the last three areas mentioned, uncertainty regarding their possible occurrence is quite high (from 46.7% to 60.9%).

***Figure 19: Property crimes—occurrence at companies***

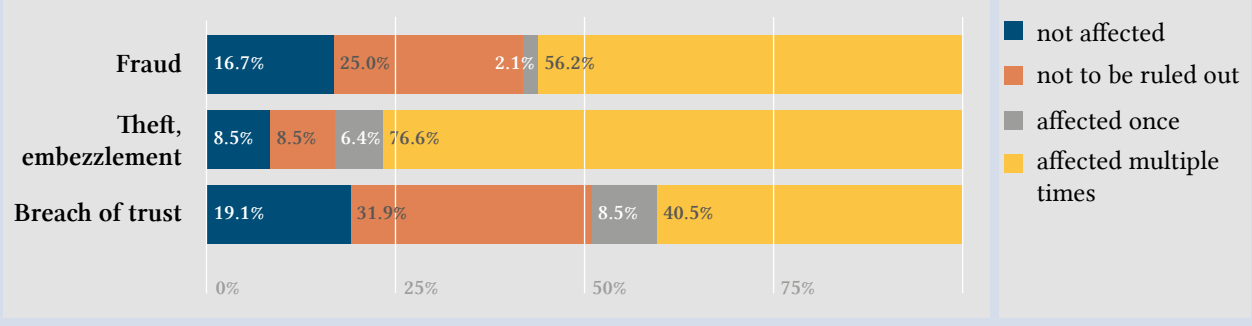
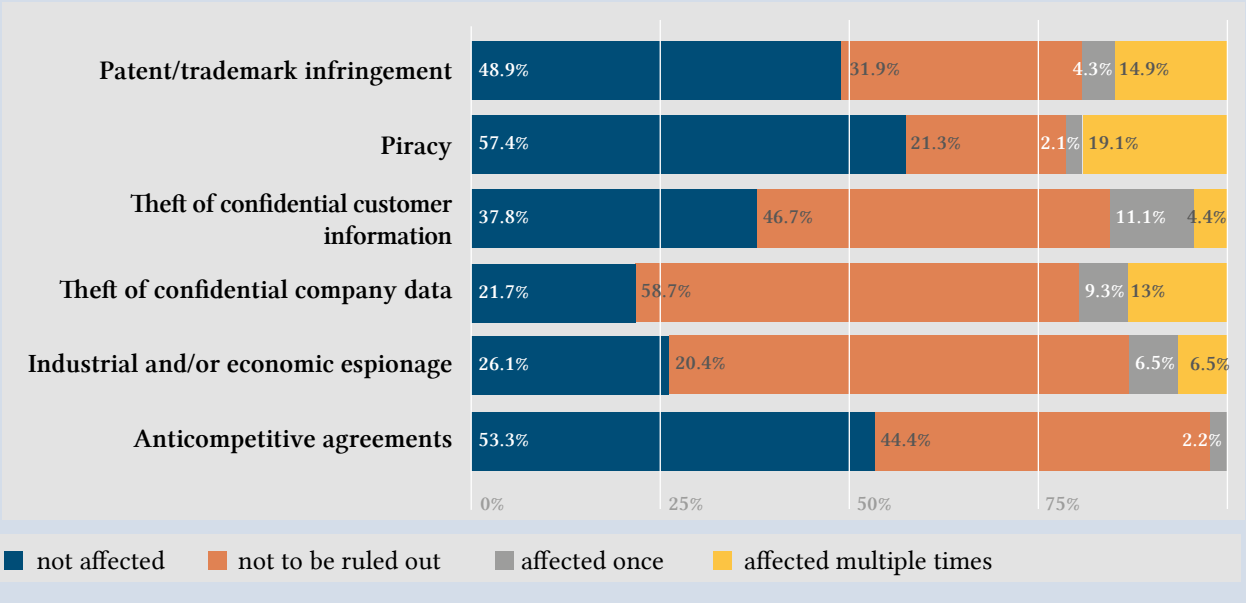


***Figure 20: Corporate crimes—occurrence at companies***




Furthermore, 22.7% of companies surveyed indicate one or more cases of corruption and bribery in the last twenty-four months. In addition, though to a lesser extent, antitrust violations (9%) and cases of money laundering (8.8%) have come to light. There is no data regarding established cases of doctoring the books. Data on "not to be ruled out" are in this case a sign of supposition of an unclear number of undetected occurrences thereof.

***Figure 21: Other criminal offenses—occurrence at companies***

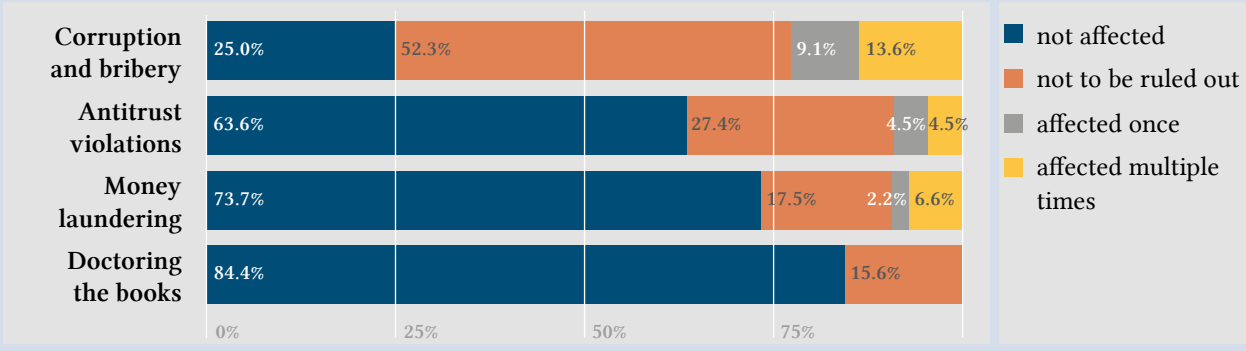
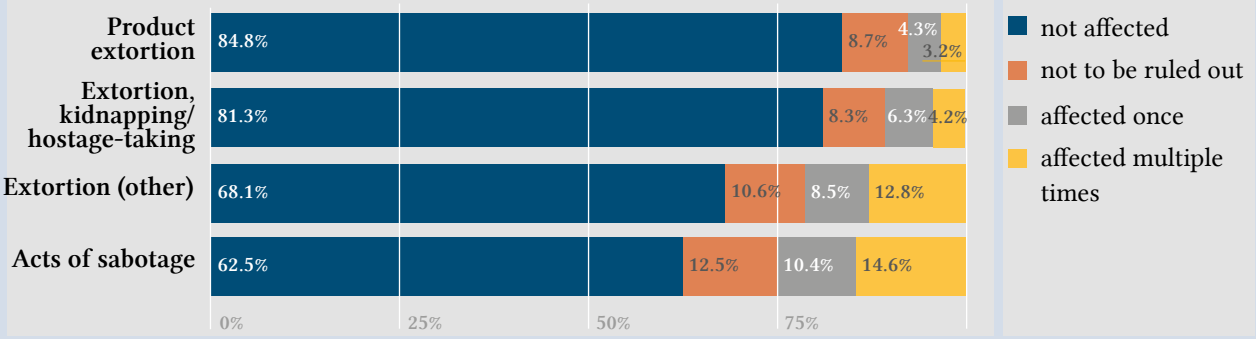


*Figure 22: Blackmail and sabotage—occurrence at companies*




## Prevalence of Extortion and Sabotage

One in four companies was victim to acts of sabotage in the two years leading up to the survey. Various forms of blackmail could be of importance to a not insignificant portion of companies: 6.5% were affected in the last two years by instances of product extortion, and 10.5% was affected by kidnapping and/or hostage-taking. Other forms of extortion were reported by 21.3% of those surveyed.

Prevalence shall be presented below as a function of the security organisation at companies, as it is to be assumed that the largest firms (with corresponding corporate security departments), in particular, fall victim to the most offenses.

The rates of prevalence depicted show the unusual extent to which large companies are affected by crime. Because the data refer only to the number of offenses reported internally at companies, one can assume that further (unknown) instances exist. That assumption is clear in light of the fact that those surveyed refuse to rule out the possibility of an offense having occurred. Participants to the survey from corporate security (as opposed to others responsible for security) indicated as such especi-

***Table 6: Crime rate by type of security organisation (prevalence over two years)***

| Offenses | Corporate security department at company (n=40) | Companies with a different security organisation (n=14) |
|---|---|---|
| Fraud** | 69.5 % | 25.0 % |
| Theft/embezzlement*** | 97.2 % | 36.4 % |
| Breach of trust | 57.2 % | 25.0 % |
| **Offenses** | **Corporate security department at company (n=40)** | **Companies with a different security organisation (n=14)** |
| Patent/trademark infringement | 22.9 % | 8.3 % |
| Product piracy | 25.7 % | 8.3 % |
| Theft of confidential customer information | 14.3 % | 20.0 % |
| Theft of know-how, confidential company data* | 22.8 % | 9.1 % |
| Industrial and/or economic espionage | 14.3 % | 9.1 % |
| Anticompetitive agreements | 2.9 % | 0.0 % |
| Corruption and bribery | 30.3 % | 0.0 % |
| Antitrust violations | 12.2 % | 0.0 % |
| Money laundering | 8.8 % | 8.3 % |
| Doctoring books/falsification of financial statements | 0.0 % | 0.0 % |
| Acts of sabotage | 29.7 % | 10.0 % |
| Product extortion | 5.8 % | 9.1 % |
| Kidnapping for ransom/hostage-taking | 13.5 % | 0.0 % |
| Extortion (other) | 25.0 % | 9.1 % |

Statistisch signifikante Unterschiede sind folgendermaßen gekennzeichnet: * p<.05, ** p<.01, p<.001

ally with industrial and/or economic espionage at a rate of 71.4% (versus 27.3% with known cases thereof), with theft of know-how, at 65.7% (versus 36.4%), and theft of confidential customer data at 51.4% (versus 30%) as well as anticompetitive agreements at 54.3% (versus 10%).

## Analysis and Reporting of Offenses

How are offenses recorded, analysed and reported at companies? The following section addresses the analysis and processing of incidents.

Overall, 72.3% of all surveyed indicated systematic collection of data on behaviour in all of the areas of criminal activity. A further 6.4% limit data collection to specific offenses. Regarding this question, there are not any significant differences among the countries.

Data on further details as to systematic collection of data on crime solely represent companies which perform such data collection.

***Figure 23: Systematic collection of data on known instances/offenses***

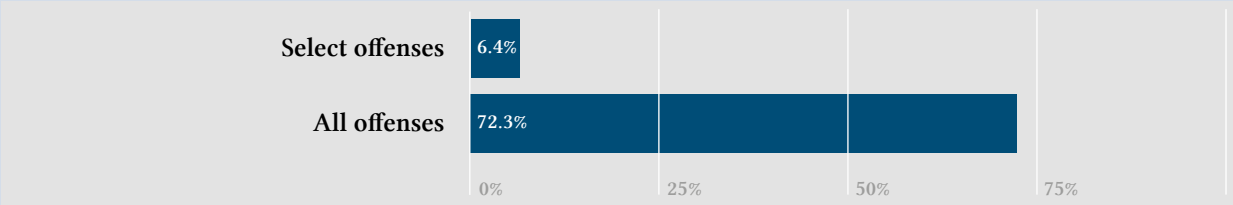
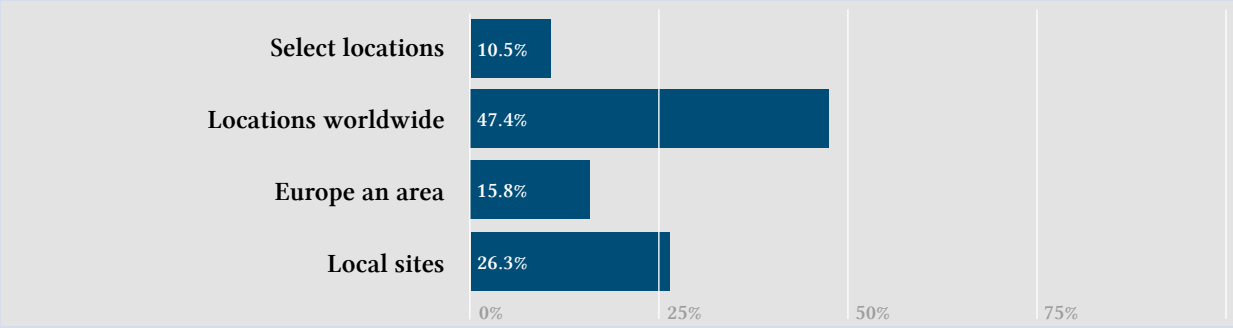



***Figure 24: Extent of systematic collection of data on known instances/offenses***

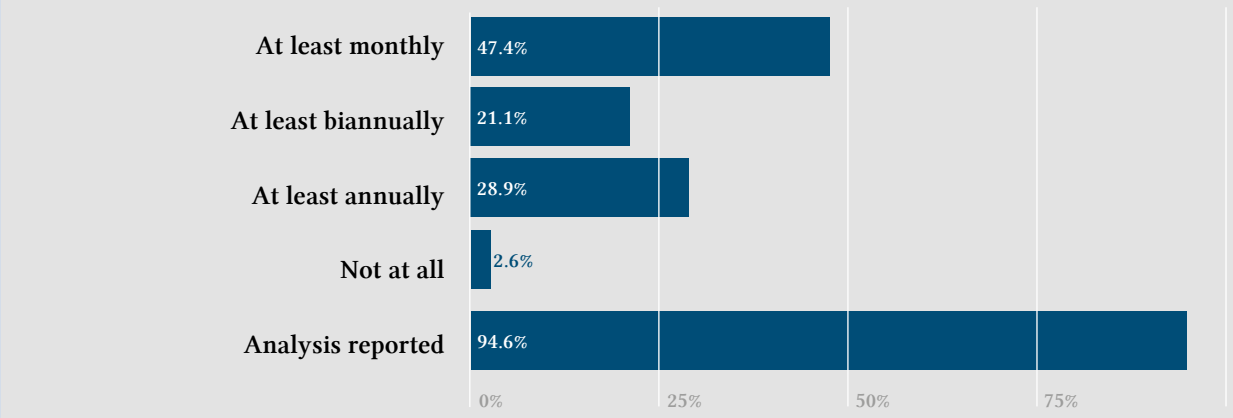



## Global Operations, Local Data Collection?

As mentioned at the start, the participating companies, banks and/or insurance providers are transnationally active. They are represented on average in forty-two countries (median: 30 countries); close to two-thirds (64.5%) are active on at least four continents.

At close to half of the companies that purposefully gather data on offenses, their approach applies to all of their locations worldwide (47.4%), while about a quarter of them do so at their local sites (26.3%), a sixth of them in the European area (15.8%), and a tenth of them at locations determined by other criteria (10.5%).

*Figure 25: Frequency and communication of analysis*




### Reporting Organised Differently

Data collected on known incidents are analysed by nearly half of these companies on a monthly basis, by the other half biannually or annually. In 94.6% of the cases, the results are reported to the management.

## 3.7 Assessments of Future Developments

To finish off, assessments of and concrete expectations for potential developments in this field of work were surveyed.

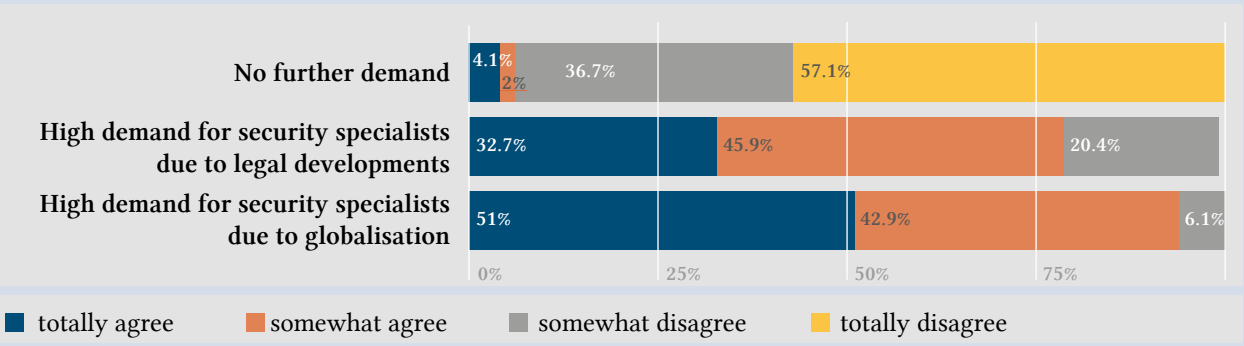
### Expectations: Great Need for Security Specialists

Numerous legal regulations determine the field of work of those responsible for security. 32.7% fully agreed, and 46.9% somewhat agreed with the statement that due to legal developments, in future there will be a greater need for security specialists. 20.4% did not share that view ("somewhat disagree").

TOP 100 companies operate in global networks, which implies particular challenges for those responsible for security. Clearly, increasing globalisation is seen as an even greater reason for the bigger demand for specialists in security matters: 51% agreed "fully" and 42.9% "somewhat" with that, as opposed to the 6.1% of respondents who "somewhat" disagreed with it.

In contrast, 4.1% and 2.0% of respondents (agreeing "fully" and "somewhat", respectively) see no further need for security specialists. 36.7% "somewhat disagreed", and a clear majority (57.1%) totally disagreed.

***Figure 26: Demand for security specialists***



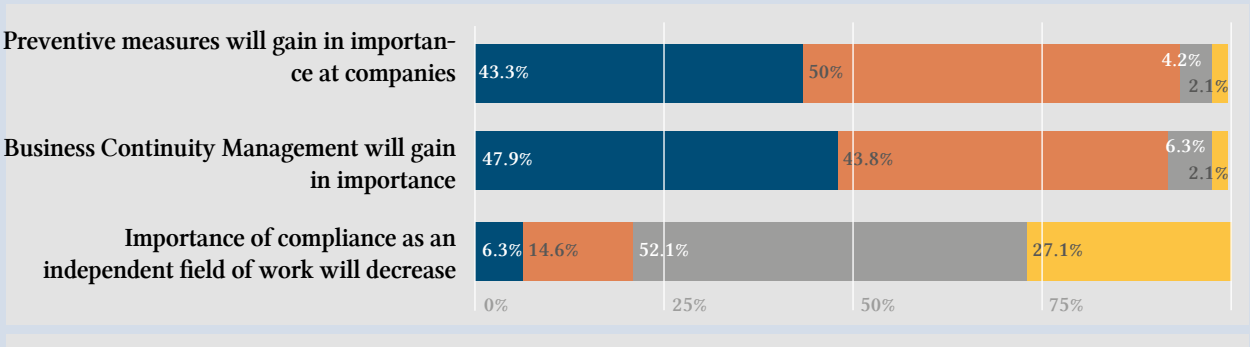

## Future Importance of Compliance, BCM and Prevention

According to the opinions of people responsible for security at TOP 100 companies, compliance will continue to be an independent field of work: only one in five believes the importance of compliance will decrease ("totally agree", "somewhat agree"), while almost 80% of those surveyed don't believe that.

Business Continuity Management was clearly identified as an issue for the future: 47.9% of respondents totally agree with the statement "Business Continuity Management will gain in importance", and another 43.8% somewhat agree. 6.3% "somewhat" disagree and 2.1% "totally" disagree. Distinctive features of particular companies or branches could be crucial factors here.

According to those surveyed, preventive measures will also gain in importance. Total agreement here comes from 43.8% of respondents, and 50% somewhat agree. Disagreement comes from only 3.7% (partial) and 1.9% (total).

***Figure 27: Future Developments***



# 4. Discussion of Results to Date

Prior to discussion of select findings within their larger context, it should be pointed out that in light of the size and features of the sampling—participants belong to the companies with the highest revenue as well as to the largest banks and insurance companies in participating countries—to generalise about all commercial enterprises of participating countries is of course not possible.

While some results match expectations and confirm historic data, others call for closer examination.

### Company Structure, Crime Rate and International Presencez

Of significance are perhaps the differing designs of the organisational structure of companies surveyed from Germany, Austria and Switzerland, which vary greatly: at nearly 90% of companies from Germany, there are corporate security departments; in contrast, they exist at approximately two-thirds of the companies in Switzerland, and in Austria at only 50% of the companies. Considerable differences persist in regards to the international presence of companies with corporate security departments as compared to those who organise security differently. The former are, on average, active in a considerably higher number of countries (M=52.2, as compared to M=8.4).

Distinctly international corporate activities may correlate closely to corporate crime rates: one to three times greater incidence was reported in the presence of a corporate security department.

Moreover, it stands to reason that greater focus would be placed on monitoring and briefing at companies with their own corporate security department. Another factor is that worldwide monitoring of crime rates occurs at more than half of the companies in Germany, but in Austria and Switzerland at merely a third.

### Crime Rates: Putting Findings into Context

Upon comparison of this study with other studies on this topic, a much higher crime rate is almost always to be observed. Here it is to be stressed that this study deals exclusively with large companies, whereas otherwise small and medium-sized companies are normally examined. Thus the risk of being affected by (economic) criminal acts grows, statistically speaking, with the size of a company.

The fact that theft/embezzlement as well as fraud and breach of trust are the most common offenses suffered by large companies is confirmed by other studies. For example, theft/embezzlement were the most common offenses in the most recent study by KPMG (2014), dealing with N=32 large companies in Germany and N=31 in Austria, followed by fraud and breach of trust, while in Switzerland (N=30), however, theft/misuse of data was number one.

Theft leads the list of the most frequent offenses even at companies that are not so large, as suggested by results of the "WIK/ASW-Sicherheits-Enquête 2012/2013", [WIK = Zeitschrift für die Sicherheit der Wirtschaft, Corporate Security Magazine; ASW = Allianz für Sicherheit in der Wirtschaft, Alliance for Security in Business Security Survey] which also indicate a high degree of occurrence (84.8%).

In this study, the unusually low occurrence of breach of trust at participating Austrian companies (as compared to German and Swiss companies) is conspicuous. These findings may be associated with specific conditions in Austria, though they may in part be attributed to security structure and thus involve the size and the international activities of Austrian companies. Of those surveyed, the percentage of Austrian firms with their own corporate security department was 46% (DE 87.5%, CH 66.7%).

The study clearly showed the influence of company organisation on the disclosure of crime rates. Companies with a corporate security department demonstrate a considerably higher prevalence than those without. This could relate to the fact that the scope of this study deals with especially large companies, which for this reason alone have a high prevalence of instances of crime. Size could also complicate the picture and lead to fewer offenses being detected. This, however, can be ruled out, because over 72% of the companies surveyed here systematically record and analyse their crime rates. These findings are of great importance when interpreting pertinent studies and the creation of future studies. Studies investigating the crime rates of companies should test whether a systematic collection of data on crime is in existence, because the results on companies with or without systematic reporting on crime cannot be easily compared. For future studies, these findings point out the possibility of abandoning the rough instrument of prevalence and not only asking whether a company has been a victim to a specific crime, but also surveying their frequency/incidence. Further possibilities would thereby open up, for example as to whether the effectiveness and importance of preventive measures can be examined in greater detail. It is no surprise that over 90% of those surveyed are acting on the assumption that prevention will play a greater role in future.

## Differing Responsibilities: Possible Reasons

Considerable differences in scopes of responsibility arose between Germany, on the one hand, and Austria and Switzerland, on the other. This could indicate a differing understanding of security at group level, but could potentially be linked to the fact that the sizes of the companies belonging to the "TOP 100" vary greatly. In regards to the functional responsibility of security departments, the study shows, on the one hand, a core collection of areas of responsibility, summarized in Cluster 1 above, based on a so-called cluster analysis. On the other hand, interesting differences resulted among the various countries involved. Especially remarkable is the high percentage of Austrians surveyed who rated know-how protection as irrelevant or of little relevance to their companies, and the high percentage who consider neither risk analysis, risk management nor prevention of property and economic crimes to fall within their realm of responsibility. Security departments or those in charge of security in Austria and Switzerland are responsible to a much greater extent than those in Germany for data protection, workplace violence, occupational health and safety, and fire safety. This led to the development of Clusters 2 and 3 in the analysis.

These differences could have a particular historical, societal or even legal background, though they could have to do with the organisational structure. They could also be associated with the varying composition, in regards to branch

and size, of the TOP 100 companies surveyed. An enquiry into the latter factors mentioned was refrained from in order to protect the anonymity of those surveyed. Due to the fact that in this and other analyses the importance of these aspects has repeatedly been demonstrated for the interpretation of results, this decision should be reconsidered for further studies. Regardless of that, the results offer the impetus of comparing notes on their experience with the various responsibilities of security departments or those in charge of security, and perhaps to readjust responsibilities based on that outcome.

A further interesting fact is the topic of whistleblowing systems, which has established itself in Germany and Switzerland, while in Austria still half of the companies has no appropriate system available or is considering introduction thereof.

## Topic for the Future: Job Satisfaction and Appreciation

In conclusion, other findings should be highlighted: the importance of satisfaction and its link to appreciation.

Basically, a relatively high level of satisfaction of those surveyed can be confirmed, especially in regards to satisfaction with their own positions as well as with the perceived support of the board. Nevertheless, 46.3% of those in charge of security feel (rather) not seen as an integral part their company‘s success.

One‘s own assessment of whether they feel they are seen as “business enablers” correlates significantly to almost all of the satisfaction values surveyed: satisfaction with a functional link to the board (Spearman-rho=.582; p<.001) and with its support (rho=.424; p<.01), with the budget available to them (rho=.459; p<.01), and last but not least to their satisfaction with their own position within the company (rho=.408; p<.01).

Security is perhaps perceived at some companies as rather a cost center and a “business disabler” than a “business enabler”. The results here suggest that a change in this perspective could have a positive effect on the (job) satisfaction of those responsible for security and their employees. From the point of view of occupational psychology, this could also have an effect on motivation and efficiency, which the company could in turn also profit from.

# 5. Conclusion

## Future Trends in the Role of CSO: Diverse Challenges

The study here on those in charge of corporate security covers a common language area which is at the same time a very developed and interdependent economic area. Due to the particular features of the TOP 100 companies (the complexity of organisations, global networking, being pioneers and/or role models, and their economic importance), it will be quite interesting to focus on the corporate security situation at those companies more closely in future. Evaluation of other data from this study will illuminate even more interesting aspects.

Overriding themes and challenges will now be outlined in forecast of the future of corporate security.

## Business Continuity: Crises Close to Europe as the New Normal?

Insurance specialists at large enterprises repeatedly identified "business interruption" as the greatest risk to companies in the "Allianz Risk Barometer on Business Risks 2014". Day after day, CSOs and their teams provide an important contribution to the fact that the value chain remains intact. Hardly a year demonstrates more clearly than 2014 how quickly the security policy situation can change: the European Union is confronted with conflict in neighbouring regions to its south, southeast and east. Along with human suffering, these carry with them economic effects. Still-unstable countries with unresolved political situations in North Africa, a flow of refugees, civil war in Syria and the accompanying ISIS terror in northern Iraq, as well as hostilities in the Ukraine impair business relationships as well. For CSOs, the picture can change at any moment, and stakeholders in the financial markets follow the activities of global companies affected very closely. As a result of the great importance of the Ukraine in energy transport, general awareness of the magnitude of international interconnectedness and the dependence of suppliers has greatly increased.

## The Future: Focus on Interconnected Global Risks

These networks have been the center of public discourse since 2013, and they are, in another regard, of great relevance to company security: with Edward Snowden's exposure of the NSA's activities, cyber security has entered the collective consciousness. Those revelations also result indirectly in discussions on regulations. The World Economic Forum's current "Global Risk Report" confirms that, as it was created in conjunction with universities and significant players in the insurance business: besides the current greatest risks perceived, "financial crises in important economies", then "high structural unemployment" and "water crises" (water supply and extreme weather catastrophes), three related risk groups were detailed. These will gain in great importance for the work of those responsible for corporate security at globally active companies:

- Greater instability in an increasingly multipolar world (demographic change in various forms, a growing middle class in developing countries, tight national budgets as well as the trend towards more limited economic ties)
- A "lost generation" of young unemployed or precariously employed who pose a challenge to the educational system, the job market and society
- The disintegration of the digital economy/society, if, due to continuing attacks resulting from the vulnerability of networks, trust is eroded in the internet as a basis for communication and economic activity.

**More Focus on Economic Crime, Compliance and IT Security**

In the area of compliance, ongoing legal developments and the interconnectedness of potential economic offenses are a starting point for continuing academic support. Comparable surveys, such as those from KPMG (2012, 2014) and PWC (2014) focus primarily on members of top management as addressees, and content-wise they focus on various aspects of economic crime and compliance. A continuous increase over the years in the degree and importance of cyber crime in its various forms is demonstrated by these studies.

A major signal that the topic is gaining in importance is the attention paid to it by the insurance business, as indicated again by the "Allianz Risk Barometer": in all three of the regions studied (the Americas; EMEA: Europe, Middle East, and Africa; and Asia Pacific), cyber crime, IT failures, and espionage have climbed in the rankings, and now constitute some of the top ten risks—perhaps as a result of discussions

on the revelations by Edward Snowden. Theft, fraud and corruption are also among the top ten in the Americas and EMEA. Varying perceptions of risk are, on the one hand, the result of being differently affected by it due to economic structures and developments. On the other hand, this leads to the question of whether different security cultures might exist.

Potential differences in approaches and attitudes of CSOs could be the object of future studies: how much emphasis do they place on technical, organisational or physical solutions? Which methods and tools are combined, and how? Is there a particular European security culture at companies? If so, how does it differ from Anglo-American security culture?

Furthermore, the findings gathered here show that a large portion of the TOP 100 companies already systematically collects data on the occurrence of crime, as well as on quantitative differences. They demonstrate that future studies should not limit themselves to the current widespread use of surveys on mere prevalence. In fact, a quite different picture of the current situation could be painted by frequency/incidence, at least at the TOP 100 companies, and they could also form the basis of future trend analyses and impact analyses of preventive measures.

## Boom for Security Experts, New Collaborations

Overall it is expected that the role and the realm of responsibility of CSOs will expand even more in regards to their analytical and strategic components. Whereas earlier, multiple risks were paid little attention, according to our assessment, professionalisation is taking place at companies of all sizes. In the mid-term, no company can afford systematic underestimation or disregard of risk, nor inadequate prevention.There are thus more opportunities for collaboration with the authorities.

Attitudes of those responsible for corporate security and their most important areas of overlap within the company—their ties to top management—had never been studied in this form prior to the research findings presented here. A continuation or repetition of this study could uncover changes over time and enable timely reactions. Questions as to expectations of future employees could generate valuable feedback for initial and continuing education.

# Bibliography


ALLIANZ (2014). Allianz Risk Barometer on Business Risks 2014. URL: www.agcs.allianz.com

Buerschaper, C. (2008). Organisationen – Kommunikationssystem und Sicherheit. In P. Badke-Schaub, G. Hofinger & K.

Lauche (Hrsg.), Human Factors – Psychologie sicheren Handelns in Risikobranchen (Kap. 9). Heidelberg: Springer Medizin Verlag.

Erwin P. M. (2011). Corporate Codes of Conduct: the effects of code content and quality on ethical performances. Journal of Business Ethics, 99(4), 535 – 548.

Fahlbruch, B., Schöbel, M. & Domeinski, J. (2008). Sicherheit. In P. Badke-Schaub, G. Hofinger & K. Lauche (Hrsg.), Human Factors – Psychologie sicheren Handelns in Risikobranchen (Kap. 2). Heidelberg: Springer Medizin Verlag.

Hofmann, S. (2008). Anti-Fraud-Management: Bilanzbetrug erkennen - vorbeugen – bekämpfen. Berlin: Erich Schmidt.

Hudson, P. (2007). Implementing a safety culture in a major multi-national. Safety Science, 45(6), 697-722.

Jöns, I., Hodapp, M. & Weiss, K. (2006). Kurzskala zur Erfassung der Unternehmenskultur. Mannheimer Beiträge 01/06. Mannheim: Universität Mannheim.

Kaptein M. & Schwartz, M. (2008) The effectiveness of business codes: A critical examination of existing studies and the development of an integrated research model, Journal of Business Ethics, 77, 111-127.

KPMG (2012). Wirtschaftskriminalität. Deutschland – Eine empirische Studie zur Wirtschaftskriminalität im Mittelstand und in den 100 größten Unternehmen. URL: www.kpmg.com.

KPMG (2013). Wirtschaftskriminalität. Deutschland, Österreich, Schweiz im Vergleich – Wirtschaftskriminalität in Grossunternehmen und dem Mittelstand. URL: www.kpmg.com.

PWC (2014). Economic Crime: A Threat to Business Globally. URL: www.pwc.com/crimesurvey.

Wecker, G. & Van Laak, H. (2009) (Hrsg). Compliance in der Unternehmenspraxis – Grundlagen,
Organisation und Umsetzung. Wiesbaden: Gabler.

Weick, K.E. & Sutcliffe, K.M. (2003). Das Unerwartete managen. Wie Unternehmen aus Extremsituationen lernen. Stuttgart: Klett-Cotta.

WIK/ASW-Sicherheits-Enquête 2012/2013 (2013). Ergebnisse der WIK/ASW-Sicherheits-Enquête 2012/2013. Gau-Algesheim: SecuMedia.

World Economic Forum (2014). Global Risks 2014, Ninth Edition. Genf: World Economic Forum. URL: www3.weforum.org.

# Partners

## University of Applied Sciences FH Campus Wien

With more than 4,600 students (as of November 2014), the FH Campus Wien is the largest accredited university of applied sciences in Austria. In the departments Applied Life Sciences, Building and Design, Health, Public Sector, Social Work and Engineering, a selection of over fifty bachelor's and master's degree programs is on offer to students. The FH Campus Wien is connected to companies, associations, schools and public institutions. Degree programs' numerous R&D projects as well as externally commissioned work are carried out through their own research and development organisations.

The field of Risk and Security Management belongs to the Public Sector Department. Both tracks—the bachelor's degree program, Integrated Security Management, and the master's degree program, Risk Management and Corporate Security—are organised as part-time tracks, and are unique in Austria.

www.fh-campuswien.ac.at

## University of Applied Sciences for Public Administration Bremen

University of Applied Sciences for Public Administration Bremen was founded in 1979 as the internal College of Civil Service. In recent years it has opened up to further degree programs focussed on justice, security and police. Degrees on offer currently include the three bachelor's programs Law Enforcement, Risk and Security Management, and Tax Law.

University of Applied Sciences for Public Administration Bremen maintains/runs two independent institutes: the Institute for Police and Security Research and the Institute for Police Training in the German state of Bremen. The training institute for police provides Bremen police with their entire professional training and engages in partnerships with the German Police Academy and other state police organisations for management training. IPOS is engaged in police- and other security-related fields of research, pursues an interdisciplinary and practice-oriented approach, and in addition to EU projects, conducts externally-funded projects and R&D projects at national and local levels.

www.hfoev.bremen.de www.ipos.bremen.de

# Autobiographies

**Prof. Dr. jur. habil. Arthur Hartmann** has led the Institute for Police and Security Research at the University of Applied Sciences for Public Administration Bremen since 2009.
After his studies in law and sociology at Ludwig Maximilians University Munich, he worked as a teaching assistant and did research on a pilot program for victim-offender settlements in juvenile law. Starting in 1992 he worked as a research assistant at the Institute for Criminology at the University of Heidelberg, where he was promoted to professor of criminology, criminal law and criminal procedure with his work on organised crime. After an interim professorship at Humbolt University Berlin and his activities as acting director of the Institute for Criminology at the University of Tübingen, he was appointed to the Hochschule für Öffentliche Verwaltung Bremen in 2002.

Contact:
Tel.: +49 421 36159-519
email: arthur.hartmann@hfoev.bremen.de

**Prof. Dr. phil. Claudia Kestermann** is professor of forensic and criminal psychology at the University of Applied Sciences for Public Administration Bremen, as well as acting director of the Institute for Police and Security Research (IPOS). Her research and development focus lies in the area of criminal research and applied security research.
After her studies in psychology, criminology and criminal law at the Universities of Bochum and Bonn, the psychologist got her doctoral degree from the University of Bremen in 2001. Her activities over several years as research assistant at the Universities of Bremen and Greifswald were followed by a change to the HfÖV. There she was substantially involved in the development and implementation of the bachelor‘s degree program Risk and Security Management, which she today directs.

Contact:
Tel.: +49 421 36159-446
email: claudia.kestermann@hfoev.bremen.de

**FH-Prof. DI Martin Langer** is director of the department Risk and Security Management at the University of Applied Sciences FH Campus Wien and directs the bachelor‘s degree program Integrated Security Management as well as the master‘s degree program Risk Management and Corporate Security.
Before that, Langer was active as a consultant on security and crisis management at scores of publicly-traded companies in Austria and Germany. In addition, he headed international operations for the Red Cross, the Austrian Federal Army, and the UN following natural catastrophes in Turkey, Mozambique, Honduras and Iran. Langer is a graduate of the Austrian government‘s Strategic Leadership Program, and is currently interested in business protection.

Contact:
Tel.: +43 1 606 68 77-2151
email: martin.langer@fh-campuswien.ac.at

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

www.fh-campuswien.ac.at
www.hfoev.bremen.de

HfÖV
Hochschule für
Öffentliche Verwaltung Bremen