



Corporate Security emerges in the executive spotlight

Corporate Security Benchmarking Survey 2024



Table of Contents

i.	Introduction	3
ii.	Survey approach	4
iii.	Key findings	5
1.	Corporate Security's appeal – strengthening an established role	6
2.	Current challenges and upcoming technological changes	9
3.	Evaluating AI's role in Corporate Security	14
4.	Risk strategies and upcoming challenges	16
5.	Conclusion	19

Introduction

In recent years, the Corporate Security function, or equivalent (henceforth called Corporate Security), has established itself as both a business enabler and a crisis responder. Corporate Security Officers (CSOs) not only react to risks but also anticipate them. This evolution is evident in times of major disruptions, such as the war in Ukraine, the economic fallout from the COVID-19 pandemic, the ongoing tensions in the Middle East, and the shifting dynamics of global trade. As businesses face a multitude of risk scenarios, Corporate Security should be recognised not merely as a supportive function but as a crucial element of business strategy and resilience.

The Corporate Security Benchmarking Survey aims to broaden the discussion around Corporate Security by incorporating the perspectives of CSOs and gathering insights from the C-suite*. The first edition of the survey, conducted 2022, revealed that

80% of the C-suite and CSOs believed Corporate Security was perceived as a business enabler throughout the organisation.

This second edition builds on the results of the first to generate a deeper understanding of Corporate Security's existing landscape and future direction. It focused on assessing Corporate Security's present status, addressing its challenges, and exploring the impact of emerging technologies, particularly AI, on its role and strategies.

The survey also addressed the risks associated with these new technologies and evaluated how well Corporate Security is positioned to attract and retain talent. Moreover, it looked at the digital maturity necessary to meet today's challenges and opportunities to maintain its strategic role. To understand Corporate Security's existing challenges and future potential, we drew insights from the C-suite and CSOs.

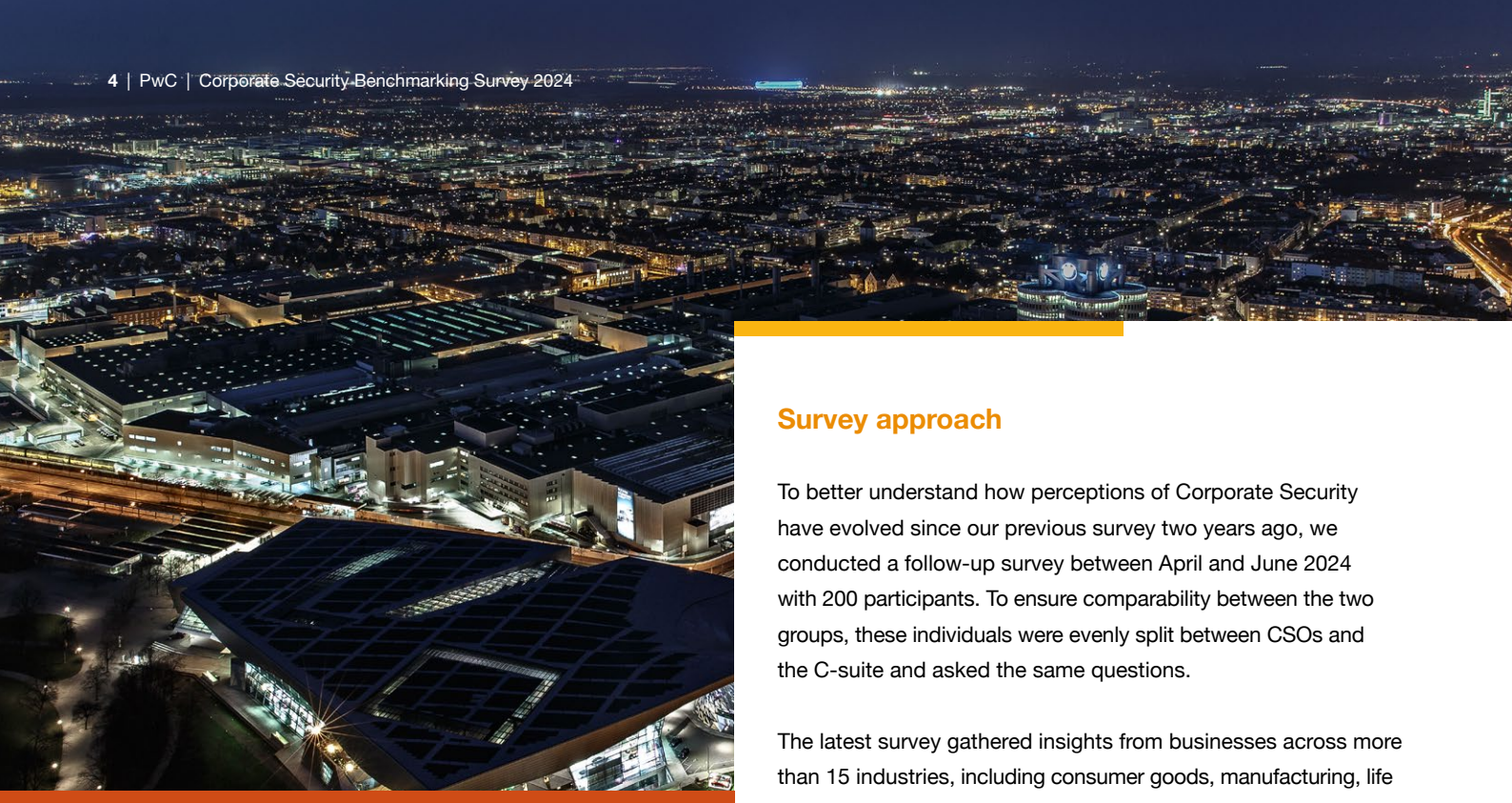
As part of our analysis of Corporate Security, we explored:

- 1 The degree of perception gap related to Corporate Security between the C-suite and CSOs
- 2 Its attractiveness for young talent in comparison to other corporate functions
- 3 Current and future trends and topics from the perspective of two groups: the C-suite and CSOs
- 4 The role of digital technologies, such as AI, and the associated security risks

- 5 Its digital maturity level and preparedness for current challenges
- 6 The risk affinity with which the C-suite and CSOs approach business

*The 'C-suite' designated target group is a collective category that includes different areas of responsibility. The participation criteria for the target group included persons from the areas of 'member of management, board of directors, C-suite'."





Survey approach

To better understand how perceptions of Corporate Security have evolved since our previous survey two years ago, we conducted a follow-up survey between April and June 2024 with 200 participants. To ensure comparability between the two groups, these individuals were evenly split between CSOs and the C-suite and asked the same questions.

The latest survey gathered insights from businesses across more than 15 industries, including consumer goods, manufacturing, life sciences and healthcare and automotive companies. Our findings consider the perspectives and experiences of a broad cross-section of organisations in terms of size, with respondents classified into three categories: small (total revenue below €500 million [m] – 46% of respondents), mid-sized (total revenue between €500 m and €1 billion [bn] – 30%), and large (total revenue above €1 bn – 25%).

The survey's findings provide further insight into how attitudes towards Corporate Security can vary depending on factors such as company size and industry. Disclaimer: All opinions are perceptions at the point of the data collection.

life sciences and
healthcare companies

12 %

50/50
C-suite/CSOs

<15

different industries

consumer goods
companies

21 %

200

survey respondents

30 %

< €1 bn

46 %

< €500 m

manufacturing
companies

19 %

automotive companies

10 %

25 %

> €1 bn



Key findings

1

The majority of C-suite and CSOs viewed Corporate Security as **equally or more attractive** than other corporate functions like Strategy, IT, and Compliance for young talents. This insight influences talent strategies, with a stronger emphasis on **internal training** over external recruitment.



2

The main **obstacles** faced by Corporate Security in adequately fulfilling its tasks are **conflicting operational priorities** and limited **financial resources**.



3

Over half of the respondents considered their Corporate Security to have an '**established**' or '**advanced**' level of **digital or technological maturity**. Only a small percentage indicated a need for significant improvement.



4

Around two-thirds of respondents believed their Corporate Security was **sufficiently digitalised** to meet **current challenges** and indicated that they would not pursue any additional **technology trends** other than the ones noted in the survey.



5

More C-suite representatives than CSOs perceived increased **security risks** for Corporate Security associated with **using AI**.



6

Most CSOs and C-suite executives exhibited a **risk-averse** approach towards **business**. They stated their key objective was to **avoid security risks** and uncertainties rather than accept the risks for particular business benefits.



7

Compared to CSOs, the C-suite was **more optimistic** about an **increase** in the **Corporate Security budget** over the next two years.



8

Both groups cited **Cybercrime**, **Information Security**, **Product Security**, and **Supply Chain Security** as the biggest challenges for their organisations' Corporate Security in the next two to three years.



1.

Corporate Security's appeal – strengthening an established role

The establishment and appeal of Corporate Security

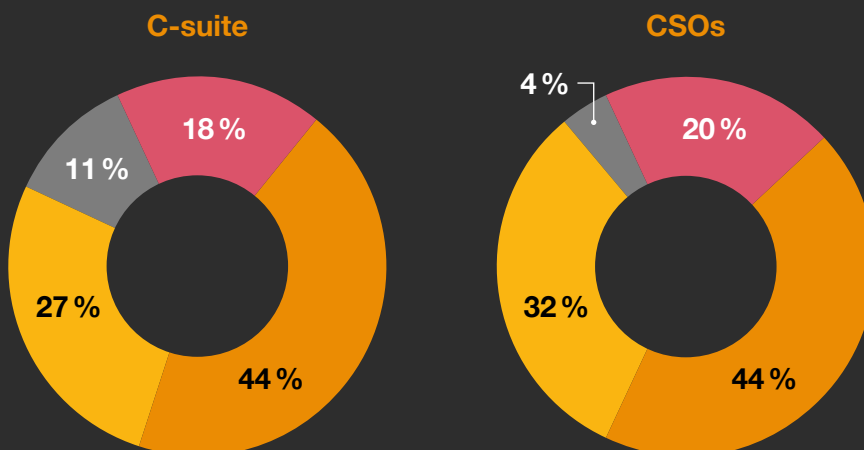
Having evolved from a business enabler to a critical business function, the next challenge for Corporate Security is solidifying its position. An important aspect of this is its attractiveness to young talent. Compared to functions like Strategy, IT, or Marketing, 44 % of participants viewed their Corporate Security as equally attractive, while 20 % of CSOs and 18 % of the C-suite considered it more attractive.

Those who considered their Corporate Security more attractive were asked what makes it appealing to young talent.

A quarter of CSOs and 28 % of the C-suite named attractive working conditions. Another important aspect for both groups was relevant and meaningful job content, highlighted by 25 % of CSOs and 22 % of the C-suite. The top factor for CSOs was varied tasks, mentioned by 35 %, whereas only 6% of the C-suite noted this.

Those who found their Corporate Security less attractive compared to other functions suggested external communication to enhance the profession's image (31 % of CSOs, 22 % of the C-suite), better working conditions (22 % of CSOs, 11 % of the C-suite), and internal communication to elevate the function's profile (13 % of CSOs, 15 % of the C-suite). Positioning Corporate Security as a desirable career option can help build a strong pipeline of future security professionals.

Overall, several factors make Corporate Security attractive. For CSOs, collaborative teamwork ranked highest at 40 %, followed by the use of advanced technologies (38 %) and work-life balance (36 %). For the C-suite, collaborative teamwork and a home office option ranked in joint top place at 40 % each, with work-life balance following (at 32 %). Notably, 10% fewer CSOs mentioned the home office option, while 10% more considered advanced technologies and employee recognition as advantages.



Talent management makes the difference

As Corporate Security cements its role and appeal, effective talent management becomes crucial for maintaining and enhancing its perceived status as attractive to young talent. For this reason, we conducted a detailed examination of CSOs' and C-suites' talent strategies.

Compared to other departments (e.g. Strategy, IT, Compliance, Audit or Marketing) Corporate Security is...

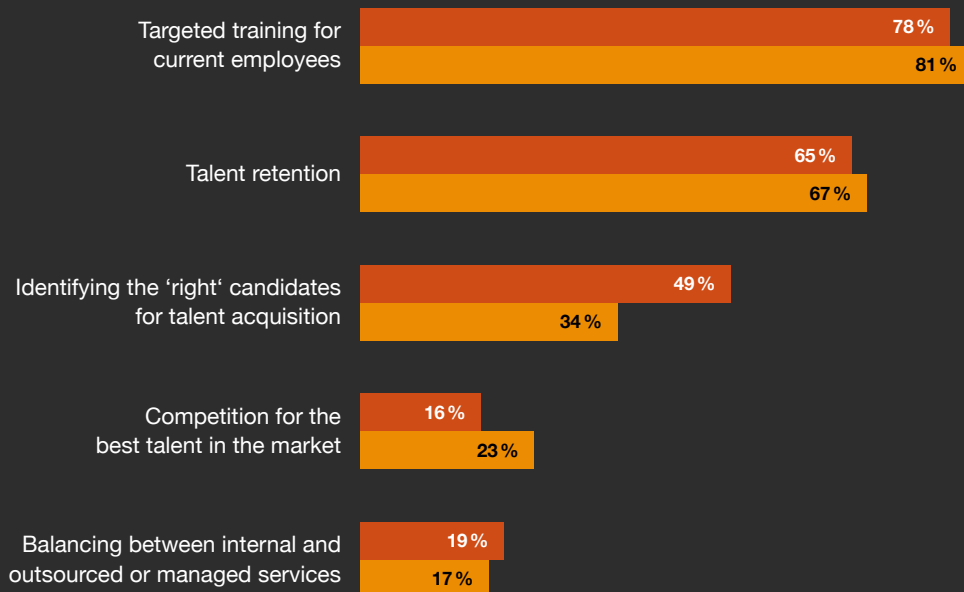
More attractive Equally attractive Less attractive Do not know/No answer

Basis: All companies



Talent strategy insights

Asked about their talent strategies, CSOs and the C-suite agreed that upskilling current employees was the most effective method; 81% of CSOs and 78% of the C-suite named it their top priority. Talent retention was also a key focus, cited by 67% of CSOs and 65% of the C-suite. Identifying the right external candidates for recruitment ranked third, mentioned by 34% of CSOs and 49% of the C-suite. Competition for the best talent in the market ranked fourth, mentioned by 23% of CSOs and 16% of the C-suite. Balancing between internal and outsourced or managed services ranked fifth, mentioned by 17% of CSOs and 19% of the C-suite.



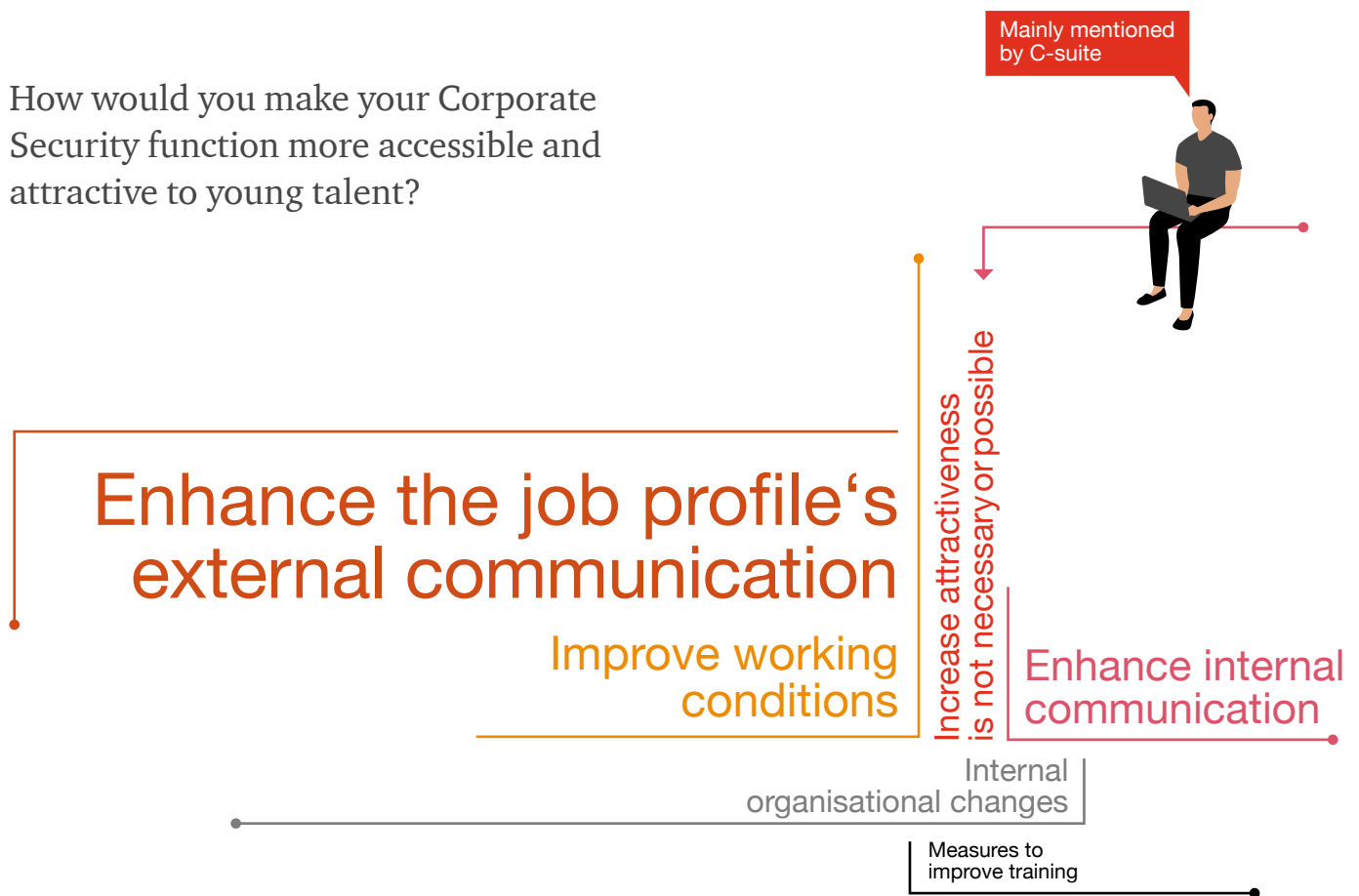
Which of the following are the top three talent strategy measures for your company's Corporate Security in the coming years?

■ C-suite ■ CSOs

Basis: All companies | Multiple answers were possible



How would you make your Corporate Security function more accessible and attractive to young talent?



Basis: Companies that consider Corporate Security to be less attractive in comparison (59 respondents)



An in-depth analysis

With Corporate Security established and fully recognised, the focus now shifts to ensuring it continues to thrive and maintains its pivotal role over the long term. We explored the current challenges and emerging technological changes crucial for achieving this.

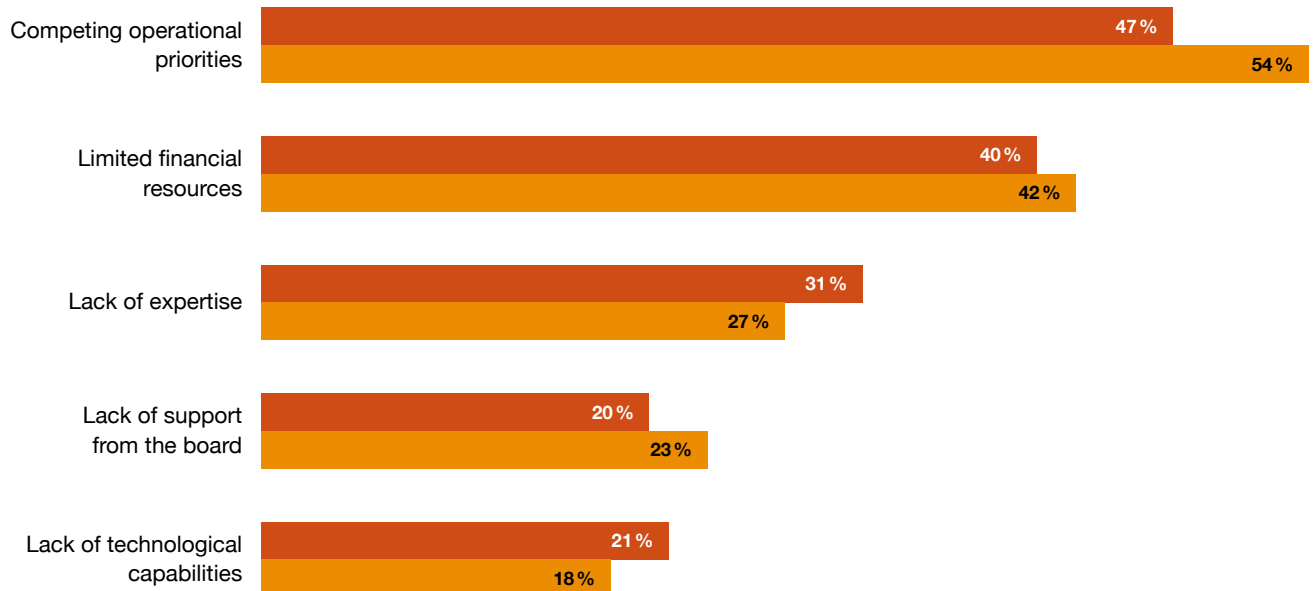
2.

Current challenges and upcoming technological changes

Current challenges

When asked what aspects hindered their Corporate Security from adequately performing its tasks, the views of CSOs and the C-suite were broadly similar. About half of the CSOs and the C-suite, 54 % and 47 %, respectively, somewhat or completely agreed that competing operational priorities are preventing their Corporate Security from adequately fulfilling its responsibilities.

Limited financial resources represented the second biggest challenge, cited by 42 % of CSOs and 40 % of the C-suite. The third most significant hindrance was a lack of expertise, noted by 27 % of CSOs and 31 % of the C-suite. Around 20 % of both groups identified a lack of support from the board and limited technological capabilities as further obstacles.



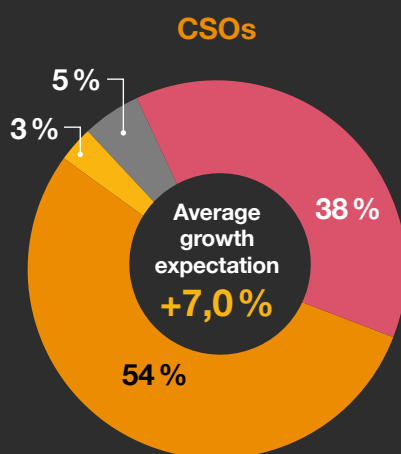
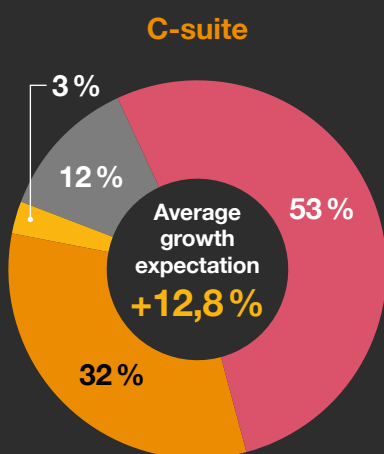
To what extent do you consider the following aspects to be factors that hinder your Corporate Security from adequately performing its tasks?

■ C-suite ■ CSOs

Basis: All companies | Presentation of the 'Top two values': 'Somewhat agree' and 'Completely agree'



Identified as the second biggest obstacle, we asked CSOs and the C-suite how they anticipated their Corporate Security budget would develop over the next two years and by what percentage. While 54 % of CSOs expected no change, only 32 % of the C-suite shared this view. In contrast, 38 % of CSOs anticipated an increase, compared to 53 % of the C-suite. The C-suite was notably more optimistic, projecting an average budget rise of 12.8 % compared to the 7 % expected by CSOs. This optimism from the C-suite could result in additional financial resources to address existing gaps and support further advancements in the area of security.



How do you expect your Corporate Security budget to develop over the next two years? For expected changes: By what percentage?

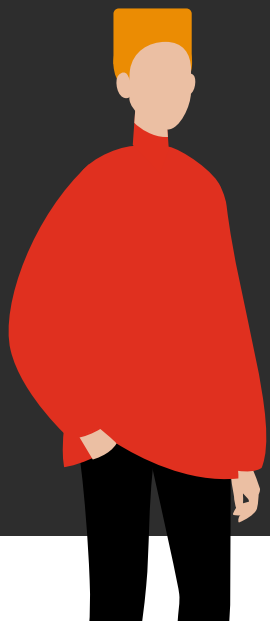
Expected development over the next two years:

- Increase
- No change
- Decrease
- Do not know / No answer

Basis: All companies

Digitisation put to the test

With a potential budget increase, investments in digital solutions could become more feasible. Evaluating digital maturity is crucial, as it will help to determine how Corporate Security can enhance its resilience and strategic capabilities.



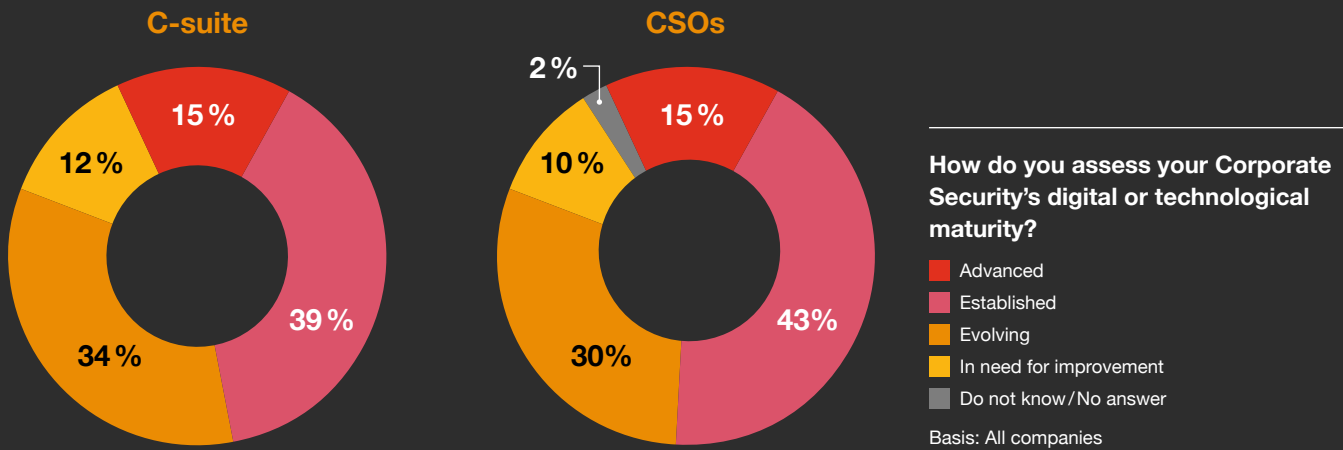
In an ever-evolving field, attracting and retaining top talent is paramount for Corporate Security. Prioritising the upskilling of current employees and implementing job rotation programmes not only enhances team capabilities but also makes Corporate Security more attractive to young professionals seeking dynamic and growth-oriented careers.”

Jens Greiner
Director, Forensic Services, PwC Germany

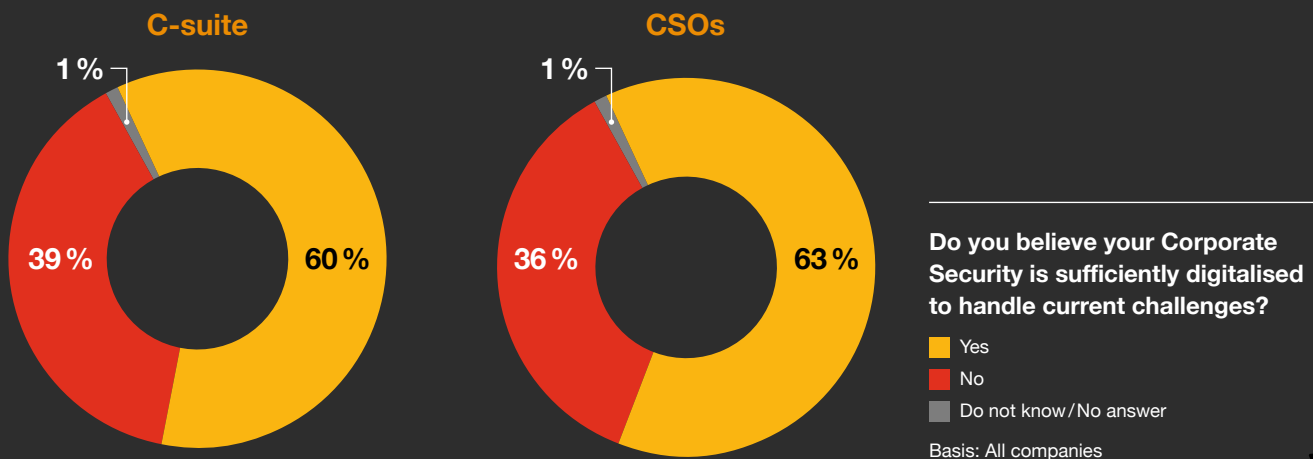


Digital maturity

A lack of technological capabilities was identified as the least significant obstacle; around 20 % of respondents highlighted it as a concern. Overall, both groups were quite confident in their digital or technological maturity: 43 % of CSOs and 39 % of the C-suite considered themselves sufficiently mature rating their digital maturity as 'established' and 15 % of each group as 'advanced'.



When asked if their Corporate Security was adequately digitalised to meet current challenges, 63 % of CSOs and 60 % of the C-suite agreed. This self-evaluation requires a critical review to understand whether it accurately reflects the respondents' actual digital maturity and capability.



Quickly check your Corporate Security's digital maturity:

1

Are current digital tools effectively addressing security challenges, or are there gaps between self-assessment and the actual status quo?

2

How does your digital maturity compare with industry standards and technological trends?

3

Are you investing in emerging technologies to enhance security and efficiency?

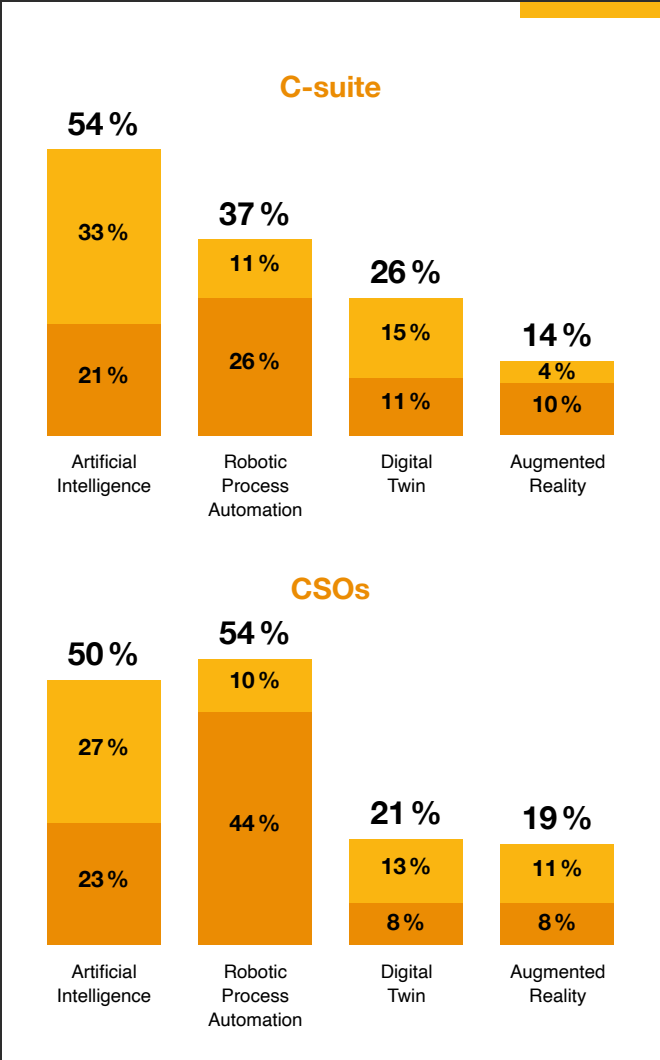


Technology drives Corporate Security

Examining the use of various technologies in Corporate Security revealed some notable contrasts, especially when focusing on the four main technologies: Artificial Intelligence (AI), Robotic Process Automation, Digital Twin and Augmented Reality. While around 20 % of CSOs and C-suite executives stated to use AI in their Corporate Security, and 27 % and 33 %, respectively, planned to do so, over 40 % did not intend to implement it. This highlights a significant divergence in technology adoption plans. Robotic Process Automation was the most widely adopted technology, with 44 % of CSOs and 26 % of the C-suite aware of its use. However, there was a significant discrepancy in perceptions about future use; 61 % of the C-suite stated that the respective technology is neither in use nor planned, while only 43 % of CSOs shared this view.



Surprisingly, 42 % of CSOs and 59 % of the C-suite indicated that they would not pursue any additional technology trends other than the ones already in use and noted in the survey. This finding suggests they believe they are sufficiently digitalised to meet current challenges. It also indicates that CSOs are more open to adopting further technologies than the C-suite.



To what extent is your Corporate Security already using or planning to use the following technologies?

Already in use Planned use

Basis: All companies



While there's confidence in digital maturity, it's intriguing to see a measured stance towards adopting emerging technologies like AI. This raises the question of how well this confidence in digital readiness aligns with a more reserved approach to newer technologies."

Jens Greiner

Director, Forensic Services, PwC Germany

Defining the future role of AI

Despite some reservations regarding AI and other evolving technologies, it is evident that AI will play a crucial role in business in the future. Therefore, it is essential to examine its role and impact on the future of Corporate Security and the associated security risks in greater detail.



3.

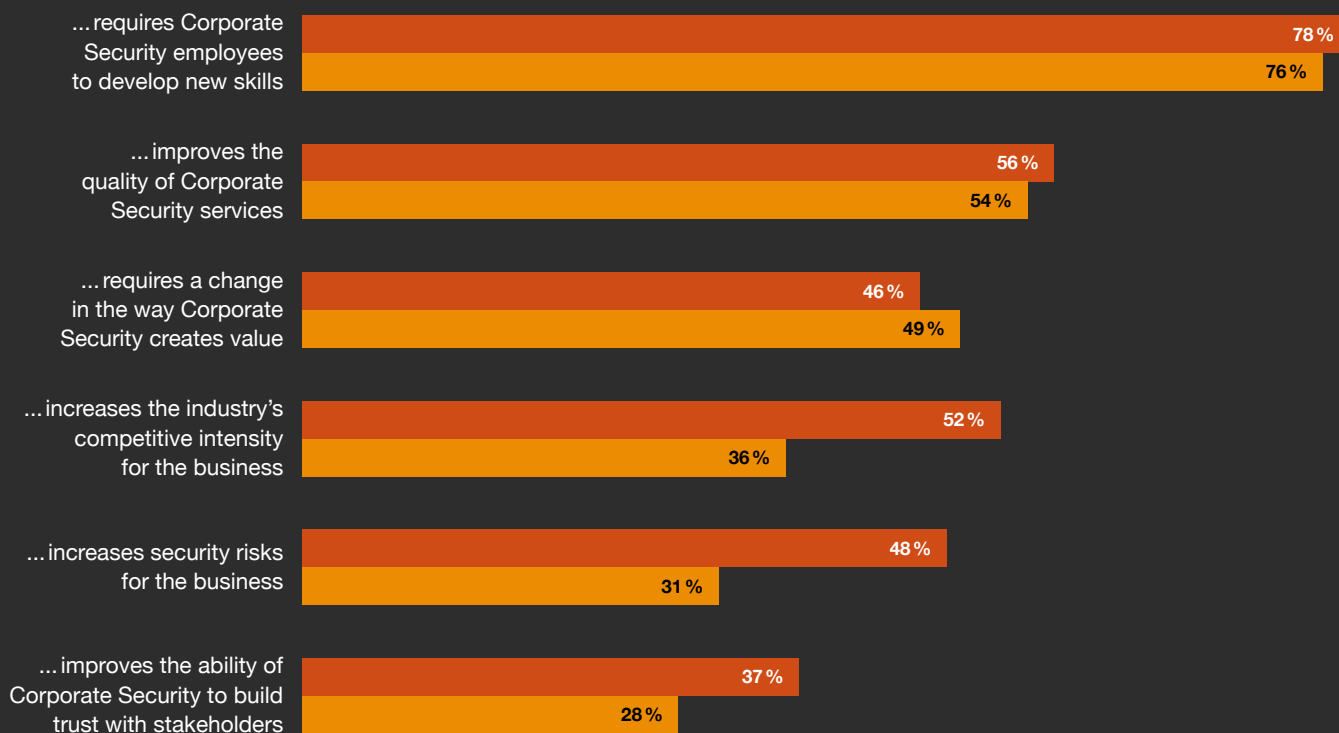
Evaluating AI's role in Corporate Security

Current AI implementation and plans

As mentioned, 50 % of CSOs and 54 % of the C-suite used or planned to use AI, while a significant number of respondents did not plan to implement it (43 % of CSOs and 42 % of the C-suite).

However, there was a consensus on the importance of upskilling employees for effective AI deployment; 76 % of CSOs and 78 % of the C-suite agreed on this point.

The use of Artificial Intelligence...



To what extent do you agree with the following statements regarding using AI in your Corporate Security?

■ C-suite ■ CSOs

Basis: All companies | Presentation of the answers for 'agree' given by CSOs and C-suite

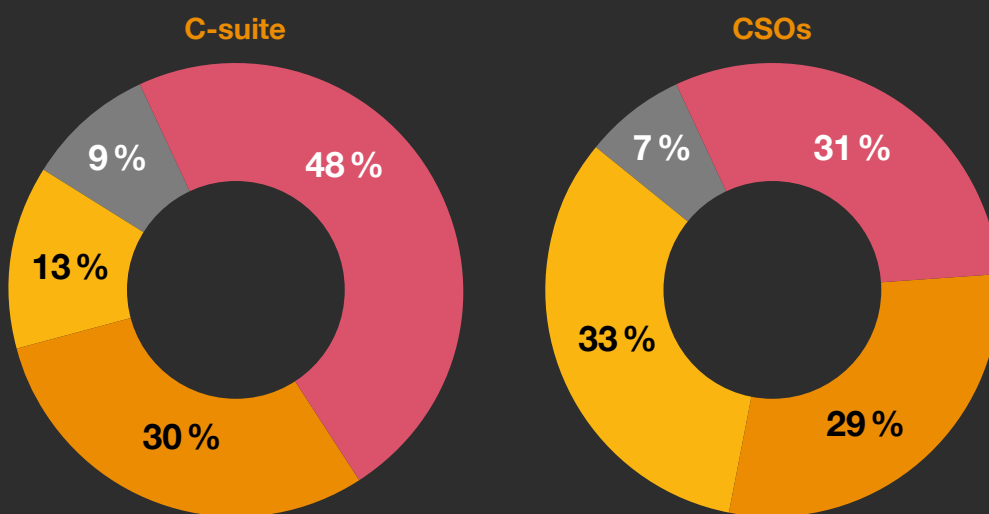
AI as an opportunity for Corporate Security

When considering the impact of AI on industry competition and quality, opinions differed. Over half of the C-suite (52 %) believed that AI would increase competition within their industry, whereas only 36 % of CSOs shared this view, highlighting a notable disparity. Nevertheless, both groups recognised the potential benefits of AI; 54 % of CSOs and 56 % of the C-suite believed that AI would improve the quality of their Corporate Security services.

There were also differences of opinion on perceived security risks. Nearly half of the C-suite (48 %) perceived greater security risks using AI, compared to 31 % of CSOs, indicating a clear difference in risk perception.

Defining the right strategy for AI

While AI presents both opportunities and challenges, it is set to become an integral part of businesses' technological landscape. The critical question is how Corporate Security will integrate AI technologies and solutions and leverage AI in interactions with external partners and service providers. To better understand how Corporate Security can prepare for the use of AI, examining how the C-suite and CSOs approach their risk strategies is crucial.



To what extent do you agree with the statement that the use of AI increases the risks for Corporate Security?

Agree Disagree Neutral Do not know/No answer

Basis: All companies

4.

Risk strategies and upcoming challenges

A risk-averse approach

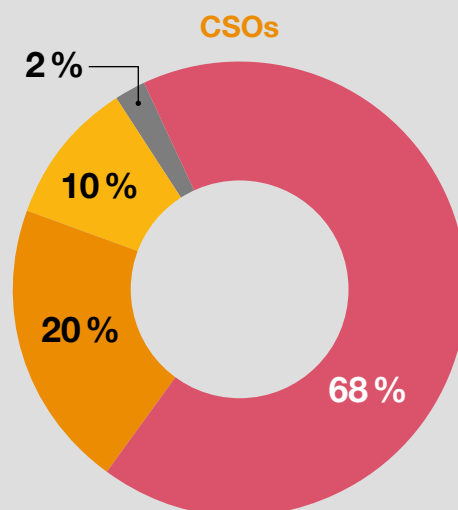
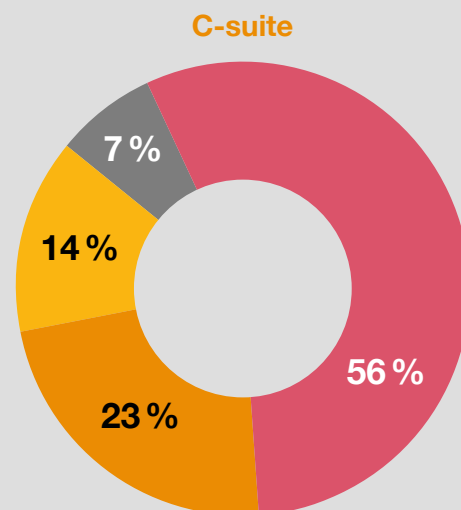
When asked about their strategies for addressing relevant security risks, companies exhibited different approaches. A significant portion — 68 % of CSOs and 56 % of the C-suite, indicated they adopted a risk-averse approach to security risks. Moreover, 20 % of CSOs and 23 % of the C-suite favoured secure options that presented low-security risks, even if those options offered limited return potential.

These findings reveal that the primary goal of both parties is to avoid security risks and uncertainties rather than accept risks for business benefits. Significantly, only 10 % of CSOs and 14 % of the C-suite were willing to embrace innovation and opt for choices that promised potentially greater benefits despite the higher security risks.

Uncertainties leave their mark

As the survey data indicates, Corporate Security is currently more inclined to prioritise managing potential threats over taking risks that could benefit the business. The challenges and uncertainties that have arisen in recent years, the increase in regulatory requirements and economic uncertainties could be seen as factors which support this development.

To gain insights into how this risk-averse approach has translated into practical actions for security risk management, the survey also explored measures implemented by Corporate Security over the past twelve months.



Companies pursue different strategies with regard to relevant security risks. Which of the following statements best describes your approach?

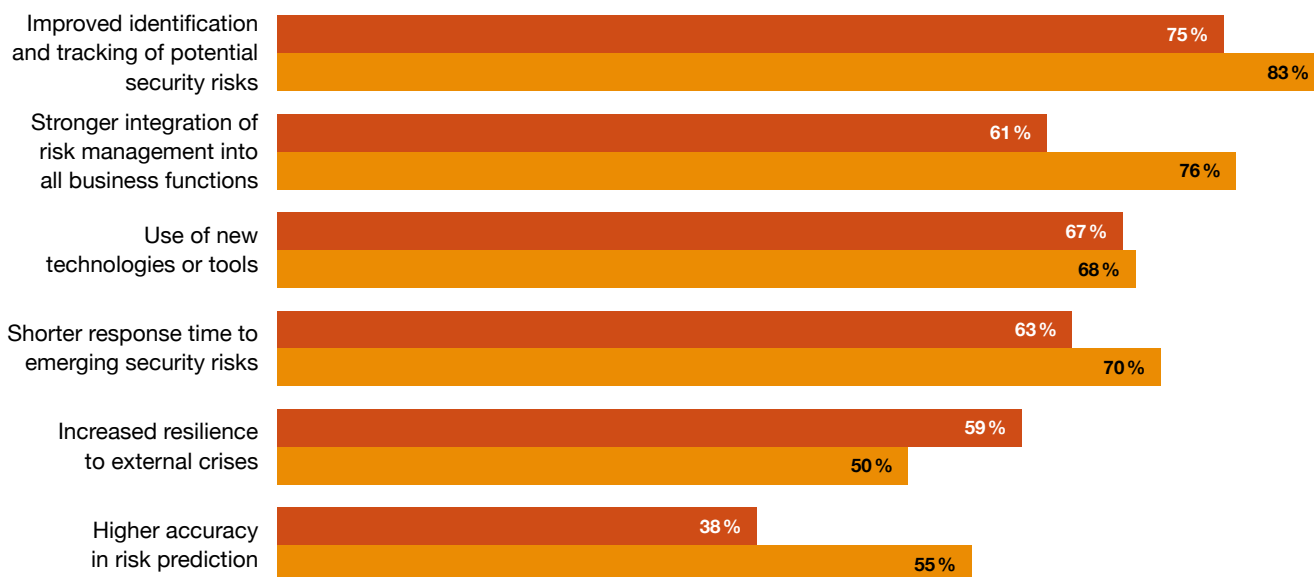
- Our primary goal is to avoid security risks and uncertainties.
- We prefer safe options that pose low security risks and may have limited return potential.
- We are willing to be innovative and choose options that, despite higher security risks, promise potentially greater business benefits.
- None of the above/No response

Basis: All companies

Key measures taken by Corporate Security

Examining the measures implemented over the last twelve months to enhance security risk management reveals significant progress. A sizeable 83 % of CSOs and two-thirds of the questioned C-suite had focused on improving the identification and tracking of potential security risks. Integrating risk management more thoroughly across all corporate functions was a measure taken by 76 % of CSOs and 61 % of the C-suite. Another measure was reducing response times to emerging security risks, which 70 % of CSOs and 63 % of the C-suite highlighted.

Furthermore, 68 % of CSOs and 67 % of the C-suite had adopted new technologies or tools to strengthen their security capabilities. At least half of the surveyed CSOs had implemented all the outlined measures, as had the C-suite, except for improving the accuracy of risk forecasting. This aspect shows a significant discrepancy, where 55 % of CSOs made strides compared to only 38 % of the C-suite. These findings might underscore the proactive steps taken by Corporate Security to strengthen its risk management frameworks.



Which of the following measures has your Corporate Security taken in the last 12 months to improve the management of security risks?

■ C-suite ■ CSOs

Basis: All companies

Bridging the perception gap

While the importance of Corporate Security is recognised, there is a perception gap in communicating the vital measures taken by Corporate Security to improve security risk management. This gap highlights the need for better alignment between the C-suite and CSOs to ensure both parties have a shared understanding of the measures in place and their effectiveness – particularly given the risks businesses will face in the coming years.

Upcoming security challenges

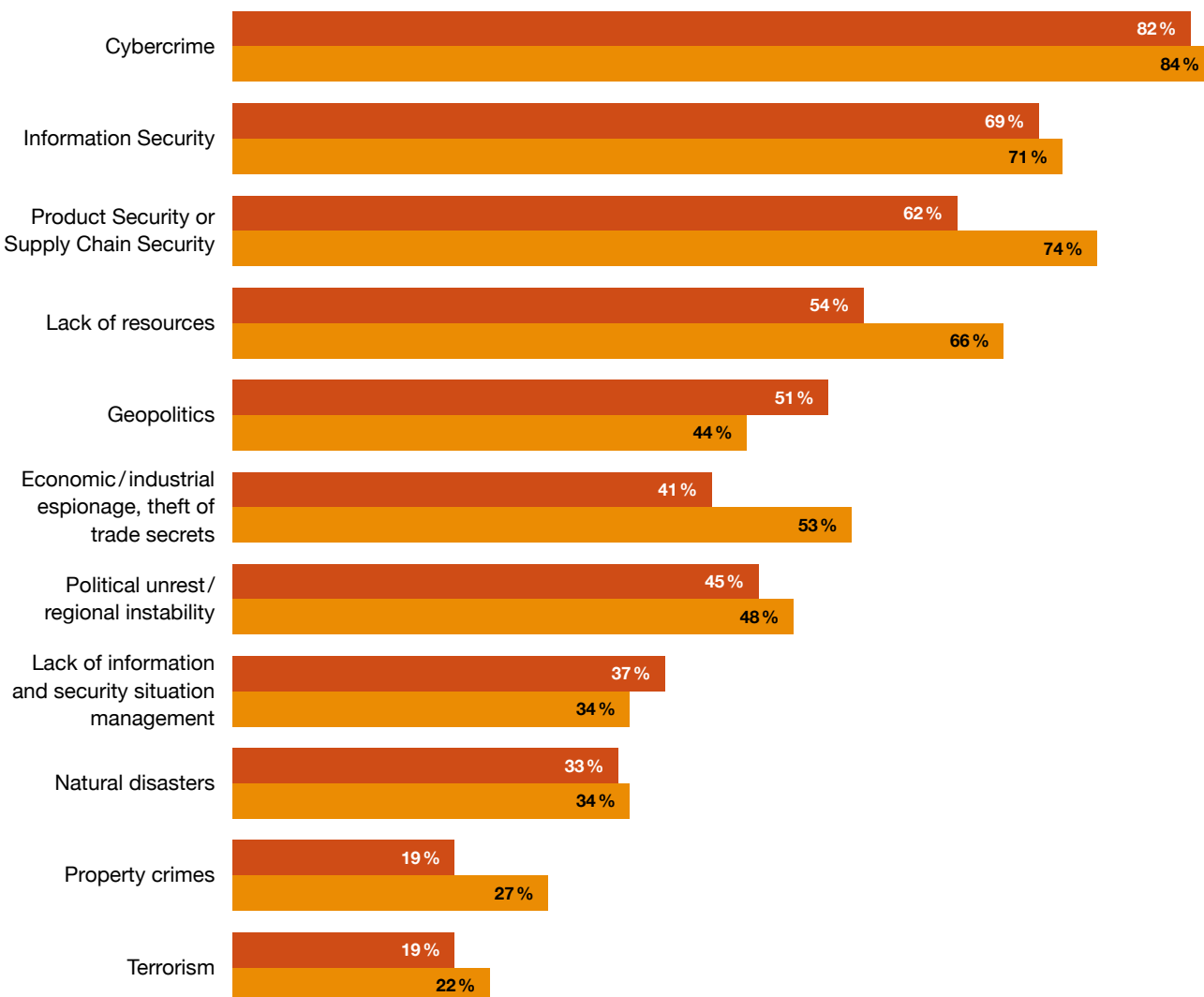
Looking ahead to the next two to three years, CSOs and the C-suite identified similar challenges for their Corporate Security. The foremost concerns were cybercrime (84 % of CSOs and 82 % of the C-suite), information security (71 % of CSOs and 69 % of the C-suite), and product or supply chain security (74 % of CSOs and 62 % of the C-suite). These areas require enhanced attention and robust strategies to mitigate potential risks.

The above highlights the importance of continuous dialogue between CSOs and the C-suite, as well as the development of strategies to address risks and handle the outlined challenges in the next two to three years. Consequently, Corporate Security should further position itself to tackle potential business risks.

The C-suite and CSOs must engage in an open dialogue about challenges and maintain ongoing communication. CSOs should leverage their earned status as business enablers to actively identify business opportunities and drive innovation.”

Jens Greiner

Director, Forensic Services, PwC Germany



What do you think are the biggest challenges for your company's Corporate Security in the next two to three years?

■ C-suite ■ CSOs

Basis: All companies

5.

Conclusion

Corporate Security emerges in the executive spotlight. Long perceived as merely a reactive force, Corporate Security has proven itself as both a business enabler and a crisis responder. This dual role strengthens its position within organisations and boosts its appeal to talent.

Corporate Security is confident that its attractiveness to young talent is comparable to that of other corporate functions. The focus on retaining talent before external recruiting also emphasises the conviction in Corporate Security's own capabilities and importance. It is questionable whether Corporate Security is also seen as attractive outside the organisation. In order to remain competitive, the aforementioned areas of development should also be addressed in the coming years.

To maintain its positive standing and remain effective, Corporate Security must prepare for upcoming challenges effectively. The primary challenges identified by CSOs included conflicting operational priorities, limited financial resources, and a lack of support from the executive board.

However, insights from the C-suite indicate a rather optimistic outlook regarding potential increases of Corporate Security budget. The possibility of a growing budget may offer CSOs with opportunities to invest in, for example, digital solutions, talent upskilling, and other initiatives, which could be beneficial for addressing current and future challenges. By aligning strategies with these potential financial prospects, Corporate Security can aim to strengthen its role as a key component of business strategy.

Most of the CSOs and C-suite executives surveyed believed their Corporate Security was sufficiently digitalised to handle current challenges. However, this perspective requires critical evaluation to confirm that these beliefs reflect their organisations' actual capabilities. Both CSOs and the C-suite recognised

opportunities and risks associated with using AI. Notably, the C-suite perceived greater security risks with AI than the CSOs. Whether Corporate Security is indeed 'sufficiently' digitalised to meet future challenges effectively remains to be seen. Reflecting on the numbers from the first Corporate Security Benchmarking Survey in 2022, it is evident that CSOs and the C-suite have significantly aligned in their perspectives, reaching consensus on most key issues. This closer alignment highlights a growing mutual understanding and shared vision between these two crucial groups.

Corporate Security has indeed taken the next step from its status as a business enabler into the executive spotlight. In the coming years, it will be intriguing to observe if Corporate Security will drive a resilience management revolution by uniting multiple resilience domains under a single framework or if there will be a stronger convergence between Corporate Security and Cyber Security – or perhaps another path entirely.



Unleash the full potential of your Corporate Security – reach out now.

Contact



Jens Greiner

Director, Forensic Services,
PwC Germany

Friedrich-Ebert-Anlage 35-37
60327 Frankfurt am Main

Tel: +49 69 9585-5831

Mobile: +49 175 353 2089

Email: jens.greiner@pwc.com



© October 2024 PricewaterhouseCoopers GmbH
Wirtschaftsprüfungsgesellschaft. All rights reserved.

In this document, "PwC" refers to PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, which is a member firm of PricewaterhouseCoopers International Limited (PwCIL). Each member firm of PwCIL is a separate and independent legal entity.

