ECSO
CISO
Community

June 2024 v1.0

INSIGHTS FROM THE ECSO CISO COMMUNITY

CYBERSECURITY BUDGETS: OWNERSHIP, REPORTING, TRENDS

ECSO CISO COMMUNITY
ECSO WORKING GROUP ON
CYBER THREAT MANAGEMENT

ecs-org.eu

DISCLAIMER

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Third-party sources are quoted as appropriate. ECSO is not responsible for the content of the external sources, including external websites referenced in this publication.

COPYRIGHT NOTICE

ABOUT THE ECSO CISO COMMUNITY

The ECSO CISO Community hosts **Chief Information Security Officers (CISOs)** and other cybersecurity experts working closely with CISOs (excluding cybersecurity managers responsible for sales of services or solutions), from all across Europe and sectors. Its objective is to promote the **exchange of information**, good practices, threat intelligence, and to develop **common positions** of cybersecurity practitioners. To achieve this, the ECSO CISO Community provides regular discussions on topics of general interest to CISOs with a variety of backgrounds and experience levels. The ECSO CISO Community is an initiative of the ECSO Working Group on Cyber Threat Management.

ABOUT THE CYBER THREAT MANAGEMENT WORKING GROUP

The ECSO Working Group on **Cyber Threat Management** provides support to organisations in tackling cyber threats in collaboration with **industry leaders** in areas of strategic importance like **cyber threat intelligence** and **EU cybersecurity policy** implementation.

ABOUT ECSO

The European Cyber Security Organisation (ECSO) is the non-profit membership-based organisation working for a more **resilient** and **strategically autonomous** Europe. Established in 2016, ECSO unites more than **320 stakeholders**, including companies of all sizes, research centres, public administrations, and many more. Organised in working groups supporting key industry areas, ECSO provides a platform for cooperation, informed decision-making, and **public-private collaboration**.

**EMPOWERING
EUROPEAN
CYBERSECURITY
COMMUNITIES**

KEY TAKEAWAYS

REPORTING STRUCTURE

1

The survey results show that 47% of CISOs report to the CIO or CEO. It's worth noting that when asked about their preference, 53% of respondents would rather report to the CEO, than to any other possible stakeholder. 78% of all respondents indicated that they are positioned at most 2 steps away from the CEO in their organisation. Lastly, some respondents suggested a risk committee as the best reporting body for the CISO.

BUDGET ACCOUNTABILITY

2

As for the budget accountability survey reveals that 45% of respondents believe that the most effective approach for determining cyber security budgets is the establishment of a Cyber Security Budget Committee, with 32% of respondents indicating openness to this strategy. However, only 26% of respondents currently have such a forum in place, leaving the majority of decision-making power within the line organisation. Over half of the CISOs are currently responsible for the IT security budget, with 64% indicating a desire to assume this accountability.

BUDGET OWNERSHIP

3

In terms of budget ownership, 47% of respondents indicated that their funds are part of the CIO budget, while 45% operate with a budget independent of the CIO. When asked about their preferences, 70% of respondents expressed a preference for a separate CISO budget from the CIO budget. In contrast, only 17% of respondents favored integration into a broader IT budget.

CERTIFICATIONS

4

Approximately half of the CISOs bears the costs of generic certifications and new cyber regulation change program costs. It is notable that 15% of CISOs are already bearing the financial responsibility associated with business line-related certification instruments.

SECURITY TOOLS

5

The costliest technologies for CISO teams are penetration testing tools, security awareness platforms, SIEM/SOAR and cyber security risk management, each owned by over 85% of teams. Despite 50% of CISOs owning data loss prevention (DLP) solutions, only 30% believe they should, contrasting with a stronger desire to increase their role as a Business Data Guardians. Additionally, CISOs show a clear desire for newer technology solutions like DevSecOps tools, cyber ranges, IoT, and GRC tools.

COST MANAGEMENT

6

Many CISOs aim to reduce incident response costs due to their unpredictability. This could indicate a need for more cost-effective incident response solutions or strategies.

RECOMMENDATIONS

RECOMMENDATION 1

Given the upward trend of CISOs reporting directly to CIO or CEO, it is crucial for organisations to assess their communication structure and identify ways to strengthen the strategic role of the CISO while optimizing the efficiency of the organisational structure.

RECOMMENDATION 2

It is recommended that organisations proactively establish a Risk Committee as a key stakeholder body to leverage its strategic advantages and critical relevance. Doing so can significantly enhance risk management frameworks and drive sustainable business growth.

RECOMMENDATION 3

Given that many CISOs operate with a budget independent from the CIO and have expressed a desire for this separation, it would be advisable for organisations to allocate a separate budget for CISOs. This approach would enable CISOs to manage IT security budgets more effectively, resulting in enhanced security measures, improved resource allocation, and greater accountability.

RECOMMENDATION 4

It is in the best interests of organisations to not only acknowledge but also actively support CISOs in their desire to own more Dev/Sec/Ops tools, cyber ranges, IoT, and GRC tools. Proactive support is essential for CISOs to stay ahead of cyber trends and respond swiftly to situational shifts, thereby significantly enhancing the organisation's overall security resilience.

RECOMMENDATION 5

In light of the CISOs objective to minimize unpredictable incident response expenses, it is recommended that organisations provide assistance in identifying and implementing more cost-effective incident response solutions or strategies.

INTRODUCTION

1.

1.1. Context and objective

The purpose of this survey analysis is to provide CISOs and their corresponding organisation's stakeholders with a broader perspective and better understanding on the ownership, cost reporting and budgets structure in the cybersecurity area. The responses provide valuable insights on existing practices and desired changes in cybersecurity cost reporting. A unique aspect of this survey is a focus on comparing the current situation of respondent organisations with what CISOs would like to see. This survey aims to answer pivotal questions such as:

- Which labour costs should be counted as cyber costs?
- What is the status of cyber cost reporting in your organisation?
- Which tools, services and capabilities related costs are counted as cyber costs?

The objective of this survey is to raise awareness on cybersecurity cost reporting and to enhance general knowledge among the interested public.

1.2. Questionnaire and sample overview

This analysis is based on the results of a survey containing 21 questions. The data consists of answers provided by 47 CISO respondents, who are members of the ECSOs CISO Community. The preliminary phase consisted of a sample distribution analysis of the size and sector of each company.

The largest group to participate in the survey - 40%, are respondents whose companies employ between 1.000 – 10.000 employees. The second largest group of participants with 28% of respondents were representatives of companies with less than 1000 employees. Not far behind with 23%, companies with more than 25.000 employees. Finally, the last group, equivalent to 9% of participants, were representatives of companies in a range between 10.000 and 25.000 employees.

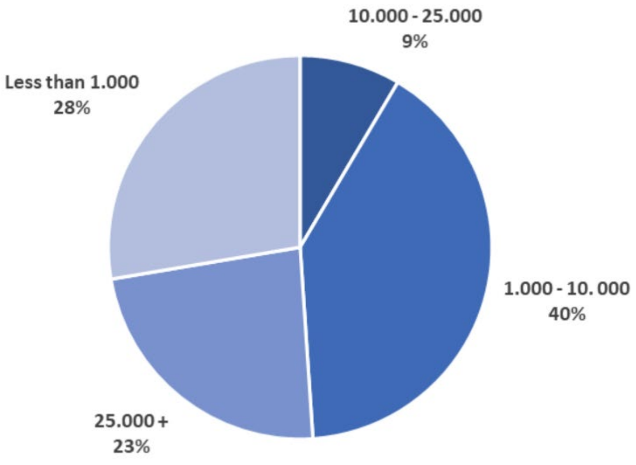

Figure 1

As for the company's origin, the participants represent 13 different sectors, with 4 companies present in multiple sectors. The most common sector, with 23% of respondents is manufacturing, whereas 13% belong to the technology/ICT sector. Equally with 11%, the financial and energy sector. Participants whose companies are present in multiple sectors correspond to 8%. Both transport and public administration/education/research sectors represent 6% each. As for the food industry, health care, retail and telecommunication, they represent 4% each. The legal and media sectors represent 2% (each).

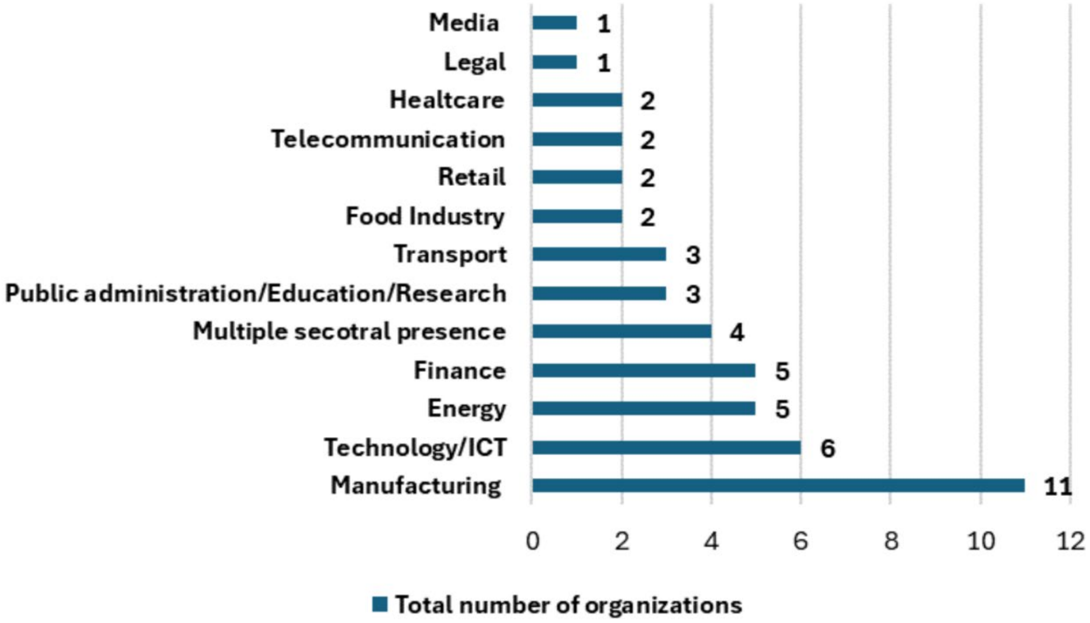

Figure 2

STANDARDISING CYBERSECURITY

2.

Understanding cybersecurity cost reporting relies on discerning the reporting channels and senior executives to whom CISOs deliver insights. Our survey reveals that 47% of CISOs report directly to either the Chief Information Officer (CIO) or the Chief Executive Officer (CEO). Beyond these two C-level roles, the rest of the CISOs indicated reporting to 25 different stakeholders i.e. COO or CRO. Moreover, when the CISOs are not reporting to either CEO or CIO, the most common CxO responsible for the cyber risk is the Chief Technological Officer (CTO). Furthermore, 78% of the respondents indicated that, in their organisation, they are positioned maximum 2 steps away from the CEO.

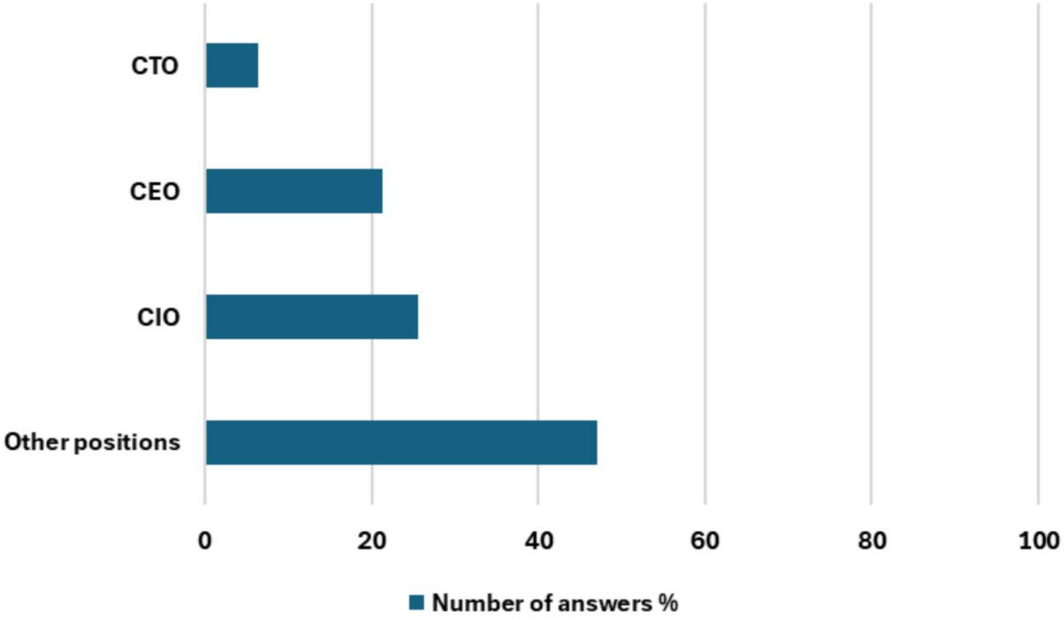

Figure 3
Where does the security function report to in your organisation – the title of the direct superior?

The data reveals a lack of consensus on the optimal reporting structure for the CISOs. Respondents suggest that the ideal reporting line should be tailor made and taking under considerations various unique factors, such as the company's maturity level, size, or operational sector. When asked about their preferred reporting structure, only 9% of respondents indicated that the CISO should report to the CIO. In contrast, 53% of respondents believe the CISO should report directly to the CEO. This preference may be driven by a desire to prioritize information security at the highest levels of the organisation, ensuring it receives the necessary attention and resources. By having the CISO report directly to the CEO, information security becomes a top priority, integrated into the strategic decision-making process. This alignment can lead to more resilient security policies, better resource allocation, and a stronger overall security posture. Additionally, it emphasizes the importance of cybersecurity as a critical business function, rather than just a technical issue, fostering a culture of security awareness and accountability across the organisation. It's worth noting that 17% are open to the CISO reporting to any C-level executive, while 21% believe the CISO should report to a collective body, such as the Board of Directors or Executive Committee.

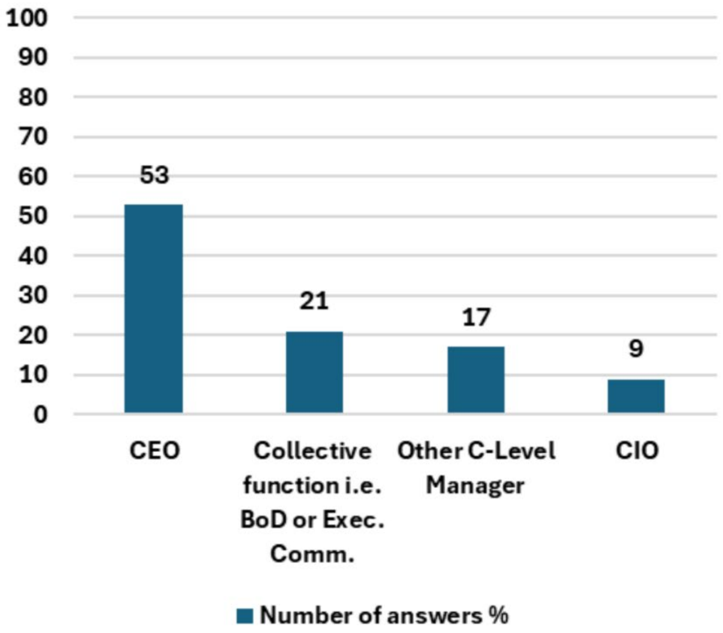

Figure 4
Where should the security function report to (how would you like to see it)?

In response to being asked whether their respective organizations have a dedicated Cybersecurity Budget Committee, only 26% of respondents indicated that such a committee is in place. This suggests a significant discrepancy between the desired (by CISOs) organizational structure and actual situations in many organizations. In the remaining companies, decision-making authority is primarily vested in the line organization, following traditional reporting structures. This can result in a lack of cohesion in decision-making processes and slower responses to emerging cyber threats. In the absence of a dedicated cybersecurity committee, organisations may encounter difficulties in distributing resources effectively, defining security priorities and formulating a well-integrated cyber strategy.

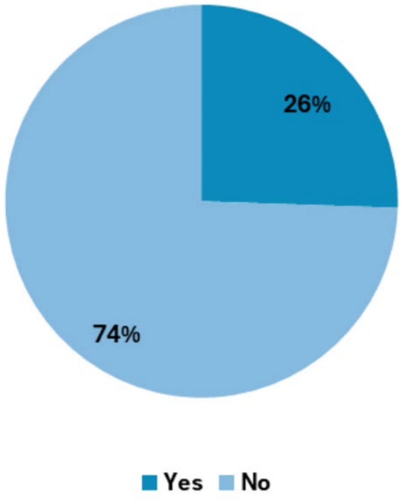

Figure 5
Does your company have an established Cybersecurity Budget Committee?

In contrast with the aforementioned situation, 45% of respondents believe that their organisation would benefit from the establishment of a Cybersecurity Budget Committee. This suggests a preference for a specialized, collaborative forum to make informed decisions about their cyber security operations and investments. Such a committee can bring together diverse expertise and perspectives, ensuring that budget allocations are strategically aligned with the organisation's security needs and priorities. Interestingly, an additional 32% of respondents are open to this idea, indicating a potential shift towards this model in the future. However, 23% of respondents believe that companies should not have Cybersecurity Budget Committees, suggesting that the current organisational structure is adequate or that alternative approaches could be adopted for managing cybersecurity budgets.

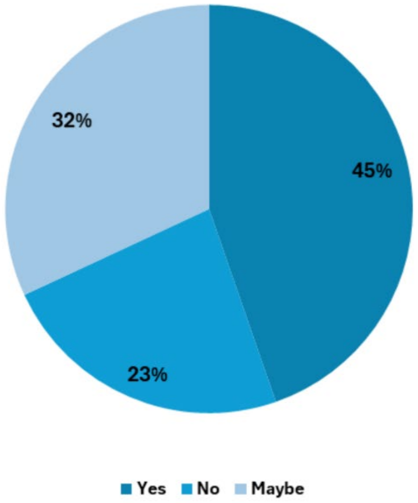

Figure 6
Do you think companies should have Cybersecurity Budget Committee (how would you like to see it)?

Where a Cybersecurity Budget Committee[1] was present, it typically consisted of the CEO, CFO, and CIO. It is essential to emphasize that the survey results revealed a variety of combinations without a clear trend. Therefore, the composition of these committees can vary widely based on the specific needs and structure of each organisation. As for the frequency of committee meetings, the answers did not provide a clear picture or trend indication. Results ranged from quarterly to annual meetings. Nevertheless, collected data allowed for the formation of the following diagram.

[1] It is our understanding that such a dedicated Cyber Security Budget Committee, could at the same time fulfil the role of a Risk Committee.

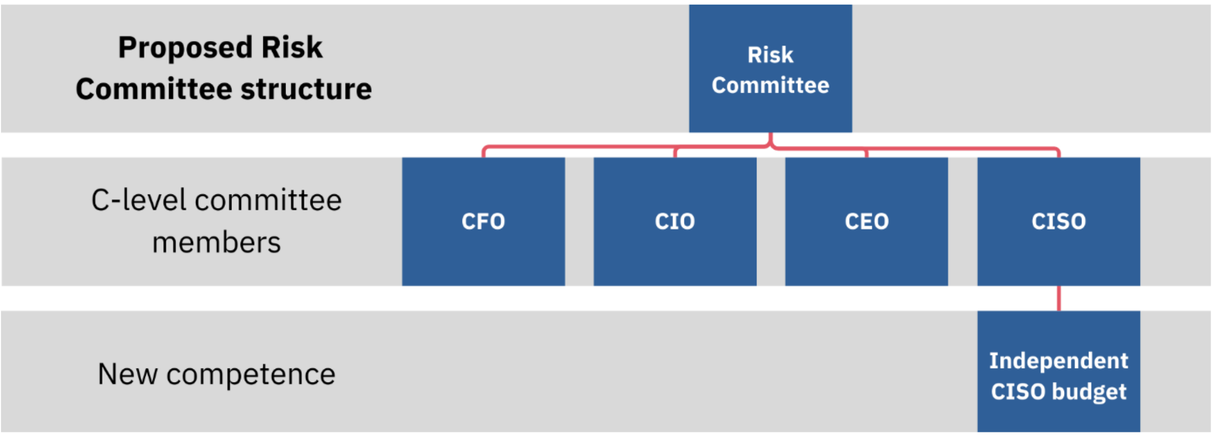

Figure 7

In terms of budget ownership, 47% of CISO budgets are part of a broader budget under the CIO. In contrast, 45% of respondents indicated that they have a budget that is independent of the CIO. Only 8% of respondents have a budget organised in a different way, despite the lack of further details provided. This distribution indicates that organisations are receptive to a more decentralized approach to cybersecurity funding. The advantages of separating IT and cybersecurity include improved financial supervision and more effective cyber problem-solving. However, it could be argued that the centralized approach allows for easier management of assets and simplifies the organisation structure that addresses IT topics without favouring any particular area.

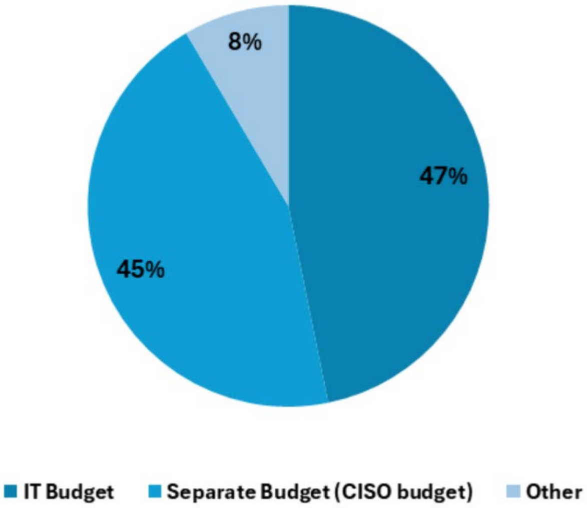

Figure 8
Is cyber a separate budget (CISO budget) or part of the IT budget in your organisation?

When asked about their preference, 70% of respondents favoured establishing of the "CISO budget" as a standalone fund. Conversely, only 17% of respondents indicated that their budget should be integrated into a comprehensive IT budget and the remaining 13% of respondents indicated that they would prefer an alternative organisational structure for the CISO budget.

This preference for a standalone structured CISO budget suggests a desire for greater autonomy and flexibility in managing cybersecurity resources. It also highlights a strategic inclination towards more specialized and focused allocation of funds, ensuring that cybersecurity initiatives receive dedicated attention and resources.

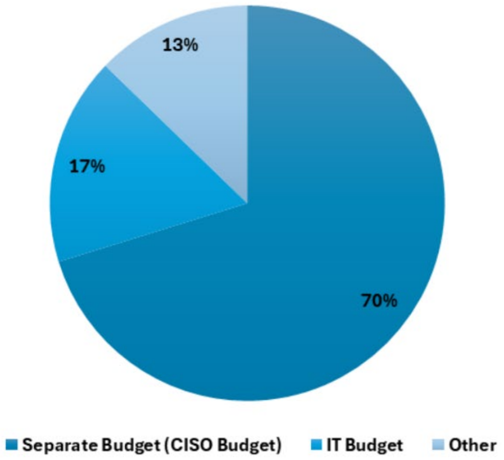

Figure 9
Is cyber a separate budget (CISO budget) or part of the IT budget

The survey results indicate that approximately 50% of CISOs are responsible for bearing the expenses associated with standard certifications. Furthermore, the results highlight the financial implications of programs modified to comply with evolving cyber regulations, underscoring the industry's heightened focus on regulatory compliance. It is noteworthy that 15% of CISOs currently bear the financial responsibility for business-line-related certification programs, with a significant proportion expressing interest in expanding their portfolio. This indicates that CISOs are willing to assume this responsibility, potentially to enhance their comprehension of and capacity to oversee risks pertinent to their respective businesses. By expanding their portfolio, CISOs can gain deeper insights into various business-line operations, improve their ability to manage sector-specific risks, and ensure that their organisations remain compliant with evolving regulatory standards. This proactive approach not only strengthens the organisation's overall security posture but also demonstrates the CISO's commitment to integrating cybersecurity with broader business objectives.

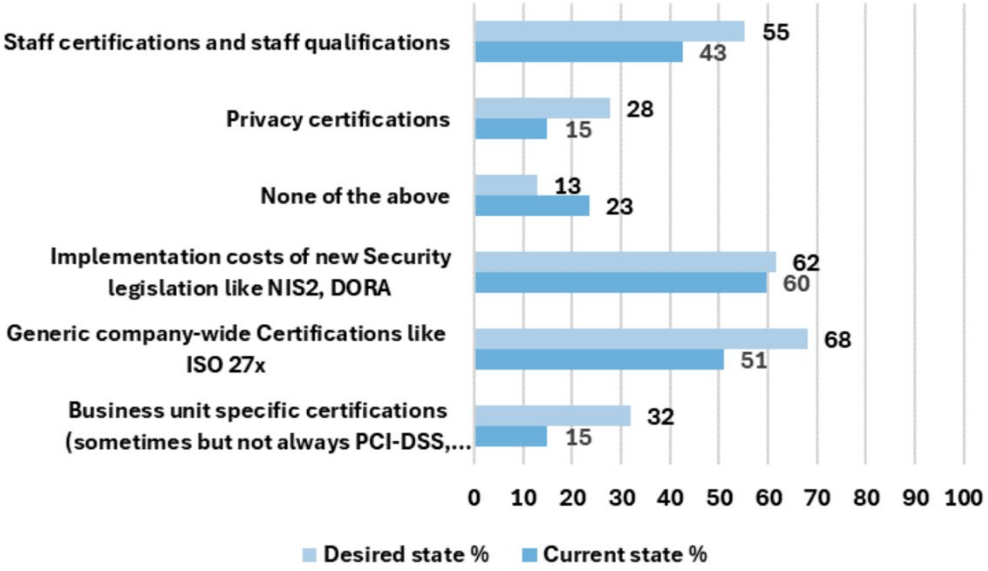

Figure 10
Which Certifications do CISO teams own pay for and how would they like to see this changing?

Furthermore, respondents were asked to indicate their current and desired position with respect to the inclusion of specific IT-related topics in the CISO budget. The responses received demonstrate that there is a clear desire among CISOs to exert greater control and influence over a range of IT-related matters. Over half of the respondents (53%) currently have responsibility for the IT security budget, and 63% indicated a preference for assuming responsibility for an IT security budget. The most significant change is with regard to the CISOs fulfilling the role of Business Data Guardians. At present, only 2% of respondents indicated that they are currently accountable for this cost, whereas 15% expressed a desire to assume this responsibility in the future. This indicates an increasing desire among CISOs to be more closely aligned with the business. A comparable trend is evident with regard to OT-Security teams, where 21% of CISOs currently bear accountability, yet 32% have indicated a desire to assume this responsibility in the future.

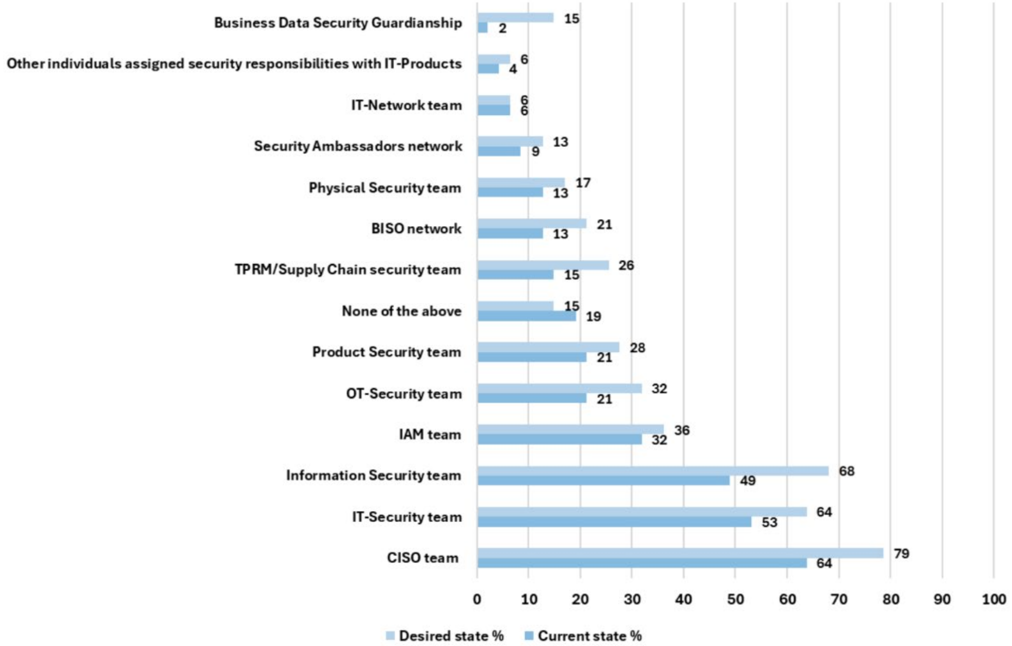

Figure 11
Which costs are currently included in the CISO budget, and which costs should be considered for future inclusion?

Finally, the study offered valuable insights into the technologies that CISOs have budgeted for and utilised, as well as their aspirations for change. The most prevalent technologies in CISO team portfolios are penetration testing, security awareness, and SIEM/SOAR, which are included in over 85% of these portfolios. However, the survey results also highlight some noteworthy trends in the aspirations of CISOs for change. Currently, 50% of CISOs own DLP solutions, yet only 30% believe they should continue to own them. In addition to that, some CISOs have expressed a desire to eliminate security awareness and training exercises. It seems that the need for human risk reduction may become less crucial with the introduction of more sophisticated technical solutions. Moreover, the greatest discrepancy between the current and desired states can be observed in relation to incident response. At present, 79% of respondents are responsible for the cost, but only 51% would like to retain this responsibility in the future. This discrepancy can be attributed to the inherent volatility and forecasting challenges associated with this cost.

This is in contrast with the clear desire among CISOs to assume greater responsibility for DevSecOps tools, Cyber Ranges, IoT, and CRG tools. The discrepancy between the current and desired states with regard to the aforementioned technologies is greater than 15%. When all of these changes are taken into account, it is evident that CISOs have a need to transition towards more advanced technological solutions. That shift could potentially provide greater predictability and reliability without compromising the cyber security standards of their organisations.

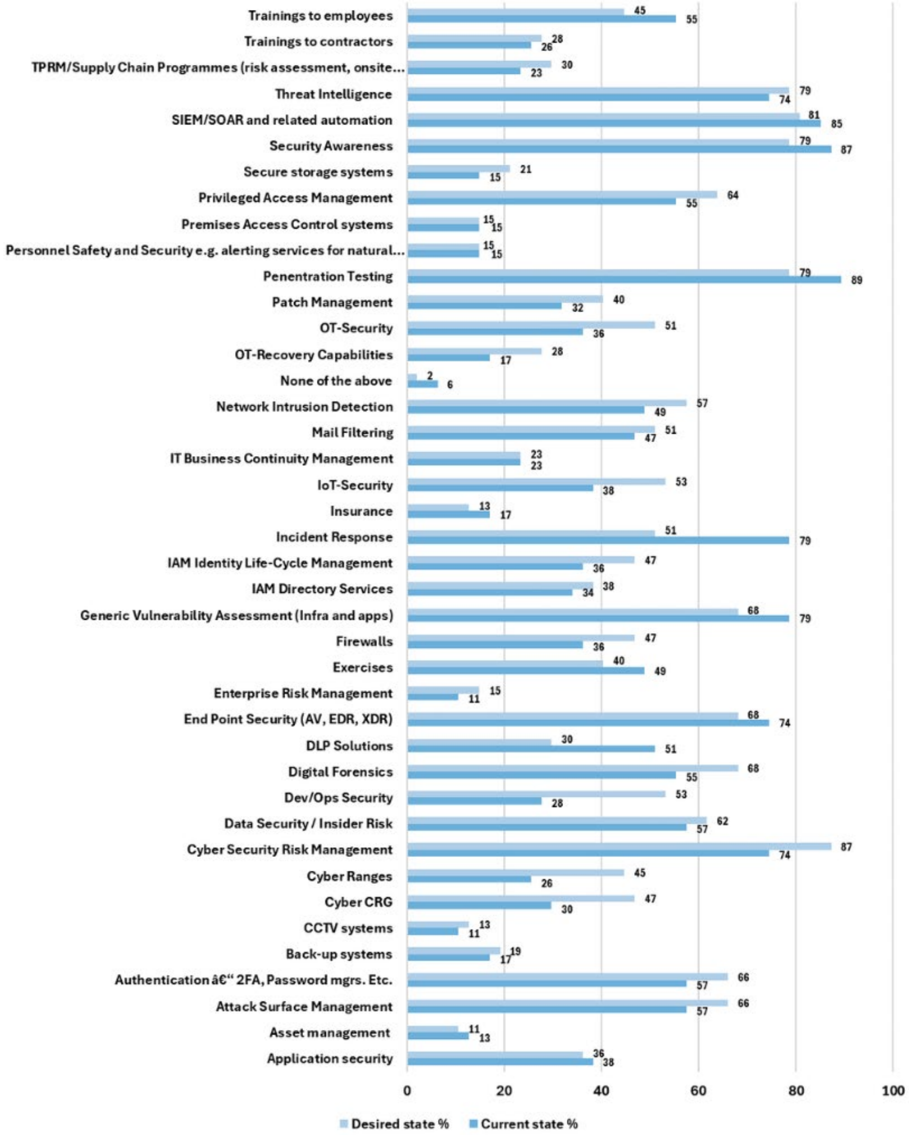

Figure 12

What technologies do CISOs currently "own" and where should potential changes be implemented?

ECSO CISO Community

Avenue des Arts 46, 1000, Brussels (Belgium)
tomasz.michalowski@ecs-org.eu
www.ecs-org.eu