An exploration into the requirements and responsibilities of CISO roles: Balancing art with science

Moufida Sadok[1] and Iain Reid[2]

[1] School of Criminology and Criminal Justice, University of Portsmouth, UK
[2] School of Criminology and Criminal Justice, University of Portsmouth, UK

Abstract

This paper presents the results of an investigation into 50 Chief Information Security Officer (CISO) job openings listed by various organisations in the UK from 2022 to 2025, aiming to identify the essential and desirable skills required by employers. The findings indicate a growing demand for both soft skills and established security certifications, such as the Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM). Furthermore, the requirements and responsibilities emphasise the key role of the CISO in aligning security with business needs, which necessitates a good understanding of business processes that support the delivery of value, as well as work practices to enhance security engagement in the workplace. This study has the potential to inform future educational and training programmes in security to close the skills gap.

Keywords

CISO, Soft skills, Hard skills, Information security, Sociotechnical approach, Job description

1. Introduction

The ubiquitous digitisation of information and the pervasive connectivity of work systems have made securing information essential to ensure business continuity, sustainability, and compliance with regulatory frameworks. The International Standards Organisation (ISO) 27001:2022 [1] recommends organisations to implement an information security management system, based on a business risk approach, including policies, procedures, guidelines, activities and associated resources, to maintain and improve the security of information assets. The Chief Information Officer (CIO), also referred to as the Chief Information Security Officer (CISO), is responsible for every aspect of information security management and is expected to advise on how to leverage technology to address an organisation's security needs. The role of CISOs is pivotal to ensure an effective security strategy supporting business model operations; therefore, it requires certain personal and professional qualifications to meet the demands of the position successfully.

The recent incidents involving CISOs from Huber and SolarWinds have raised questions about the liability of CISOs. The U.S. Securities and Exchange Commission has charged SolarWinds Corporation and its former CISO with fraud and internal control failures related to the company's cybersecurity practices leading up to the 2020 cyberattack [2]. Although the charges against them were subsequently dismissed, this case still shows the challenges in identifying who should be considered

The 11th International Workshop on Socio-Technical Perspectives in IS (STPIS'25) September 17-18, 2025 Skopje, North Macedonia.

[1] Corresponding author: Mou ida Sadok

mou ida.sadok@port.ac.uk
0000-0003-2981-6516 (M. S); 0000-0003-4072-7557 (I. R)

CC-BY logo and © 2025 Copyright for this paper by its author(s). Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0)

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2025-12-20

CEUR-WS.org/Vol-4134/paper5.pdf

liable when under a cyber-attack. In May 2023, a former Uber CISO was fined and sentenced to three years' probation after being the first cybersecurity executive to be convicted of covering up elements of a data breach perpetrated by external attackers [3]. These incidents also raise questions about the applicability of the parity principle of authority and responsibility, as CISOs seem to lack the required autonomy and decision-making authority to run and maintain an effective information security management system. CISOs are seen as being answerable to the C-Suite, rather than being part of it, with Da Silva et al. [4] arguing that CISOs "are often scapegoated when things go wrong".

This paper aims to identify the qualifications required to fulfil the job of a CISO. It presents a content analysis of 50 job postings from different organisations between 2022 and 2025 in the UK. The study of job listings offers a comprehensive overview of the key skills employers expect. The longitudinal approach to data collection has the potential to identify patterns in terms of required qualifications and skills.

This paper is organised as follows. The next section provides some background on the role of CISO. Section three details the study and data collection. The last section discusses the results and provides some concluding remarks

2. Background

It is widely acknowledged that the CISO is a key player responsible for developing and implementing a security strategy that supports the delivery of business value. This involves an effective assessment of significant risks and the development of a security policy that mitigates or prevents them from impacting the continuity of the business. Further, the CISO must ensure that security measures comply with privacy and regulatory frameworks.

The importance of the CISO role is continuously growing. The research by Karanja [5] investigating the role of CISOs before and after an IT security breach shows that hiring a CISO was a key element in a reactive plan. Maynard et al. [6] argue that there are five requisite dimensions to the strategic role of the CISO: (a) dimension of thought reflecting the ability to be creative and innovative to keep up with the evolving and uncertain threat landscape; (b) dimension of contextualisation which involves the ability to achieve an appropriate alignment between security strategy and the business model requirements; (c) dimension of execution which involves the ability to use efficiently available resources to implement an actionable security plan; (d) dimension of response reflecting the ability of a CISO to be proactive and responsive to significant changes in the business environment; and (e) dimension of advocacy which involves the ability to effectively communication the relevance of security controls to different groups of stakeholders.

Complementary skills, alternatively known as soft skills, are considered highly important within the UK cyber sector, with 28% of respondents rating them as essential in the Cyber Security Skills in the UK Labour Market 2024 [7]. However, 34% of businesses report that they have a complementary skills gap within their organisation. Whilst such soft skills are often seen as being necessary within the role of a CISO, they may not always be listed in job adverts [8]. Within a Dutch context, whilst soft skills are valued by CISOs, they may not always be explicitly stated in job adverts. This, in turn, may create a potential mismatch between what organisations are advertising for in the role of a CISO and what CISOs' experience of the job actually is. By being more explicit in job adverts regarding the need for soft skills then better recruitment decisions may be made, including ensuring that applicants know what their responsibilities will be in the role of CISO [8].

Information security research has also focused on the need for effective communication of the relevance of security controls to employees involved in implementing those controls in their everyday work practices ([9]; [4]; [10]; [11]). The CISO role may further be seen as a mediator, facilitating communication between technical employees and higher levels of management ([10]; [12]). Hooper and McKissack [13] question the technically-oriented job descriptions of CISOs and suggest that CISOs should play a key role in matching security to business requirements. This entails both a broad understanding of business processes supporting the delivery of value and strong communication skills needed to work effectively with different groups of stakeholders, including managers, business process owners and end-users [4]. Ashenden and Sasse [14] showed that CISOs often experience difficulties in communicating the why and how behind security measures and that there is a need to use more effective channels or methods of communication to "sell" the relevance of such measures. The authors also emphasise the challenge CISOs face in gaining credibility due to a lack of authority and ambiguity about their responsibilities.

It is not always clear who CISOs should be reporting to, whether to the CEO or to the CIO, depending upon the nature of a vacancy, i.e. a newly created role versus a replacement [15]. CISOs may need to report to the board, with some research arguing that CISOs should be part of the board itself due to the security of information assets being a critical business function [11]. Shayo and Lin [16] further argue that there is no one-size-fits-all reporting structure for CISOs, and that any reporting structure will reflect the organisational, cultural, and socio-technical make-up of an organisation. This may, in turn, compound the challenges in assessing CISOs' responsibilities, liabilities, and who they are answerable to when there is no consistent job role description for CISOs.

The findings of the 2022 Global Cybersecurity Outlook 2022 Insight Report [17], which involved 120 cybersecurity leaders from 20 countries, confirm the challenges faced by CISOs and identify three main gaps between security-focused and business executives (Chief Executive Officers). Firstly, CISOs believe that cyber is not prioritised enough in business decisions. As a consequence, the second gap deals with the lack of involvement of CISOs in business decisions, which could result in security issues. The third gap concerns recruiting and retaining cybersecurity talent. While CISOs find it challenging to respond to a cybersecurity incident due to the shortage of skills within their team, business executives appear less acutely aware of the gaps.

In one study exploring pathways to the role of a CISO, Kappers and Harrell [18] examined degree requirements, certifications, hard skills and soft skills, alongside broader security risk management abilities, and business management. Their work attempted to identify the key skills required for the role of a CISO as identified by practitioners and academics. Although the sample size is limited, this study highlights the importance of developing the skills required for a CISO from an undergraduate degree level. This further reflects broader changes within the UK higher education ecosystem, as attempts are made to professionalise cybersecurity career pathways and reduce the cyber skills gap. Specifically, cybersecurity degree pathways are being mapped against the Cyber Security Body of Knowledge, including those that reflect the skills required for a CISO role.

3. The study

The data collection was carried out through the teaching of the module "Information Security Management" delivered to final-year undergraduate students. The first assignment in this module is to find three job openings for the position of Chief Information Security Officer (CISO), each from a different organisation. Students should critically discuss and compare the required essential and

desirable skills between the organisations' adverts. Students must also critically discuss, using academic literature, the key challenges a CISO faces in managing information security.

The module has been running for four years, and the authors of this paper, who are also the assessors of the assignment, collected the data using the links provided for the job adverts. The keywords that guided the analysis of the data include: experience, education, certification, soft skills, and IT-related skills.

Over the years, job descriptions have been shaped by technological and legislative factors. For instance, big data influenced job descriptions in 2022. By 2025, nearly all job vacancies will require some knowledge of Artificial Intelligence. In recent years, there has been a growing focus on complying with the General Data Protection Regulation 2016, and within the UK context, the Data Protection Act 2018.

The table below presents the outcomes of the content analysis of 50 job adverts between 2022 and 2025 in the UK.

Table 1
Key essential and desirable skills required by employers

	Essential skills	Desirable skills
Qualifications, requirements and skills	Experience of at least five years	Organisational leadership and management
	Master's degree in a relevant subject	Programming, Cloud security
	Certification and standards (ISO 27001, CISSP, CISM, GDPR)	MBA
	Communication, problem-solving, proactive thinking	Industry-specific regulations (e.g. SOX)

4. Discussion and conclusion

Cybersecurity roles, in particular cybersecurity leadership roles, are in high demand. The 2024 study by the Department of Culture, Media and Sport on Cyber Security skills in the UK labour market estimates that around half (44%) of businesses have skills gaps in basic technical areas. Further, nearly half (48%) of cyber leads within businesses lack confidence in their ability to undertake a

cybersecurity risk assessment and in developing cybersecurity policies. The participants in this study suggest that the combination of soft and technical skills is rather a rare skill set.

The 2024 Global Cybersecurity Outlook report states that organisations lack the right number of people with critical technical and soft skills, preventing them from achieving their strategic cyber-resilience objectives. To upskill the workforce, as many as 91% of organisations are willing to pay for cybersecurity training and certification for their employees. Certifications or short educational courses are one way to fill skills gaps.

The findings of this study are consistent with the recent research by Ramezan [19] that involved 250 job adverts listed across 27 nations. In particular, employers value prior professional experience, strong communication skills, and knowledge of regulatory frameworks and cybersecurity standards. The study also reveals that employers value bachelor's or master's degrees in business fields, which could equip CISOs with relevant business knowledge that has the potential to support a better alignment between security and business strategy. Ramezan [19] recommends the inclusion of management, data privacy, or business strategy modules within cybersecurity program curricula to reflect the shift of the CISO role to a more management and strategic focus.

The outcomes of this study are useful to improve the content of this module and inform future cybersecurity training programs. A valuable next step would be to incorporate qualitative research methods, such as interviews or focus groups with CISOs and hiring managers responsible for creating CISO job descriptions. This could provide deeper insights into how the listed requirements align with real-world practices and highlight which criteria are considered most critical during the hiring process.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] ISO 2022 https://www.iso.org/standard/27001

[2] U.S Security and Exchange Commission, 2023. https://www.sec.gov/newsroom/press-releases/2023-227

[3] U.S Attorney's Office, 2023. https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-sentenced-three-years-probation-covering-data

[4] Joseph Da Silva and Rikke Bjerg Jensen. 2022. "Cyber security is a dark art": The CISO as Soothsayer. Proc. ACM Hum.-Comput. Interact. 6, CSCW2, Article 365 (November 2022), 31 pages. https://doi.org/10.1145/3555090.

[5] Karanja E. (2017) The role of the chief information security officer in the management of IT security. Information & Computer Security Vol. 25 No. 3, pp. 300-329. DOI 10.1108/ICS-02-2016-0013

[6] S.B. Maynard, M. Onibere, A. Ahmad Defining the strategic role of the chief information security officer Pac. Asia J. Assoc. Inf. Syst. (2018), pp. 61-86, 10.17705/1pais.10303

[7] Department for Science, Innovation & Technology. (2024). Cyber security skills in the UK labour market 2024. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2024/cyber-security-skills-in-the-uk-labour-market-2024#current-skills-and-skills-gaps.

[8] van Yperen Hagedoorn, Jeroen M.J.; Smit, Richard; Versteeg, Patric; and Ravesteyn, Pascal, "Soft Skills of The Chief Information Security Officer" (2021). BLED 2021 Proceedings. 31.https://aisel.aisnet.org/bled2021/31I. Editor (Ed.), The title of book two, The name of the series two, 2nd. ed., University of Chicago Press, Chicago, 2008. doi:10.1007/3-540-09237-4

[9] Albrechtsen, E. (2007), "A qualitative study of users' view on information security", Computers and Security, Vol. 26 No. 4, pp. 276-289.

[10] A. Karlsson, F., Karin Hedström, K. and Göran Goldkuhl, G. (2017), "Practice-based discourse analysis of information security policies", Computers and Security, Vol. 67, pp. 267-279.

[11] Monzelo, Pedro and Nunes, Sérgio, "The Role of the Chief Information Security Officer (CISO) in Organisations (2019). *CAPSI 2019 Proceedings*. 36. https://aisel.aisnet.org/capsi2019/36

[12] Sjøberg Sveen, H., Østrem, F., Radianti, J., & Munkvold, B. E. (2020). The CISO role: a mediator between cybersecurity and top management. In Norsk IKT-konferanse for forskning og utdanning (No. 2)

[13] Hooper, V. and McKissack, J. (2016), "The emerging role of the CISO", Business Horizons, Vol.

No. 6, pp. 585-591..

[14] Ashenden, D. and Sasse, A. (2013), "CISOs and organisational culture: their own worst enemy?", Computers and Security, Vol. 39, pp. 396-405.

[15] Karanja, Erastus and Rosso, Mark A. (2017) "The Chief Information Security Officer: An Exploratory Study," Journal of International Technology and Information Management: Vol. 26: Iss. 2, Article 2. DOI: https://doi.org/10.58729/1941-6679.1299.

[16] Shayo, C., & Lin, F. (2019). An exploration of the evolving reporting organizational structure for the Chief Information Security Officer (CISO) function. *Journal of Computer Science*, *7*(1), 1-20.

[17] World Economic Forum. (2022). *Global Cybersecurity Outlook 2022*. World Economic Forum.

[18] Kappers, W. M., & Harrell, M. N. (2020, June). From degree to chief information security officer (CISO): A framework for consideration. In 2020, ASEE Virtual Annual Conference Content

[19] Ramezan A (2025). Understanding the chief information security officer: Qualifications and responsibilities for cybersecurity leadership. Computers & Security 152