South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865



# Bridging the cybersecurity skills gap for effective cyber audit and governance in the telecommunications sector

Check for updates

**Authors:**
Kabelo Mokhonoana[1]
Zaakir Ally[1]
Pranisha Rama[1]

**Affiliations:**
[1]Department of Accounting, College of Business and Economics, University of Johannesburg, Johannesburg, South Africa

**Corresponding author:**
Zaakir Ally,
zaakira@uj.ac.za

**Dates:**
Received: 14 Aug. 2025
Accepted: 25 Nov. 2025
Published: 29 Jan. 2026

**How to cite this article:**
Mokhonoana, K., Ally, Z. & Rama, P., 2026, 'Bridging the cybersecurity skills gap for effective cyber audit and governance in the telecommunications sector', *South African Journal of Information Management* 28(1), a2075. https://doi.org/10.4102/sajim.v28i1.2075

**Copyright:**
© 2026. The Authors. Licensee: AOSIS. This work is licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0) license (https://creativecommons.org/licenses/by/4.0/).

**Read online:**
Scan this QR code with your smart phone or mobile device to read online.

**Background:** The emergence of the Internet transformed global communication and operations, evolving into an essential tool that underpins daily life. Technological advancements such as artificial intelligence, blockchain and robotics have reshaped the digital landscape. Telecommunications, which enables communication across distances, has experienced rapid innovation now entering the era of 5G. However, this progress has been accompanied by escalating cybersecurity risks that threaten the integrity of systems and data.

**Objectives:** This study investigates the cybersecurity skills required to protect the telecommunications sector from emerging cyber threats. It aims to identify skill gaps and determine which cybersecurity competencies are viewed as most critical by audit professionals within the sector.

**Method:** A qualitative approach was adopted, using interviews to collect data from cybersecurity professionals in the South African telecommunications sector. The sample comprised 15 participants in the audit field purposefully selected based on their demonstrated experience and expertise in cybersecurity.

**Results:** Findings indicate that participants recognise the importance of cybersecurity skills, yet gaps remain in areas such as threat detection, incident response and secure system design. Respondents emphasised the need for continuous training and the importance of understanding cybersecurity frameworks.

**Conclusion:** The telecommunications sector must address both technical and soft skills in cybersecurity. Strengthening the workforce's cyber capabilities is vital for sustainable protection against threats.

**Contribution:** This study provides valuable insights into sector-specific cybersecurity needs and highlights the importance of skills development. It supports future policy, training and strategic interventions aimed at building cyber resilience in the telecommunications sector.

**Keywords:** cybersecurity risk; cybersecurity defence; telecommunication sector; cybersecurity skills; cybersecurity threats.

## Introduction

Over time, cybercrime has changed dramatically, from straightforward assaults on lone Personal Communication Services to extremely complex schemes aimed at vital infrastructure and large enterprises. Hackers primarily used simple techniques such as phishing or using malware to steal personal data to achieve their goals of financial gain or public recognition (Nurse 2020). However, with the development of technology, methods have become more sophisticated and varied for cybercriminals. The modern composition of cybercrime includes, but is not limited to, ransomware attacks where attackers encrypt the information of the victim to ransom it off by demanding money for its decryption. Advanced Persistent Threats (APTs) involves hackers gaining access to other people's networks and staying there, concealed, for extended periods with the intention of intelligence theft or disrupting operations (Jones 2024). State sponsored Cyber Espionage is a form of cyberwar that is waged between different nations with the view to gaining an upper hand tactically over others.

This has been further complicated by the advent of cryptocurrencies, which have made cybercriminal methods of receiving payments even more anonymous and untraceable. This evolution underlines the fact that the digital world keeps growing in complexity and

interconnectedness, thus demanding more robust and dynamic cybersecurity measures to keep up with an increasingly sophisticated and diverse range of threats (Smith 2021).

The research focuses on cybersecurity and Information Technology (IT) auditors professionals within the telecommunications sector. United Nations Office on Drugs and Crime (2021) revealed that cybercrime is a dynamic, new wave of transnational crime. In addition, the increasing role of organised crime groups adds to the complicated character of crime in the unburdened territory of cyberspace (Europol 2020). Perpetrators of cybercrime and their victims can be in different regions, and its effects can ripple through societies around the world, highlighting the need to mount an urgent, dynamic and international response (UNODC 2021). Besides, it shows the importance of cyber-skilled personnel, and the role played by information system audits.

Information Technology auditing has a significant role for the protection and usability of the information systems, especially in the telecommunications sector. Information Technology auditing is the process of continuous study of the IT processes and its factors with an aim of ascertaining whether the information systems of the organisation are functioning correctly and whether they are protected from all possible risks (Trabelsi et al. 2012). This framework helps the organisation to identify, for instance, system misconfigurations or unauthorised access, and compliance to regulations.

In addition to financial or operational audits, IT audits also play a huge role in the determination of cybersecurity measures. Other benefits of an IT audit are to determine the security flaws so that it is certain that the implemented measures are efficient (Grossman 2017). In the telecommunications sector where massive amounts of data pass through networks, IT auditing becomes more important as data leakage or hacking can cause a company a lot of reputational loss and fines resulting in more frequent auditing to control the risk (Pathak 2016). Pathak (2016) further elaborated his points by stressing on the fact that an IT auditor is not just a technical person who performs audit jobs but the professional who also has a strategic position in an organisation especially those dealing with cybersecurity. They confirm that corresponding procedures of risk management are implemented, and they validate that controls correspond to possible risks, which include unauthorised access, leakage of information, internal threats etc. Such an auditing process will enable organisations to remain compliant to frameworks like Control Objectives for Information and Related Technologies (COBIT) that provide structures of governance of information and cybersecurity (Grossman 2017).

However, among those firms that indeed have internal audit departments, those internal audit functions are evidently more effective in detecting and reporting security issues at a company (Goodwin-Stewart & Kent 2006). This aligns with the postulation that internal auditor structures are usually a necessity for identifying embezzlement and averting a system breakdown (Coram, Ferguson & Moroney 2008). The Information Systems Audit and Control Association's (ISACA) 2015 Triennial Cybersecurity Benchmarking study shows that the auditing frameworks such as COBIT can be used to increase the efficiency of cybersecurity policies. In their 2019 IT Audit Benchmarking Study, ISACA and Protiviti (2019) show how globally, organisations increasingly integrate IT auditing into their cybersecurity frameworks, further proving its relevance.

This research aims to demonstrate how companies should embrace and develop their cyber-skilled employees, given the significant shift in their roles owing to the modernisation of most work processes.

## Theoretical framework

The role theory examines human behaviour within the context of their social positions or statuses. It suggests that roles are developed based on expectations associated with role behaviour (Biddle 2013; Hindin 2007). Consequently, individuals who embody a specific role are motivated to do so because they understand the expected behaviours, while others are motivated through their expectations to guide and reinforce appropriate behaviours for those in that position (Biddle 1986; Lapalme, Kabiwa & Tardif 2019). An individual's comprehension of their own and others' expectations plays a crucial role in effectively fulfilling a role. The degree to which one understands these roles is influenced by their prior experiences and the knowledge acquired through observations, discussions or formal education (Biddle 2013; Lapalme et al. 2019).

Debates stemming from this theory have centred around what scholars refer to as the 'audit expectation gap'. As described by Ebimobowei, Kereotu and Brass Island (2011), this gap represents the disparity between what the public (including people, management and board of directors) expects from auditors and what auditors perceive their responsibilities to encompass. While Ebimobowei et al. (2011) highlight public trust as the core value of a profession and argue that betraying this trust renders the profession futile, Ramsarghey and Hardman (2020) contend that societal expectations of audits often exceed the actual standard of performance that auditors can realistically achieve.

This theory posits that it is the auditor's responsibility to detect and prevent cyberattacks, including managing risks and recovering losses resulting from such attacks. The theory highlights the importance of how cybersecurity roles are defined, understood and executed. Role Theory helps to explain why these gaps turn into risks for the organisation.

## Purpose of the study

The study investigates the cyber-skills required in the telecommunications sector. The study is directed by the following objectives:

To identify cybersecurity skills and competencies required to support effective cybersecurity assurance and auditing within the telecommunications sector.

To explore how existing audit frameworks (COBIT, International Organisation for Standardisation [ISO], National Institute of Standards and Technology [NIST]) can guide the development of cybersecurity competencies.

## Literature review

The rapid digitisation of the global economy means that data, networks, and systems have become the spine of modern societies, requiring stringent cybersecurity structures, which include cybersecurity skills. The demand for cyber-skilled personnel has increased in the workplace because of the rampant increase in the use of technology across all aspects in the workplace. From creating paperless offices to creating the office-less (virtual offices), technology has revolutionised the modern work environment. The Council of Economic Advisers (2018) points out that a general shortfall of cyber-skilled personnel capable of handling cybersecurity tasks represents an issue for both economic development and national security. Dawson and Thomson (2018) argue that, continuous development is key in addressing cybersecurity skills, given the rapid changing nature of cybersecurity threats. This becomes even more prevalent, in the age of artificial intelligence (AI), which will further enhance the effectiveness and inclusivity of cybersecurity practices together with cyber-skills (Chukwurah et al. 2024).

The increase in hacking cases and the rise in independent hacking groups have created the need for individuals who can strongly protect corporations' information (Hawamleh et al. 2020). This escalating cybersecurity threat landscape underscores the importance of robust cybersecurity measures and skilled professionals who can safeguard sensitive data. One such component of these measures is the IT audit or information systems audit which aim to obtain effective assurance over processes (Tinnel & Lindqvist 2022). Thus, having cybersecurity skilled personnel is key in managing and mitigating cybersecurity risks.

To establish effective cybersecurity assurance, organisations often rely on established standards or frameworks that offer management assurance techniques against significant threats (Bozkus Kahyaoglu & Caliyurt 2018). Jamison, Morris and Wilkinson (2018) highlight the significance of cybersecurity frameworks that define the principles that auditors should assess. Various specialised frameworks tailored to specific industries and control environments are in use, including those from organisations such as the ISO, the NIST, the International Information System Security Certification Consortium 2, and COBIT (Jamison et al. 2018). These frameworks help organisations to meet regulatory requirements, satisfy sector regulators, comply with internal audits and enhance their cybersecurity strategies.

These frameworks establish the standards, guidelines and procedures that auditing teams will use during assessments, making them essential in shaping the audit process (Drljača & Latinović 2017). Auditors must consider an organisation's regulatory policies, legal requirements and standards, as well as weigh the advantages and disadvantages of each framework while selecting one for an organisation (Bozkus Kahyaoglu & Caliyurt 2018; Jamison et al. 2018). A joint research effort by the Internal Audit Foundation and Crowe (Jamison et al. 2018) identified the top three most commonly used frameworks for defining cyber security approaches as the NIST framework, Control Objectives for Information Technology (COBIT5), and the ISO 27001 framework. The same trend is also evidenced by findings on the percentage of organisations utilising each framework for performing cybersecurity assessment, as reported by the ISACA and Protiviti (2019) annual global IT audit benchmarking study. Precisely, the report indicated that 64% of the organisations used the NIST Cybersecurity Framework, while 50% utilised the ISO 27001/27002 standards. Other frameworks include the COBIT framework, utilised by 42% of the organisations, while 29% utilised the Computer Information Systems Controls (ISACA & Protiviti 2019).

As digital transformation rewrites the rules of global commerce, an effective telecommunications sector has never been more critical to linking communities and breathing life into our economy (Arum 2021). The significance of this sector is even greater with the continued rise in 5G technology, Internet of Things and cloud services adoption which are all expected to improve networks connectivity, data transmission speeds as well overall communication network efficiency (GSM Association 2023).

Telecommunication companies carry information on a massive scale, which is important and confidential; therefore, they are also targeted by hackers. This, in combination with the complexity of telecommunications networks and their importance to both national security and economic supremacy, is what makes telecoms not only a prime target for cyber criminals but also state-sponsored actors (European Union Agency for Cybersecurity 2022).

Various specific cybersecurity vulnerabilities in the telecommunications sector may be understood by the fact that this sector acts like a backbone for other sectors. Since telecommunication networks are interconnected, part of the network's security breach impact was cascading across multiple services that other industries have, which include banking and finance, healthcare or critical infrastructure. Distributed Denial of Service attacks, data breaches and APTs (a type of threat that wants former malware examples) trying to infiltrate networks to extract information over long periods are also common cyber security threats for the sector (Verizon 2023).

Considering these threats, more and more telecommunications have started to up their security ante. These include better encryption, ongoing network monitoring and strong response

tactics in the event of a breach. In addition, regulatory bodies around the world have been pushing stricter cybersecurity measures to be adopted by telecommunication operators for them to strengthen their security frameworks against those incoming threats (Citaristi 2022).

The integration of IT auditing in telecommunications is crucial for adherence, maintaining customer trust and safeguarding infrastructure. Regular audits enable telecommunication companies to pinpoint vulnerabilities, evaluate the efficiency of security measures and be prepared to address cyber threats (Szczepaniuk & Szczepaniuk 2022). This proactive stance towards cybersecurity is essential in a sector where security breaches can have consequences. By assuring the integrity of cybersecurity measures, auditors will have even greater confidence instilled in various stakeholders, including customers, regulators and investors, so that the company can protect its networks and data against cyber risks. The link between IT auditing and cybersecurity is considered crucial in the field of telecommunications because cyberattacks might have a linked effect on the sector.

# Research methods and design

For this study, a qualitative research approach was chosen. This approach aligns with the study's objective to investigate the participants' perspectives with regard to skills required for cybersecurity within the telecommunication sector with a focus on audit and governance. Qualitative research was considered appropriate because of its capacity to capture rich, contextualised data that reflects the complexities of human experiences and behaviours (Liamputtong 2020). The focus on comprehending the nuances of participants' experiences necessitated an approach that would facilitate an in-depth exploration and interpretation of their viewpoints and contexts.

## Sample

In research, a target population serves as the focal point of investigation, encompassing the specific group or individuals under scrutiny for a given study. This concept aligns with the premise that research endeavours must be directed towards a particular group in order to draw meaningful insights and conclusions (Marvasti 2018). The identification and delineation of the target population plays a pivotal role in shaping the research scope, methods and overall applicability of findings. The whole population of cyber-skilled personnel and companies could not be considered for the study because of time and financial constraints. This study, therefore, targets cybersecurity personnel within the telecommunications sector, specifically with cybersecurity audit experience.

In this study, the researcher opted for purposive sampling as the non-probability sampling approach. Purposive sampling entails the selection of participants based on specific criteria that are relevant to the research objectives (Dawson 2019). This approach was chosen because it allows for the deliberate selection of participants who possess the characteristics and experiences necessary to address the research questions effectively. The researchers used purposive sampling to select participants' information. Purposive sampling is a form of non-probability sampling in which settings, persons and events are deliberately selected in order to provide important information, which is difficult to obtain from other people (Andrade 2021). Sampling is a principle used to search for a sample that can represent and act as a microcosm of a wider population (Thomas 2022). It is the process of selecting units or a representative population of interests to represent the whole population. The sample for this study comprised 15 participants who were purposefully selected based on their demonstrated experience and expertise in cybersecurity within the telecommunications sector, specifically within the audit and assurance space. Each of the participants signed a consent form indicating their participation as part of the study. Table 1 provides a summary of the sample selected.

## Data analysis

Thematic analysis stands as a qualitative data analysis technique dedicated to the identification, analysis and subsequent reporting of patterns or themes embedded within data (Bougie & Sekaran 2019). It provides a structured, yet adaptable, approach to uncovering the intricate meanings concealed within textual or visual data (Liamputtong 2020). This method transcends surface-level interpretations, delving into the underlying narratives, concepts and interpretations present within the data. In this study, the decision to employ thematic analysis as the data analysis approach was driven by its alignment with the research objectives and the qualitative nature of the collected data.

By leveraging thematic analysis, the study aimed to pinpoint recurring themes that encapsulate the essence of the identified challenges and their multifaceted impacts, thus fostering a deeper comprehension of the intricate dynamics at play. There were three researchers involved in the research project, the first researcher completed the coding process, and thereafter the remaining two researchers verified each of the codes, a total of four rounds of coding were completed, before the final themes were derived.

The process of conducting thematic analysis unfolded through a series of well-defined manual steps. Initially, the qualitative data, derived from sources such as interviews and observations, was diligently transcribed and subjected to familiarisation to immerse in its content. Subsequently, the data underwent a systematic coding process, during which individual data segments were assigned codes. These codes were then systematically organised into themes, which

**TABLE 1:** Sample selected.

| Number of years in the telecommunications sector | Number of participants | Percentage |
|---|---|---|
| 5–10 | 3 | 20 |
| 11–15 | 3 | 20 |
| 16+ | 9 | 60 |
| **Total** | **15** | **100** |

encapsulated broader patterns and overarching concepts present within the data. Throughout this process, meticulous attention was directed towards ensuring that the identified themes remained coherent, distinct and truly representative of the underlying data. These themes were subjected to a continuous process of refinement and review, all while maintaining close reference to the original data to ensure the accuracy and alignment of the analysis.

This process was conducted using excel, which is considered appropriate, given the smaller size of the sample (Bree & Gallagher 2016). The selection of the thematic analysis approach was underpinned by its inherent flexibility, which enabled the research to adapt to the complexity and richness of the data. This approach provided the researcher with the means to uncover both the anticipated themes and those that emerged organically, ensuring a comprehensive exploration of the identified challenges and their far-reaching implications. This process revealed two key themes as depicted in Table 2.

### Ethical considerations

Ethical clearance to conduct this study was obtained from the University of Johannesburg, School of Accounting Research Ethics Committee (SAREC20240523/13). Based on ethical clearance received for the study, age/gender/occupation etc. was not included. In terms of occupation all participants were involved in cybersecurity audit as set out in our sample discussion. Participants were only identified using numbers for example "Participant 1" as included within the results section.

## Results

### Theme 1: Enhancing cybersecurity competence through continuous learning, technical skills development and organisational support mechanisms

This section delves into a crucial theme that emerged from the data, namely the cyber-skills required of personnel in the telecommunications sector. This theme sheds light on the specific competencies and knowledge areas that individuals in this sector must possess to navigate the complex landscape of cybersecurity effectively. One of the participants, Participant 3 (P3), highlighted the importance of continuous learning and adaptation in the field of cybersecurity thus, 'In this sector, you can't afford to become stagnant. Cyber threats evolve rapidly, and so should our skills'.

**TABLE 2:** Themes.

| Theme | Categories | Examples |
|---|---|---|
| 1. Enhancing Cybersecurity Competence through Continuous Learning, Technical Skills Development, and Organisational Support Mechanisms | • Soft skills<br>• Technical skills<br>• Ongoing learnings | • Continuous learning<br>• Technical skills<br>• Network security<br>• Encryption<br>• Intrusion Detection<br>• Risk Assessment<br>• Internal mentorships |
| 2. Integrating Cybersecurity Frameworks for Effective Governance, Standardisation, and Regulatory Compliance | • Governance<br>• Risk management<br>• Operational Processes | • COBIT for governance and risk management<br>• ISO for international standards and communication<br>• NIST flexibility<br>• Regulatory challenges |

COBIT, Control Objectives for Information and Related Technologies; ISO, International Organisation for Standardisation; NIST, National Institute of Standards and Technology.

This sentiment echoes the dynamic nature of cybersecurity, where staying up to date with the latest trends and threats is paramount.

Results show that there is need to learn constantly when it comes to cybersecurity, and this is a known problem in the cybersecurity sector. Cyber threats constantly change and develop, which makes the work of a professional depend on the new technologies and tools as well as newly discovered attacks. This need is supported in the literature through the reality that owing to the dynamic nature of threats with which cybersecurity professionals deal with, they must constantly update their knowledge and skills (Pfleeger & Caputo 2012). The sophistication with which the threats are developed is much higher than the acquisition of skills in the conventional method, hence constant learning is mandatory for cybersecurity professionals in the telecommunication sector.

Participant 8 (P8) highlighted the significance of technical expertise, stating:

> 'A deep understanding of network security, encryption, and intrusion detection is non-negotiable. These are the foundational skills needed to protect our systems.' (P8)

This perspective underscores the essential technical competencies required to safeguard telecommunications networks.

Results emphasised the importance of technical knowledge in areas such as network security, encryption and intrusion detection system (IDS). This is in line with the existing body of knowledge that underscores the importance of network security as a key issue of concern, particularly regarding issues of access, leakage of information and disruption of services (Tariq, Khan & Asim 2021). Encryption is used for maintaining data confidentiality and its integrity whereas IDS is used to detect the outbreaks of attacks (Stallings 2015). These technical competencies are the cornerstones of any security agenda enabling telecommunications corporations to safeguard their extensive networks and the information that they process.

Participant 2 (P2) paid attention to the critical role of risk assessment skills, noting:

> 'Identifying vulnerabilities and assessing risks is a crucial part of our job. Without these skills, we can't proactively protect our systems.' (P2)

Effective risk assessment is indeed a fundamental aspect of cybersecurity, enabling organisations to identify and mitigate potential threats.

Furthermore, Participant 9 (P9) highlighted the importance of soft skills in cybersecurity, submitting that:

> '*Communication and collaboration skills are often overlooked, but they're vital.* We need to work together to respond to incidents and share knowledge.' (P9)

In addition, Participant 12 (P12) indicated that:

> '… to enhance cyber-skills, telecommunications companies should implement internal mentorship and knowledge-sharing programmes. By pairing experienced cybersecurity professionals with newer staff, we can facilitate hands-on learning and knowledge transfer. Additionally, investing in continuous learning platforms that offer courses on the latest cybersecurity trends and tools will help keep skills up to date in a rapidly evolving field.' (P12)

These insights underscore the significance of interpersonal skills in a field that often requires cross-functional cooperation. Participant 4 (P4) contributed to the discussion by highlighting the need for specialisation:

> 'While a broad understanding of cybersecurity is essential, specialisation in areas like penetration testing or threat analysis can set individuals apart.' (P4)

This perspective aligns with the idea that cybersecurity professionals may choose to specialise in specific domains to deepen their expertise.

An effective risk assessment process involves identifying, analysing and evaluating risks to the confidentiality, integrity and availability of information systems. Without this, organisations may struggle to pre-emptively manage cyber threats (Tipton & Krause 2007). This proactive approach is essential for minimising the potential damage that can be caused by cyberattacks. In addition, as the complexity of cybersecurity threats has grown, so too has the need for specialisation. Rostami, Karlsson and Gao (2020) has pointed out that cybersecurity professionals who specialise in areas such as ethical hacking, forensic analysis or incident response are in higher demand owing to the complexity of these domains. Specialised skills enable individuals to tackle specific, highly technical challenges that are beyond the scope of general cybersecurity knowledge (Toregas, Hoffman & Heller 2016).

Technical competencies, risk assessment abilities, continuous learning, soft skills and specialisation all play crucial roles. These insights underscore the complexity of the field, and the diverse skill set demanded of those working within it. In addition, it is evident from the participants' contributions that a holistic approach to cyber-skills is essential. This approach includes not only technical proficiency but also the ability to communicate effectively, assess risks and adapt to evolving threats. As Participant 3 (P3) aptly put it:

> 'It's not just about knowing the tools; it's about knowing how to use them and when to use them.' (P3)

Participants highlighted the need for continuous learning, technical expertise, risk assessment skills, soft skills and specialisation. These insights underscore the dynamic and challenging nature of cybersecurity in this sector, where individuals must possess a diverse skill set to effectively protect telecommunications networks and systems.

Participants acknowledged the increasing importance of cyber-skills in the telecommunications sector. Participant 1 (P1) stated:

> 'With the rapid advancement of technology, cyber-skills are indispensable. They're the backbone of ensuring data security in our sector.' (P1)

This sentiment was echoed by Participant 10 (P10), who said:

> 'Cyber-skills are like a currency in our field; without them, you're at a disadvantage.' (P10)

These observations align with literature that points to cybersecurity as a critical capability in the digital age (Mansfield-Devine 2016; Tipton & Krause 2007).

Despite recognising the significance of cyber-skills, participants also expressed concerns about their own skill levels. Participant 9 (P9) mentioned:

> 'I feel like I'm lagging behind in terms of cyber-skills. It's a fast-paced field, and sometimes, it's overwhelming to keep up.' (P9)

This sentiment of inadequacy was further highlighted by Participant 5 (P5), who admitted:

> 'I know the basics, but I'm not sure if that's enough. Cyber threats are evolving so quickly.' (P5)

Participants discussed the challenges they faced in staying updated with the ever-changing landscape of cybersecurity. Participant 7 (P7) shared:

> 'It's not just about having the skills; it's about constantly learning and adapting. It's a lot of pressure to stay on top of the latest trends and threats.' (P7)

*This sentiment resonated with many participants who felt that the dynamic nature of cybersecurity required continuous effort.*

Some participants mentioned the need for additional training and development opportunities to enhance their cyber-skills. Participant 1 (P1) said:

> 'Investing in training programmes and certifications is essential. It not only improves individual skills but also contributes to the overall security posture of our organisation.' (P1)

Participant 10 (P10) added:

> 'Our sector should offer more opportunities for skills development. It's a win-win for both employees and employers.' (P10)

These sentiments reflect a broader challenge in the sector, where professionals often struggle to keep pace with evolving threats and technological advancements. According to Wilkerson (2021), continuous learning is essential in the cybersecurity field, but the rapid rate of change can be daunting for many.

Interestingly, participants also discussed the importance of collaboration and knowledge sharing within the sector. Participant 9 (P9) opined:

> 'We shouldn't feel like we're in this alone. There is so much we can learn from each other. Collaboration can bridge the gap in cyber-skills.' (P9)

Participant 5 (P5) echoed this sentiment, saying:

> 'Networking and sharing experiences can be as valuable as formal training.' (P5)

While participants acknowledged the critical role of cyber-skills, they also expressed concerns about their adequacy and the challenges of staying updated. The need for continuous learning, training opportunities and sector collaboration emerged as key themes. These insights highlight the dynamic nature of cybersecurity in the telecommunications sector and the ongoing efforts required to maintain and enhance cyber-skills.

The theme of cyber-skills within the telecommunications sector gives a multidimensional overview of the competence needed for the dynamic nature of cybersecurity. Participants in this study pointed to the need for continuous learning, technical expertise, risk assessment, soft skills and specialisation. Cybercrime is one of the fastest evolving areas of criminal activity and hence, there needs to be continuous training (Davis & Magrath 2013). In contrast, research identified basic technical competencies in network security, encryption and intrusion detection, representing some of the main 10 competencies in cybersecurity (Gordon et al. 2015).

Other than technical skills, soft skills were also mentioned to be very important, and participants also indicated that one should be able to communicate and collaborate within a team and be able to mentor others. This is consistent with other research indicating that cross-functional collaboration and communication are critical for incident response and foster cybersecurity knowledge-sharing among employees inside an organisation (Grossman 2017). The second key element is that of specialisation; practitioners are incentivised to develop focus areas such as Penetration Testing or Threat analysis, again supported in the literature on the need for deep expertise in selected aspects of cybersecurity. Participants acknowledged the dynamism and the high speed of the area, and there were fears regarding keeping up with the evolving threats. This is also supported by literature showing challenges in staying current within cybersecurity and increased requirements of skilled workers (Gordon et al. 2015). In addition, participants underlined sector collaboration and knowledge sharing, which also aligns with studies drawing on notions of collective defence mechanisms and learning from peers in cybersecurity.

## Theme 2: Integrating cybersecurity frameworks for effective governance, standardisation and regulatory compliance

Participant 9 (P9) also highlighted the value of COBIT, stating:

> 'COBIT is our guiding light. It sets the standards for governance and control. We use it as a framework to ensure that our IT systems align with business objectives.' (P9)

However, Participant 14 (P14) indicated that:

> 'Regulatory compliance is a significant challenge in maintaining robust cybersecurity measures. Telecommunications companies have to navigate a complex landscape of local and international regulations and ensuring compliance can be resource intensive. Failure to comply not only exposes us to legal penalties but also to reputational damage. The challenge is to implement cybersecurity measures that meet regulatory requirements while also being flexible enough to adapt to changing laws and standards.'

These participants' perspective underscores the pivotal role of COBIT in providing a structured approach to IT governance and aligning technology initiatives with organisational goals.

Participant 4 (P4) echoed similar sentiments regarding COBIT, highlighting its significance in risk management. Participant 4 (P4) asserted:

> 'COBIT helps us identify and assess risks comprehensively. It's not just about compliance; it's about understanding our vulnerabilities and taking proactive measures.' (P4)

This viewpoint accentuates COBIT's utility in risk assessment, demonstrating its practical application beyond mere compliance. This underscores COBIT's value in aligning IT and business goals while offering structured governance. According to De Haes et al. (2020), COBIT serves as an integrated framework that helps organisations to optimise IT investments, manage risks and ensure compliance with external regulations, all while ensuring that technology supports business objectives.

Participant 8 (P8) shared insights on ISO, remarking,

> 'ISO is like a universal language. It allows us to communicate our cybersecurity practices effectively with partners and clients. It builds trust.' (P8)

This perspective underscores ISO's role as an internationally recognised standard that facilitates collaboration and trust-building in the telecommunications sector.

Participant 3 (P3) provided a different angle on ISO, focusing on its role in continuous improvement. Participant 3 (P3) stated:

> 'ISO's Plan-Do-Check-Act (PDCA) cycle is invaluable. It encourages us to continually assess, plan, implement, and improve our security processes.' (P5)

Participant 3's viewpoint highlights ISO's contribution to a culture of ongoing enhancement in cybersecurity practices.

Participant 5 (P5) contributed insights on NIST, highlighting its adaptability. Participant 5 (P5) mentioned:

> 'NIST's flexibility allows us to tailor security controls to our specific context. It's not one-size-fits-all, which is crucial in our diverse sector.' (P5)

This perspective highlights NIST's adaptability to the unique needs and contexts within the telecommunications sector. According to Stallings and Brown (2018), ISO standards provide a framework that helps organisations communicate their security practices clearly, thus enhancing trust among stakeholders and partners in the telecommunications sector. The use of ISO standards can also enhance customer confidence and help organisations to demonstrate their commitment to maintaining high levels of security.

The COBIT is perceived as a guiding framework for governance, risk management and alignment with business objectives. The ISO is valued for its universality and ability to foster trust and effective communication, while NIST is appreciated for its flexibility and adaptability to diverse sector contexts. Furthermore, these frameworks are not seen as static compliance measures but as dynamic tools that promote proactive risk assessment, continuous improvement and tailored security controls. This thematic analysis underscores the importance of these frameworks in shaping information security practices and audit processes within the telecommunications sector.

Participants generally recognised the value of established frameworks such as COBIT, ISO and NIST in enhancing cybersecurity within the telecommunications sector. Participant 9 (P9) highlighted:

> 'Frameworks like COBIT, ISO, and NIST provide a structured approach to cybersecurity. They offer guidelines and best practices that can help organisations strengthen their defences against cyber threats.' (P9)

One recurring theme in the analysis was the frameworks' ability to address specific cyber threats effectively. Participant 4 (P4) highlighted thus:

> 'ISO, for instance, offers a comprehensive set of controls that cover various aspects of information security. This can be particularly useful in countering specific threats, like data breaches or malware attacks.' (P4)

Participants appreciated the global nature of these frameworks, which contributed to consistency in cybersecurity practices across the telecommunications sector. Participant 8 (P8) stated:

> 'The beauty of ISO and NIST is that they provide a common language for cybersecurity. This consistency allows organisations to align their efforts with global best practices.' (P8)

The participants acknowledged that these frameworks provided a degree of customisability to suit the specific needs of telecommunications organisations. Participant 3 (P3) explained:

> 'COBIT, ISO, and NIST are not one-size-fits-all. They can be tailored to fit the unique requirements of our sector, which can vary significantly from one company to another.' (P3)

Frameworks such as NIST allows organisations to adapt their cybersecurity practices based on their specific contexts, thus enhancing their resilience against diverse threats.

Despite the strengths of these frameworks, participants also highlighted challenges in their implementation. Participant 5 (P5) shared:

> 'While these frameworks are great, they can be complex to implement. It's not just about adopting them; it's about integrating them into our existing systems and processes'. (P5)

Resource allocation emerged as a significant concern in the analysis. Participant 9 (P9) expressed:

> 'Implementing and maintaining these frameworks can be resource intensive. It requires a substantial investment in terms of both finances and personnel'. (P9)

Participants recognised the ever-evolving nature of cyber threats and the need for frameworks to keep pace. Participant 4 (P4) stated:

> 'Cyber threats are not static. They evolve continuously. Frameworks like NIST need to be updated regularly to remain relevant.' (P4)

Some participants underscored the importance of complementing frameworks with sector-specific expertise. Participant 8 (P8) said:

> 'While these frameworks are invaluable, they are not a replacement for deep sector knowledge. Telecommunications organisations should also invest in cybersecurity experts who understand our unique challenges'. (P8)

The analysis revealed a consensus among participants regarding the need for a holistic approach to cybersecurity. Participant 3 (P3) articulated:

> 'Frameworks are just one piece of the puzzle. Effective cybersecurity involves a combination of people, processes, and technology, with frameworks guiding the process.' (P3)

Participants also highlighted the significance of continuous monitoring and evaluation of cybersecurity measures. Participant 5 (P5) stressed:

> 'Implementing these frameworks is not a one-time effort. Regular audits and assessments are essential to ensure that our cybersecurity measures are effective.'

Participants' reflections on the use of COBIT, ISO and NIST reveal a deep appreciation for these frameworks within the telecommunications sector. These frameworks play multifaceted roles, ranging from governance and risk management to international communication and adaptability. Moreover, participants viewed these frameworks as dynamic tools that promote proactive risk assessment and continuous improvement. This thematic analysis highlights the significance of COBIT, ISO and NIST in shaping information security practices and audit processes, underlining their pivotal roles in ensuring the integrity and resilience of telecommunications systems. However, challenges in implementation and resource allocation were acknowledged. The dynamic nature of cyber threats necessitated regular updates to these frameworks. Participants highlighted the importance of sector expertise

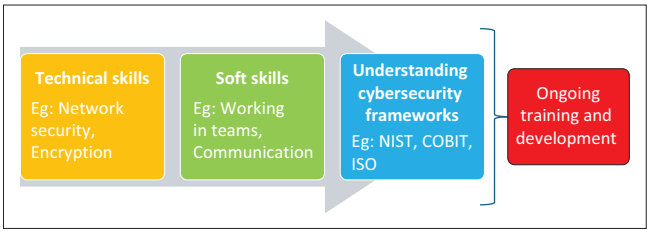
and a comprehensive approach to cybersecurity, highlighting the need for continuous monitoring and evaluation.

These insights reflect the complex landscape of cybersecurity within the telecommunications sector, where frameworks play a vital but evolving role. The idea of the supporting tools for audits, toolkits on cybersecurity, and those frameworks that are already established such as COBIT, ISO and NIST- play a very vital role in security enhancement, operational efficiencies and governance of the telecommunications sector. The participants made it emphatic how these supported tools and frameworks have become effective in proactive protection of systems, anomaly detection and collaboration. The developments in auditing tools are in line with the literature pointing out the emergingly greater use of AI in cybersecurity for enhancement in the threat detection and response times (Chio & Freeman 2018). Results also reveal how such tools make operations efficient with ease, allowing professionals to pay attention to their core tasks of security efficiently, which aligns with the general research provided by Shahzad et al. (2023) on operational efficiencies created and provided by automated cybersecurity tools.

Cybersecurity frameworks in the form of COBIT, ISO and NIST represented fundamental building blocks in the governance, risk management and operational processes of telecommunications companies. Participants revealed that COBIT mostly serves to align IT with business objectives. Indeed, this is reflected in the literature; COBIT ensures a systematic approach to managing IT risks and embedding them into organisational goals. International Organisation for Standardisation's universal applicability is very well documented in various studies that have established evidentially how ISO ensures standardisation and trust in global cybersecurity operations (International Organisation for Standardisation [ISO]/International Electrotechnical Commission [IEC] 2017). In addition, participants emphasised the balance between tight security and operational efficiency and research that calls for the balance between usability and robust security measures (Johnson 2015).

However, respondents mentioned challenges to the actual deployment of these frameworks, mainly related to their complexity and resource utilisation. For example, participants indicated that high costs are needed in terms of financing and people, as also identified in the literature by Fernandes et al. (2016) when they mention that comprehensive and proper cybersecurity frameworks represent extremely costly implementations. This is further supported by participants discussing the need for ongoing improvement. This indeed supports other literature from studies that have emphasised that cyber threats themselves change in such frequency, and hence frameworks should evolve continuously to cope with the new emerging threats.

Participants' reflections indicate how auditing tools and cybersecurity frameworks such as COBIT, ISO and NIST are




COBIT, Control Objectives for Information Technologies; ISO, International Organisation for Standardisation; NIST, National Institute of Standards and Technology.

**FIGURE 1:** Cybersecurity skills.

fundamentally important to the telecommunications sector. These frameworks ensure risk management, compliance and operational efficiency without foregoing the agility and adaptability principle while addressing sector-specific requirements. However, implementation issues and ever-changing cyber threats call for intensive learning, resource allocation, and an integrated cybersecurity approach, involving people and technologies.

The key skills required for cybersecurity is technical, soft skills and understanding cybersecurity frameworks, which required ongoing training and development, to stay abreast to the escalating threat landscape. Figure 1 graphically depicts skills required within cybersecurity.

Applying Role Theory, cybersecurity skills in the telecommunications sector are socially constructed through interactions among stakeholders. Frameworks such as COBIT, ISO and NIST provide role clarity and closure by standardising expected competencies, behaviours and responsibilities, thereby strengthening security, operational efficiency and governance.

### Recommendations

- Cybersecurity auditors must be upskilled with technical and soft skills
- Technical skills include, but not limited to, network security, ethical hacking, forensic analysis, encryption, intrusion detection, penetration testing risk assessment and incident management
- Soft skills include, but are not limited, working in teams, communication management, corroboration, continuous learning collaboration, mentorship and knowledge management
- Upskilling through training programmes, and certifications, to stay up-to-date, and improve the overall security posture of an organisation.
- Gaining an understanding of cybersecurity frameworks (e.g. COBIT, ISO, etc.) is important given the emphasis on governance, risk management and cyber defences required for an organisation.

## Conclusion

The study highlights that bridging the cybersecurity skills gap is not only essential for operational protection but also for strengthening audit and governance processes that

ensure compliance and resilience in telecommunications. The findings provide valuable insights into the multifaceted contributions of cybersecurity challenges faced by telecommunications companies. Furthermore, the data also describes the essential cyber-skills required by personnel in the telecommunication sector and the critical role of skills and frameworks in ensuring security and compliance. Lastly, it highlights the pivotal role of organisational capacity, including resources, leadership support, training, communication and culture, in strengthening the effectiveness of cybersecurity professionals. Another significant finding revolves around the evolving and dynamic nature of cybersecurity challenges faced by telecommunications companies. Participants observed the ever-changing landscape of cyber threats, including the shift towards organised cybercrime and the adaptability of hackers. This underscores the need for continuous adaptation and vigilance in cybersecurity efforts, as well as the importance of staying ahead of the curve in identifying and mitigating vulnerabilities.

The impact of cyberattacks on the financial health and reputation of telecommunications companies emerged as a recurring concern. Participants highlighted that a single breach could result in substantial financial losses and erode customer trust. This finding underscores the tangible consequences associated with cyber vulnerabilities and the high stakes involved in cybersecurity within the telecommunications sector. The data also revealed the diverse attack vectors that telecommunications firms must contend with, including attacks on customer data, industrial espionage and even critical infrastructure. This multifaceted threat landscape emphasises the need for comprehensive cybersecurity strategies that encompass various attack scenarios and vulnerabilities. As far as limitations are concerned, this study only focused on the telecommunication sector, and was limited to 15 participants. Future research could focus on, other sectors or industries, providing, additional skills that may be required for cybersecurity professionals.

## Acknowledgements

This article is based on research originally conducted as part of Kabelo Mokhonoana's master's thesis titled 'Cyber security skills required in the telecommunications industry', submitted to the College of Business and Economics, Department of Accounting, University of Johannesburg in 2025. The thesis was supervised by Mr Zaakir Ally and Ms Pranisha Rama. The manuscript has since been revised and adapted for journal publication. The original thesis is currently unpublished and was not publicly available online at the time of publishing this article.

### Competing interests

The authors, Kabelo Mokhonoana, Zaakir Ally and Pranisha Rama declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

### CRediT authorship contribution

Kabelo Mokhonoana: Conceptualisation, Writing – original draft. Zaakir Ally: Formal analysis, Supervision, Writing –review & editing. Pranisha Rama: Formal analysis, Supervision, Writing – review & editing. All authors reviewed the article, contributed to the discussion of results, approved the final version for submission and publication, and take responsibility for the integrity of its findings.

### Funding information

The authors received no financial support for the research, authorship and/or publication of this article.

### Data availability

The data that support the findings of this study are available from the corresponding author, Zaakir Ally, upon reasonable request.

### Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research. They do not necessarily reflect the official policy or position of any affiliated institution, funder, agency or that of the publisher. The authors are responsible for this article's results, findings and content.

## References

Andrade, C., 2021, 'The inconvenient truth about convenience and purposive samples', *Indian Journal of Psychological Medicine* 43(1), 86–88. https://doi.org/10.1177/0253717620977000

Arum, B.U., 2021, 'Hacking and cyber security in Nigeria telecommunication sector: Implication for teaching and learning', *SIST Journal of Religion and Humanities* 1(1), 121–136.

Biddle, B.J., 1986, 'Recent developments in role theory', *Annual Review of Sociology* 12(1), 67–92. https://doi.org/10.1146/annurev.soc.12.1.67

Biddle, B.J., 2013, *Role theory: Expectations, identities, and behaviors*, Academic Press, London.

Bougie, R. & Sekaran, U., 2019, *Research methods for business: A skill building approach*, John Wiley & Sons, Hoboken, NJ.

Bozkus Kahyaoglu, S. & Caliyurt, K., 2018, 'Cyber security assurance process from the internal audit perspective', *Managerial Auditing Journal* 33(4), 360–376. https://doi.org/10.1108/MAJ-02-2018-1804

Bree, R.T. & Gallagher, G., 2016, 'Using Microsoft Excel to code and thematically analyse qualitative data: A simple, cost-effective approach', *All Ireland Journal of Higher Education* 8(2), 2811–2819. https://doi.org/10.62707/aishej.v8i2.281

Chio, C. & Freeman, D., 2018, *Machine learning and security: Protecting systems with data and algorithms*, O'Reilly Media, Inc., Sebastopol, CA.

Chukwurah, N., Abieba, O.A., Ayanbode, N., Ajayi, O.O. & Ifesinachi, A., 2024, 'Inclusive cybersecurity practices in AI-enhanced telecommunications: A conceptual framework', *Journal of AI and Telecommunications Security* 8(2), 45–60.

Citaristi, I., 2022, 'International Telecommunication Union – ITU', in H. Canton (ed.), The *Europa Directory of International Organizations 2022*, pp. 365–369, Routledge, New York, NY.

Coram, P., Ferguson, C. & Moroney, R., 2008, 'Internal audit, alternative internal audit structures and the level of misappropriation of assets fraud', *Accounting & Finance* 48(4), 543–559. https://doi.org/10.1111/j.1467-629X.2007.00247.x

Davis, J. & Magrath, S., 2013, *A survey of cyber ranges and testbeds*, Cyber Electronic Warfare Division, Edinburgh.

Dawson, A., 2019, *Research methods and statistics in physical education*, Scientific e-Resources, ED-Tech Press, United Kingdom.

Dawson, J. & Thomson, R., 2018, 'The future cybersecurity workforce: Going beyond technical skills for successful cyber performance', *Frontiers in Psychology* 9, 744. https://doi.org/10.3389/fpsyg.2018.00744

De Haes, S. & Van Grembergen., 2020, 'COBIT as a framework for enterprise governance of IT', in *Enterprise governance of information technology: Achieving alignment and value in digital organizations*, pp. 125–162, Springer, Switzerland.

Drljača, D. & Latinović, B., 2017, 'Audit in public administration's information systems – External or internal?', in *IOP conference series: Materials science and engineering*, vol. 200, no. 1, p. 012026, IOP Publishing.

Ebimobowei, A., Kereotu, O.J. and Brass Island, P.M.B., 2011, 'Role theory and the concept of audit expectation gap in South-South, Nigeria', *Current Research Journal of Social Sciences* 3(6), 445–452.

European Union Agency for Cybersecurity, 2022, Th*reat landscape for telecommunications: Assessing security in the telecom sector*, European Union Agency for Cybersecurity, viewed 17 August 2024, from https://www.enisa.europa.eu/publications/telecom-security-threat-landscapePP.

Europol, 2020, *Internet organised crime threat assessment (IOCTA) 2020*, European Union Agency for Law Enforcement Cooperation, Netherlands.

Fernandes Jr, G., Carvalho, L.F., Rodrigues, J.J. & Proença Jr, M.L., 2016, 'Network anomaly detection using IP flows with principal component analysis and ant colony optimization', *Journal of Network and Computer Applications* 64, 1–11. https://doi.org/10.1016/j.jnca.2015.11.024

Goodwin-Stewart, J. & Kent, P., 2006, 'Relation between external audit fees, audit committee characteristics and internal audit', *Accounting & Finance* 46(3), 387–404. https://doi.org/10.1111/j.1467-629X.2006.00174.x

Gordon, L.A., Loeb, M.P., Lucyshyn, W. & Zhou, L., 2015, 'The impact of information sharing on cybersecurity underinvestment: A real options perspective', *Journal of Accounting and Public Policy* 34(5), 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Grossman, M., 2017, 'The human capital model', in *Determinants of health: An economic perspective*, pp. 42–110, Columbia University Press.

GSM Association, 2023, *The mobile economy 2023*, GSM Association, viewed 01 September 2024, from https://www.gsma.com/mobileeconomy/.

Hawamleh, A.M.A., Alorfi, A.S.M., Al-Gasawneh, J.A. & Al-Rawashdeh, G., 2020, 'Cyber security and ethical hacking: The importance of protecting user data', *Solid State Technology* 63(5): 7894–7899.

Hindin, M.J., 2007, 'Role theory', in G. Ritzer (ed.), *The Blackwell encyclopedia of sociology*, pp. 3959–3962, Blackwell Publishing, Hoboken, NJ.

International Organization for Standardisation/International Electrotechnical Commission, 2017, *ISO/IEC 27001:2017 information technology – Security techniques – Information security management systems – Requirements*, International Organization for Standardization, Geneva.

ISACA & Protiviti, 2019, *2019 Global IT audit benchmarking study*, viewed 01 October 2024, from https://www.isaca.org/bookstore/bookstore-misc-landing-pages/it-audit-benchmarking-2019.

ISACA, 2015, 'Cybersecurity 360-degree vision', *ISACA Journal* 5, 1–59.

Jamison, J., Morris, L. & Wilkinson, C., 2018, 'The future of cyber security in internal audit', *Disponibil Online*, viewed 13 September 2024, from https://www.crowe.com/-/media/Crowe/LLP/folio-pdf/The-Future-of-Cybersecurity-in-IA-RISK-18000-002A-update.pdf.

Johnson, K.N., 2015, 'Managing cyber risks', *Georgia Law Review* 50, 547.

Jones Sr, J.A., 2024, 'Cybersecurity methods to increase visibility, threat detection, and cyber defense in critical infrastructure', Doctoral dissertation, Capitol Technology University.

Lapalme, J., Kabiwa, V. & Tardif, P.M., 2019, 'Relationship between information technology auditors and auditees and their impacts on auditors', *International Journal of Engineering Business Management* 2019, 11. https://doi.org/10.1177/1847979019878980

Liamputtong, P., 2020, *Qualitative research methods*, 5th edn., Oxford University Press, Docklands, Victoria.

Mansfield-Devine, S., 2016, 'Ransomware: Taking businesses hostage', *Network Security* 2016(10), 8–17. https://doi.org/10.1016/S1353-4858(16)30096-4 [Mathematical Foundations, MITRE Technical Report 2547, Volume 1].

Marvasti, A., 2018, 'Research methods', in A.J. Trevino (ed.), *The Cambridge handbook of social problems*, vol. 1, pp. 23–37, Cambridge University Press, Cambridge.

Nurse, J.R.C., 2020, 'Cyber-crime and you: How criminals attack and the human factors that they seek to exploit', *Computers & Security* 90, 101720.

Pathak, D.P., 2016, 'Cybersecurity: Model for cybercrime prevention and controlling', *International Journal of Novel Research in Computer Science and Software Engineering* 3(1), 58–61.

Pfleeger, S.L. & Caputo, D.D., 2012, 'Leveraging behavioral science to mitigate cyber security risk', *Computers & Security* 31(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Ramsarghey, K. & Hardman, S.G., 2020, 'The auditing profession's role in terms of accountability: A South African perspective', *Southern African Journal of Accountability and Auditing Research* 22(1), 39–49.

Rostami, E., Karlsson, F. & Gao, S., 2020, 'Requirements for computerized tools to design information security policies', *Computers & Security* 99, 102063. https://doi.org/10.1016/j.cose.2020.102063

Shahzad, A., Kayani, H.U.R., Malik, A.A., Raza, M.A. & Saleem, A., 2023, 'Big data security, privacy protection, tools and applications', *Pakistan Journal of Science* 75(02), 353–372. https://doi.org/10.57041/pjs.v75i02.850

Smith, P., 2021, *Cyber espionage is here to stay: A realist approach to cybersecurity*, Canadian Association for Security and Intelligence Studies, Toronto.

Stallings, W. & Brown, L., 2018, *Computer security: Principles and practice*, 4th edn., Pearson Education Limited, London.

Stallings, W., 2015, *Foundations of modern networking: SDN, NFV, QoE, IoT, and Cloud*, Pearson Education, Inc., New Jersey, NJ.

Szczepaniuk, E.K. & Szczepaniuk, H., 2022, 'Analysis of cybersecurity competencies: Recommendations for telecommunications policy', *Telecommunications Policy* 46(3), 102282. https://doi.org/10.1016/j.telpol.2021.102282

Tariq, N., Khan, F.A. & Asim, M., 2021, 'Security challenges and requirements for smart internet of things applications: A comprehensive analysis', *Procedia Computer Science* 191, 425–430. https://doi.org/10.1016/j.procs.2021.07.053

The Council of Economic Advisers, 2018, *The cost of malicious cyber activity to the U.S. economy*, Executive Office of the President of the United States, Washington, DC.

Thomas, F.B., 2022, 'The role of purposive sampling technique as a tool for informal choices in a social sciences in research methods', *Just Agriculture* 2(5), 1–8.

Tinnel, L. & Lindqvist, U., 2022, 'Importance of cyber security analysis in the operational technology system lifecycle', in J. Staggs & S. Shenoi (eds.), *Critical infrastructure protection XVI*, pp. 73–101, Springer, Cham.

Tipton, H.F. & Krause, M., 2007, *Information security management handbook*, 6th edn. CRC Press, Boca Raton, FL.

Toregas, C., Hoffman, L.J. & Heller, R., 2016, 'Exploring ways to give engineering cyber security students a stronger policy and management perspective', in *2016 Spring ASEE Mid-Atlantic Section Conference*, April 08–09, The George Washington University, Washington, DC.

Trabelsi, Z., Hayawi, K., Al Braiki, A. & Mathew, S.S., 2012, *Network attacks and defense: A hands-on approach*, CRC Press, Boca Raton, FL.

United Nations Office on Drugs and Crime, 2021, *The global impact of cybercrime: A roadmap for policymakers*, United Nations Office on Drugs and Crime, Vienna, viewed 08 September 2024, from https://www.unodc.org.

Verizon, 2023, *2023 Data breach investigations report: Public sector snapshot*, CA, viewed 01 September 2024, from https://www.verizon.com/business/resources/search/?query=2023%20Data%20Breach%20Investigations%20Report.

Wilkerson, W.S., 2021, 'Development of a Social Engineering eXposure Index (SEXI) using open-source personal information', Doctoral dissertation, Nova Southeastern University.