CYBERSECURITY SKILLS GAP SURVEY

Compiled by: Dr Namosha Veerasamy, Danielle Badenhorst, Oyena Mahlasela, Errol Baloyi and Noku Siphambili

1. INTRODUCTION

Organisations around the world face the challenge of attracting and maintaining critical cybersecurity skills. There is a growing demand for these critical skills as cyberattacks gain momentum, making it crucial for organisations to have the necessary expertise to deal with the barrage of attacks. Preventive, investigative and responsive actions are needed.

Cyberattacks have various implications, like decreased revenues, loss of services and reputational damage. The cyber response needs a team of skilled professionals. However, many organisations may struggle to appoint the necessary personnel to handle cybersecurity issues. Lengthy recruitment times, difficulty finding candidates with the necessary skills or qualifications or budget constraints are common obstacles.

South Africa, as a developing nation, could also become a prime target for cyberattacks. With the growing adoption of technology and digital processes, the attack surface also widens. Cyber knowledge of key areas may not be strong enough for organisations to protect themselves.

The CSIR would like to investigate the state of the cybersecurity skills gap within the country to determine whether South Africa is facing similar global challenges with regard to skills. The study also aimed to determine recruitment strategies, skills needs and critical areas of skills interventions.

The Cybersecurity Skills Gap Survey aimed to assess how organisations within South Africa are addressing skills shortages, training requirements and building up their pool of knowledgeable cybersecurity workers.

In this first study of cybersecurity skills in South Africa, we examine the findings from a survey used to capture a snapshot of the country.

The need for cybersecurity skills cannot be stressed enough. The need for organisations to protect themselves from cybersecurity threats is vital to ensure operations, continuity, and security. Some organisations may fail to realise the importance of cybersecurity, while others may have a significant investment.

1.1 CYBERSECURITY SKILLS GAP SURVEY

The CSIR undertakes directed, multidisciplinary research and technological innovation that contributes to the improved quality of life of South Africans. In addition, the CSIR seeks to build and transform human capital.

Empirical research can assist in the fulfilment of these values. With this in mind, the CSIR and its research partner Thirdstream embarked on a nationwide survey that sought to gather information on skills gap issues in South African organisations. The survey collected information on, among other things:

- Cybersecurity skills sector;
- Investment in cybersecurity skills;
- Lack of specific skills;
- Critical skills are needed in the foreseeable future;
- Cybersecurity positions in organisation;
- Unfilled positions;
- Scare skills; and
- Qualifications.

The objective of the survey was to establish a baseline with respect to the state of cybersecurity skills in multiple sectors.

The report begins with an executive summary showing the most pertinent findings.

2. EXECUTIVE SUMMARY

- The majority of the organisations were relatively small, under 1 000 employees.
- Most of the respondents came from the main provinces of Gauteng, the Western Cape and KwaZulu-Natal.
- In particular, organisations (88%) are choosing to invest in cybersecurity and have recognised the need for these critical skills. The majority (32%) of organisations stated that they could not invest in cybersecurity resources because their business is too small and 16% stated that they could not afford or see the need to invest in resources to manage their cybersecurity. While other organisations (3%) stated that their systems are secure, are governed by the department, and will look into investing in resources.
- 33% of the respondents indicated that between 21 to 40% of the cybersecurity positions were unfilled, while another 29% also had a substantial indication of 41 to 60% of the positions unfilled. 14% had a staggering 61 to 80% of their positions unfulfilled. This shows the notable challenges that organisations face in filling cybersecurity positions.
- The most unfilled cybersecurity positions are the security manager (26%), individual contributor (25%), and senior manager or director of security (21%)
- The most sought-after qualifications by employees and organisations are Certified Information System Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), and Certified Information Privacy Professional (CIPP).
- Many organisations struggle to find candidates with the minimum qualifications needed. 38% indicated that the applicants had less than 25% of the required qualifications. 35% of the applicants responded that they had 25 to 50% of the required qualifications. Only 4% indicated that the applicants had 75 to 100% of the necessary qualifications. This shows that core skills are in short supply.
- In terms of Human Resources (HR) challenges faced by organisations, 55% mentioned that they face challenges recruiting cybersecurity employees, with 35% facing retention challenges of cybersecurity employees, while 10% mentioned that they do not face any cybersecurity recruitment or retention challenges. It is significant to note that the majority of organisations polled are facing a major challenge in recruiting and retaining cybersecurity employees. Globally, there is also a shortage of cybersecurity skills, and this survey finding substantiates this issue.
- The most valued skills of an organisation relate to incident response, cloud security and risk, governance, and compliance.
- Required skills for the future will include artificial intelligence, threat intelligence, data breach handling and privacy enforcement.
- 61% believe that women face challenges in cybersecurity roles due to gender bias, lack of awareness, etc.
- A growing requirement for cybersecurity workers will be the ability to work from home. After Covid-19, many members prefer to work from home. However, many organisations in South Africa require members to be in the office at least once a week. Hybrid working conditions are thus currently the most popular approach.
- The key findings of the survey are encapsulated in the infographic below.

CYBERSECURITY SKILLS GAP STATUS IN SOUTH AFRICA

IS YOUR ORGANISATION STRUGGLING TO FIND QUALIFIED CYBERSECURITY PROFESSIONALS?

This **infographic** highlights the **key findings of a 2023 survey developed by the CSIR on the cybersecurity skills gap in South Africa**. The majority of the organisations were relatively small – under 1000 employees. **Most respondents stemmed from major provinces: Gauteng, Western Cape and KwaZulu Natal**. A summary:

1 CRITICAL SKILLS:

- The most valued skills of an organisation relate to incident response, cloud security and risk, governance and compliance.
- Required skills for the future will include Artificial Intelligence, Threat Intelligence, data breach handling and privacy enforcement.
- Cybersecurity is considered a scarce skill due to a lack of awareness in the field as well as financial reasons.

2 SKILLS GAP, CERTIFICATIONS AND INVESTMENT:

- **88%** invest in cybersecurity resources, but **50%** agree that there isn't enough investment in skills development.
- Threat intelligence, incident response and cloud security are highly valued skills.
- **74%** believe there's a greater shortage of cybersecurity skills compared to general Information Technology skills.
- The most sought-after certifications by employees and organisations are Certified Information System Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) and Certified Information Privacy Professional (CIPP).

3 HIGH DEMAND, LOW SUPPLY:

- **62%** of cybersecurity roles are partially or fully unfilled.
- Security managers are the most sought-after **(26%)**.
- Only **25%** of applicants have the required qualifications.

4 CHALLENGES IN RECRUITMENT AND RETENTION:

- **Scarce skills (64%)** and competitive salaries (43%) are the biggest hurdles in filling vacancies.
- Retaining talent is another issue (**35%** due to better offers, lack of training opportunities, etc.)
- Recruiting qualified candidates is difficult (**55%** of Human Resource professionals report this).

5 REMOTE WORK AND GENDER REPRESENTATION

- **46%** of cybersecurity professionals consider work-from-home very important.
- **77%** agree that the need for specialised cybersecurity skills has increased due to remote work.
- **61%** believe women face challenges in cybersecurity roles due to gender bias, lack of awareness, etc.
- **82%** believe cybersecurity positions are dominated by males.

WHAT'S NEXT?

Address the skills gap through targeted **training programmes** and certifications.

Promote diversity and inclusion initiatives in recruitment and retention.

Encourage women to pursue cybersecurity careers through mentorship and role models.

IN CONCLUSION

Overall, South Africa faces a significant cybersecurity skills gap. Increased investment in skills development, competitive offerings and fostering a diverse and inclusive work environment are crucial to addressing this challenge.

3. ABOUT THE RESPONDENTS

The majority of the 320 respondents who participated in the 2023 Cybersecurity Skills Gap Survey were from general management (37%). Participants also stemmed from operations (13%), human resources (12%), risk management (9%), IT management (8%), cybersecurity (7%), sales and marketing (7%) and finance (2%). 5% indicated other domains.

3.1 SECTOR TYPES

The survey covered a wide range of sectors, including banking, IT and higher education, as well as small, medium and micro enterprises.

IT, professional and technical services totalled 20% of the responses, while the financial services and educational sectors each had 9% of the participants. See igure 1.

IT, Professional, Scientific and Technical	**20%**
Financial Services and Insurance	**9%**
Education and Training	**9%**
Agriculture, Forestry, Fishing and Food	**8%**
Healthcare	**7%**
Construction	**6%**
Wholesale and Retail Trade	**6%**
Manufacturing	**6%**
Tourism	**5%**
Arts, Entertainment and Recreation	**4%**
Transport	**4%**
Communication	**2%**
Mining and Quarrying	**2%**
Housing	**1%**
Utilities (Electricity, Gas, etc.)	**1%**
Other (specify)	**10%**

Figure 1: Top sectors represented

3.2 ORGANISATIONAL SIZE

1 - 29	**22%**
30 - 100	**29%**
101 - 999	**24%**
1 000 - 1 999	**9%**
2 000 - 2 999	**4%**
3 000 - 3 999	**6%**
4 000 - 4 999	**2%**
5 000+	**8%**
Don't know	**1%**

Figure 2: Organisational size

Organisational sizes represented in the survey were largely in favour of very small organisations, with 75% having 1 to 999 employees. 8% worked in large organisations with over 5 000 employees.

3.3 LOCATION OF RESPONDENTS

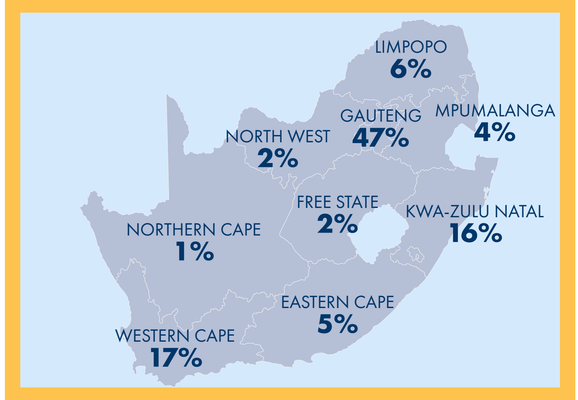

Figure 3: Province distribution

The majority of the respondents stemmed from Gauteng (47%). This is mainly due to Gauteng being the country's key economic hub. The other provinces had smaller representation, but it should be noted that Gauteng, the Western Cape and KwaZulu-Natal are the more predominant role-players in the technology field of South Africa.

For more information, visit **www.csir.co.za**

science & innovation
Department:
Science and Innovation
REPUBLIC OF SOUTH AFRICA

CSIR
Touching lives through innovation

CYBERSECURITY SKILLS GAP SURVEY

Compiled by: Dr Namosha Veerasamy, Danielle Badenhorst, Oyena Mahlasela, Errol Baloyi and Noku Siphambili

<CONTINUED>

SURVEY RESULTS (2 OF 3)

4. SURVEY RESULTS

4.1 INVESTMENT IN SKILLS

88% reported investing resources and services in cybersecurity. The reasoning of the 12% of participants who did not invest resources and services in cybersecurity is shown in the next figure.

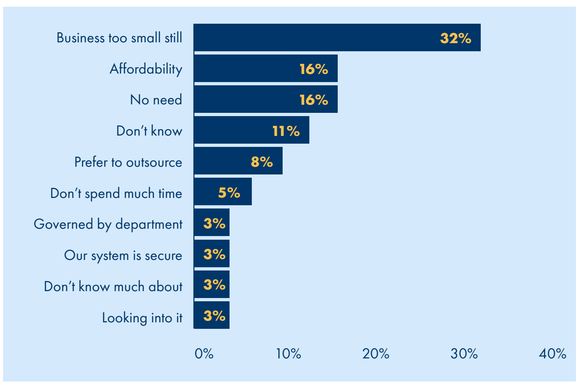

Figure 4: Reasons for not investing in cybersecurity

The majority (32%) of organisations stated that they could not invest in cybersecurity resources because their business is too small and 16% stated that they could not afford or see the need to invest in resources to manage their cybersecurity. Other organisations (3%) stated that their systems are secure, are governed by the department and will look into investing in resources. This could be due to those organisations that have not invested in cybersecurity not seeing the value of cybersecurity in their organisations. However, most organisations should recognise the need to invest in cybersecurity resources to reduce threats like data breaches that could result in the exposure of data and information.

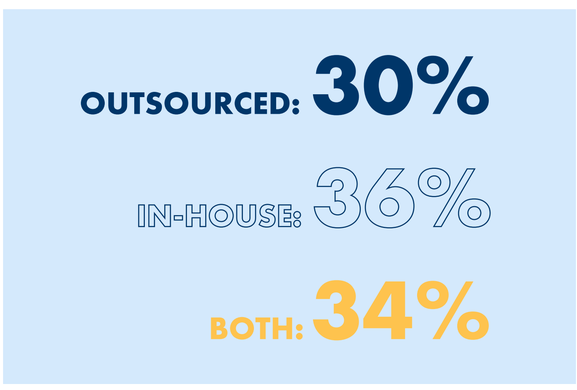

Figure 5: Sourcing of cybersecurity skills

In terms of how skills are sourced, 36% mentioned that they source their cybersecurity skills in-house, and 30% of the skills are outsourced. However, 34% mentioned that they acquire internal skills and outsource their cybersecurity skills.

50% agreed that there is not enough investment in cybersecurity skills in the country.

4.2 CRITICAL SKILLS

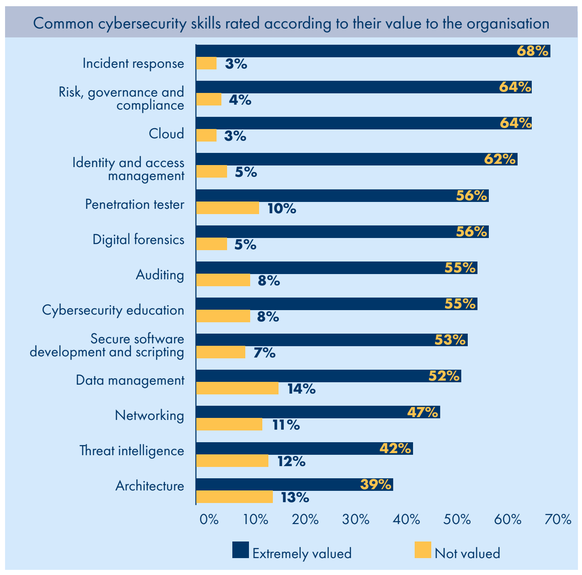

Figure 6: Most valued skills

Regarding common cybersecurity skills, the survey considered which skills were valued by the organisation. Here, it is considered 'extremely valued' or 'not valued'. The most widely valued skills include incident response, risk, governance and compliance, cloud, identity and access management. Incident response, risk management, governance and compliance, cloud security, and identity and access management are critical skills that contribute to the security posture of an organisation. For example, having incident response capabilities ensures swift recovery and minimises damage and downtime. Risk management is critical to identify and assess potential threats to an organisation. Cloud security helps ensure unauthorised data access and breaches. Identify management also ensures authorised access and prevents data breaches.

The least valued skills include data management, networking, threat intelligence and architecture. These skills are also critical for an organisation, but other skills are often of a higher priority.

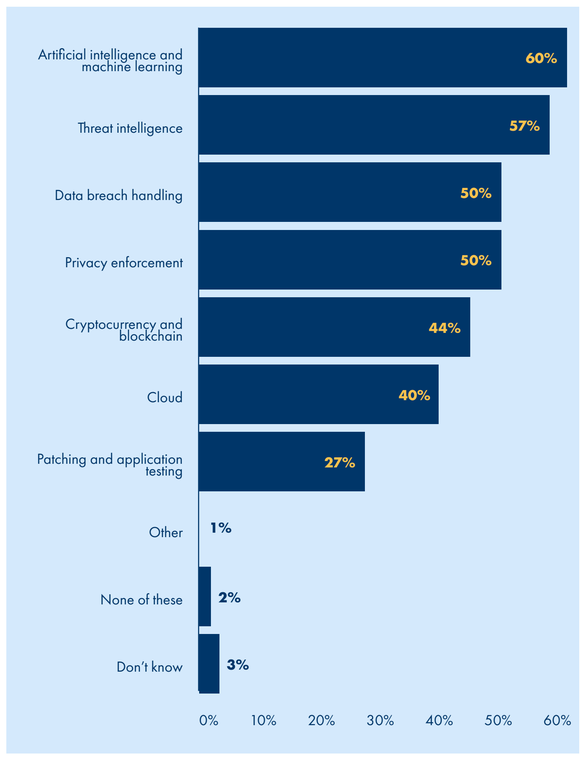

Figure 7: Required skills

Among the top skills considered important in the future, respondents included artificial intelligence (AI) and machine learning (ML), threat intelligence, data breach handling and privacy enforcement.

As AI and ML become increasingly applied in organisational contexts and within cybersecurity, these skills are essential to stay ahead of evolving threats. In addition, threat intelligence is becoming essential to anticipate and mitigate attacks before they cause damage. Increased regulations, such as the Protection of Personal Information Act, have increased the need for data protection and breach management; organisations must ensure they have the expertise to manage data breaches, enforce privacy laws, and maintain compliance.

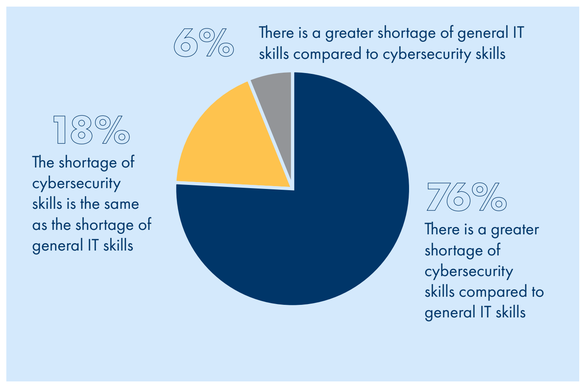

Figure 8: Shortage of cybersecurity skills compared to IT skills

The fact that 76% of the respondents identified a greater shortage of cybersecurity skills compared to general IT skills emphasises the urgency for organisations to invest in building a skilled cybersecurity workforce (shown in Figure 8)

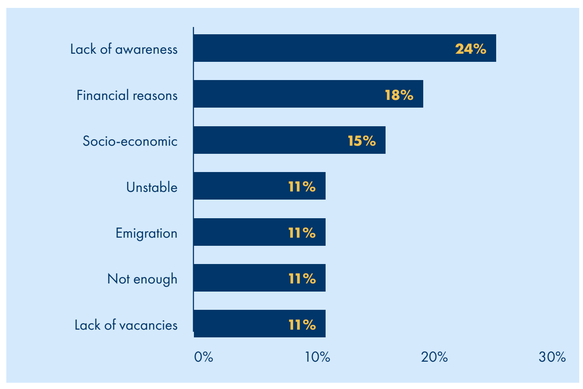

Figure 9: Cybersecurity as a scarce skill

The survey data in Figure 9 indicates key reasons why cybersecurity is considered a scarce skill in South Africa. This includes lack of awareness, financial reasons, and socioeconomic factors. A significant proportion of the respondents attributed the scarcity of cybersecurity skills to a general lack of awareness of cybersecurity as a career path. This could include a lack of understanding of the opportunities and importance of cybersecurity roles, both at educational institutions and within organisations.

Financial constraints are another major factor. Cybersecurity professionals often demand high salaries due to the specialised nature of their skills, and many organisations, especially smaller businesses or those in the public sector, may struggle to afford competitive salaries. Socioeconomic challenges, such as inequality in education and limited access to resources, also contribute to scarcity. Many people in South Africa may not have access to the necessary training or infrastructure to develop cybersecurity skills, especially in underserved communities. This limits the pool of qualified people available to fill critical roles in cybersecurity.

4.3 UNFILLED POSITIONS

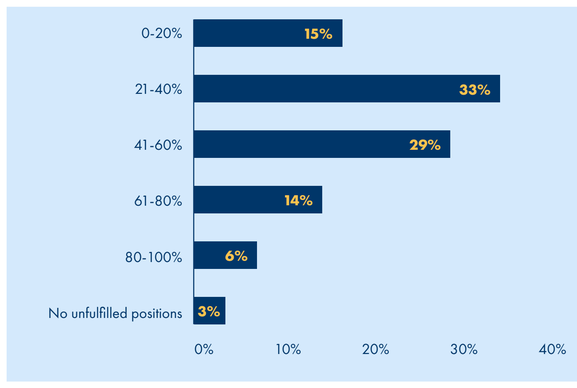

Figure 10: Unfulfilled positions

33% of the respondents indicated that between 21 to 40% of the cybersecurity positions were unfilled, while another 29% also had a substantial indication that 41 to 60% of the positions were unfilled. 14% had a staggering 61 to 80% of their positions unfulfilled. This shows the notable challenges that organisations face in filling cybersecurity positions.

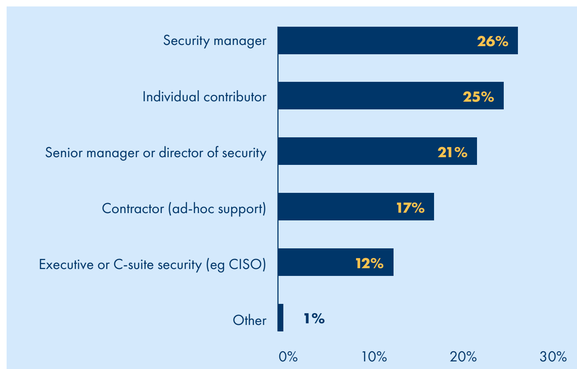

Figure 11: Most unfulfilled positions

With regard to the number of unfilled cybersecurity positions for organisations, the security manager position was rated the highest with 26%, followed by individual contractors with 25%. The senior manager position was rated 21% and the Contractor Ad hoc support was rated 17%. The Executive security position had 12% unfulfilled position and only 1% was not specified. This shows that the lower management and operational positions had the highest numbers of unfulfilled positions when compared to the upper management positions.

4.4 QUALIFICATIONS

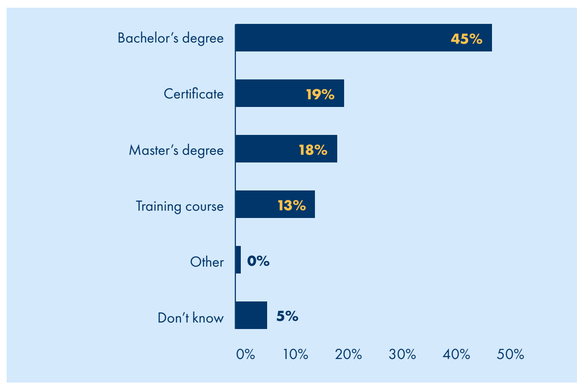

Figure 12: Minimum qualification

In terms of the minimum requirement for a cybersecurity specialist, 45% of the organisations mentioned that a bachelor's degree is the minimum requirement and 19% said that a certificate would suffice. 18% mentioned that a master's degree is a minimum requirement. 13% mentioned that a training course was a basic requirement and 5% were uncertain.

Most sought-after certifications by your organisation	
Certified Information System Security	52%
Certified Information Systems Auditor (CISA)	36%
Certified Information Security Manager (CISM)	36%
Certified Information Privacy Professional	35%
Systems Security Certified Practitioner	34%
COMPTIA Cyber Security Analyst	31%
COMPTIA Security+	31%
COMPTIA Network+	26%
COMPTIA Data+	25%
COMPTIA Cloud+	22%
COMPTIA A+	17%
COMPTIA Pentest+	15%
Offsec Certified Professional (OSCP)	14%
None	7%

Figure 13: Organisational demanded certifications

In terms of certifications that are mostly considered when hiring new employees, 52% mentioned that CISSP was sought after. CISSP depends on the cybersecurity role as this certification is not an entry-level certificate. CISA and CISM came second, with 36% of organisations saying they look for them. Again, CISA and CISM are not entry-level certifications, as one would consider CISA if hiring for a system auditor and CISM for a senior cybersecurity role. The rest of the certifications, which got lower rankings, are the ones that organisations can consider since they indicate that the person at least has a basic understanding of cybersecurity, with the exception of OSCP, which is a more technical certification done by experienced penetration testers.

Most sought-after certifications by your organisation	
Certified Information System Security	48%
Certified Information Security Manager	33%
Certified Information Privacy Professional	32%
Certified Information Systems Auditor (CISA)	29%
Systems Security Certified Practitioner	27%
COMPTIA Data+	26%
COMPTIA Cyber Security Analyst	26%
COMPTIA Cloud+	25%
COMPTIA Network+	25%
COMPTIA Security+	25%
COMPTIA A+	18%
COMPTIA Pentest+	13%
Offsec Certified Professional (OSCP)	10%
Other [Specify]	2%

Figure 14: Employee sought certifications

Similarly, the most sought-after certifications by employees themselves are CISSP (48%), CISM (33%), CIIP (32%) and CISA (29%).

Figure 15: Minimum security experience

The majority (58%) indicated that three to five years of security experience was required. A significant amount (29%) showed that only zero to two years of security experience was needed. This showed that organisations were in need of beginner to mid-level experience and only 9% needed longer work experience between six to nine years.

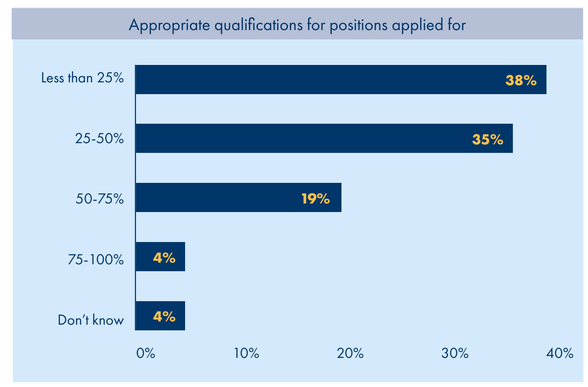

Figure 16: Appropriate qualifications

38% indicated that the applicants had less than 25% of the required qualifications. 35% of the applicants responded that they had 25% to 50% of the required qualifications. Only 4% indicated that the applicants had 75% to 100% of the necessary qualifications. This shows that core skills are in short supply.

4.5 VACANCIES

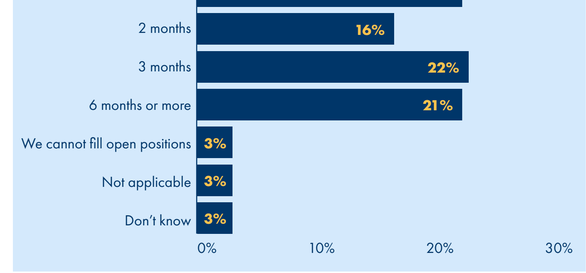

Figure 17: Time to fill positions

The majority (22%) revealed that it took three months to fill positions, with 21% indicating that it took six months or more. 21% were in a strong position to fill cybersecurity positions within a month, and 10% were even able to achieve it within two weeks. 3% indicated that they were unable to fill open positions. The responses were diverse and spread across various time frames.

science & innovation
Department:
Science and Innovation
REPUBLIC OF SOUTH AFRICA

For more information, visit **www.csir.co.za**

CSIR
Touching lives through innovation

CYBERSECURITY SKILLS GAP SURVEY

Compiled by: Dr Namosha Veerasamy, Danielle Badenhorst, Oyena Mahlasela, Errol Baloyi and Noku Siphambili

<CONTINUED>

SURVEY RESULTS (3 OF 3)

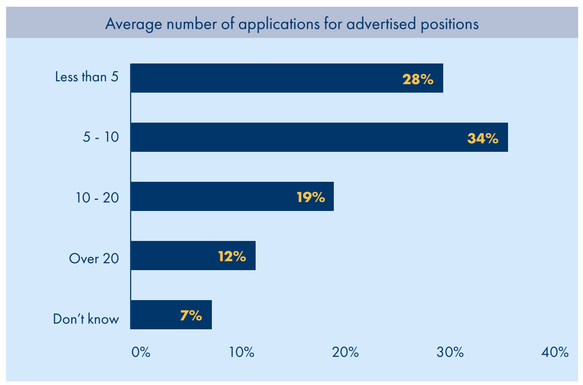

Figure 18: No applications

34% of the respondents had between five to ten applications for advertised positions. 28% received fewer than five applications. 19% had between 10 and 20 responses to the advertised positions, and 12% received more than 20 applications.

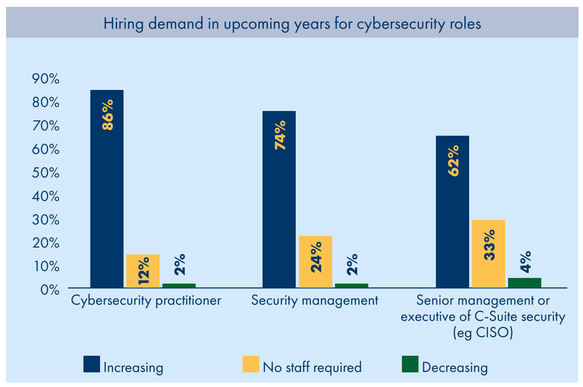

Figure 19: Hiring demand

Figure 19 shows the responses to the question, "In the upcoming years, where do you see the hiring demand moving toward the following roles in your organisation?".

Respondents showed a growing requirement for all three roles of cybersecurity practitioner (86%), security manager (74%) and senior management (62%). This shows that cybersecurity needs will continue to rise and not decrease a great deal.

Figure 20: Reasons for the resignation of

The main reason for resignations is better salary options (23%). This indicates that financial drive will remain one of the key competing forces for skills attraction. Organisations offering competitive salaries will elicit the best from the workforce pool. Other reasons indicated were benefits (18%), working conditions (17%), poor management style (15%) and no training (14%). These findings show that employees would leave an organisation if they were not happy with the management environment. Additionally, training is the key to attracting and maintaining good talent to ensure the maintenance of skills and learning on demand.

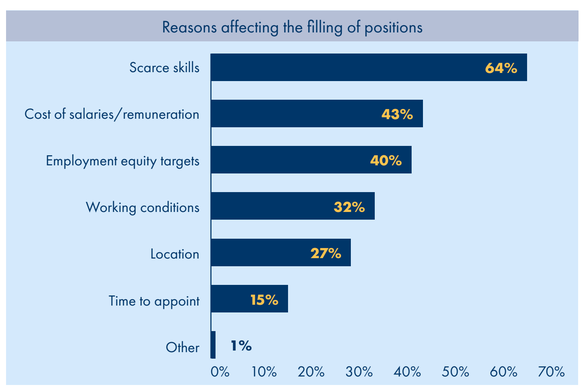

Figure 21: Reasons affecting the filling of positions

Regarding the reasons why some vacancies are not filled, 64% mentioned that some skills are scarce, 43% mentioned that there are costs involved in filling vacancies, 40% mentioned that they reach the employment equity targets and 32% stated that working conditions that are organisations implementing hybrid working conditions result in some vacancies not being filled. 27% mentioned that location plays a role, 15% stated that it takes time to appoint a new employee and 1% mentioned that there were other reasons for not filling vacancies.

Figure 22: HR challenges

In terms of HR challenges faced by organisations, 55% mentioned that they face challenges recruiting cybersecurity employees, 35% faced challenges with retaining cybersecurity employees, while 10% mentioned that they do not face any cybersecurity recruitment or retention challenges. It is significant to note that most organisations polled face a major challenge in recruiting and retaining cybersecurity employees. Globally, there is also a shortage of cybersecurity skills, and this survey finding substantiates this issue.

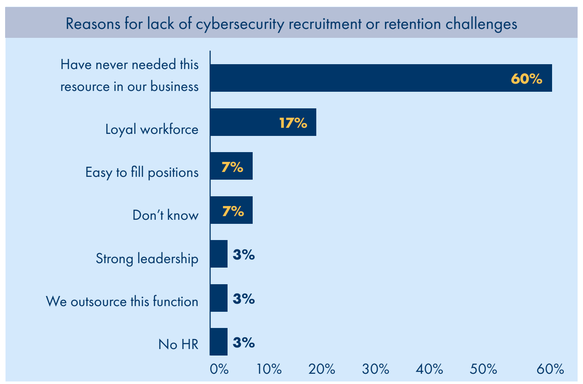

Figure 23: Reasons for lack of cybersecurity recruitment and retention challenges

Of the 10% minority who stated that they do not have cybersecurity recruitment or retention challenges, 60% mentioned that they have never seen the need for this resource. 17% stated that they have loyal staff, 7% stated that it is easy to fill positions and they do not understand why this is the case. Additionally, 3% of the organisations mentioned that they have strong leadership, 3% do not outsource this function and 3% mentioned that they have no HR function in their organisations.

It is noteworthy to find that the strongest reason given is that they had never had a need for this resource. It may be significant to note that some organisations have not realised the need for and implications of cybersecurity, especially in terms of data protection, access control and overall operational functionality.

4.6 WORK FROM HOME

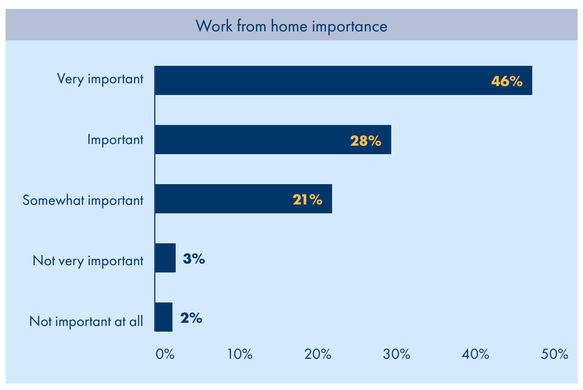

Figure 24: Work from home importance

For many cybersecurity professionals, an added advantage is the ability to work from home. In information and communication technology (ICT), the key feature of remote connectivity provides the ability to be located anywhere but still be able to work. After the remote working conditions forced by Covid-19, many cybersecurity specialists still prefer the remote working mode. In the survey, a large majority, 46%, showed that working from home is very important and 28% indicated that it is important.

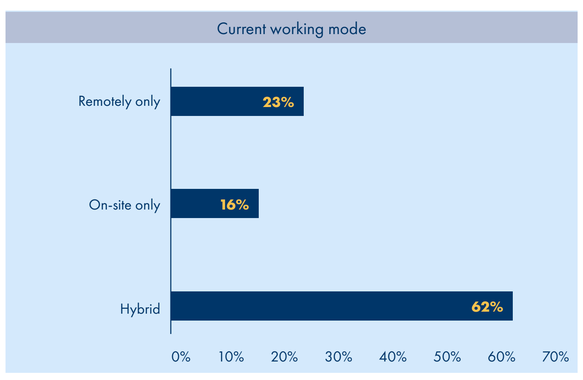

Figure 25: Current working mode

Many employees have now returned to the office after the remote working conditions imposed during Covid-19. Many organisations now adopt a hybrid approach where employees go into the office premises a few times a week and work from home on other days. The survey results corroborate this with 62% working under hybrid conditions. 23% work remotely only, and 16% work on-site only. On-site only may refer to critical functions that require teams to work physically together and be in close proximity to each other.

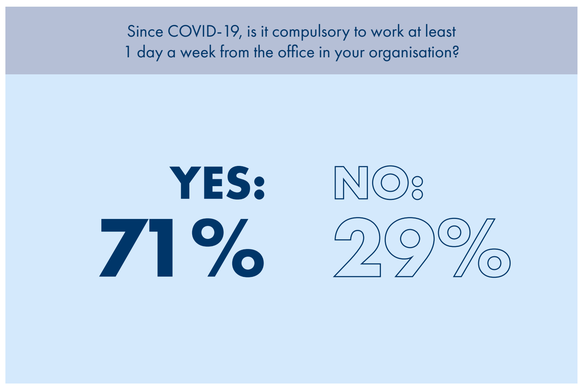

Figure 26: Compulsory to be in office one day a week

71% indicated that after Covid-19, it is a requirement to work at least one day a week at the office. This is a strong indication of hybrid working arrangements that many organisations have adopted.

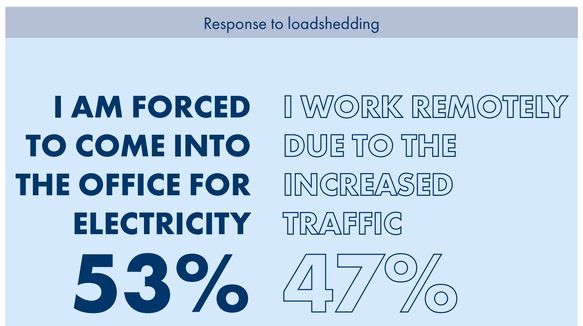

Figure 27: Response to load shedding

Due to the shortfall in electricity production, South Africa is in an unfortunate situation of load shedding. At times, load shedding schedules can be unpredictable and severe, with locations without power for hours at a time. This has had an impact on working conditions, as employees may not be able to work at home or face longer traffic times. The results of the question, 'What do you normally do when there is load shedding?' were almost even, with 53% saying that they are forced to come to the office for electricity and 47% indicating that they work remotely due to increased traffic.

Figure 28: More specialised cybersecurity skills

With more people working from home, there is a stronger reliance on ICT systems and infrastructure. This, in turn, increases the need for more specialised cybersecurity skills to ensure access and security. The survey supported this issue, with 77% indicating that their organisations needed more cybersecurity skills as people worked from home.

4.7 CHALLENGES FACED BY FEMALES

Challenges for females in cybersecurity roles	
Gender bias	44%
Discrimination	39%
Lack of awareness and representation	37%
Opportunity and progression limitations	28%
Educational hurdles	26%
Recruitment inclusivity issues	24%
Poverty and income streams	18%
Retention challenges	15%
Other (specify)	1%
Women are NOT facing any challenges	19%

Figure 29: Challenges faced by females

When examining the challenges faced by women in cybersecurity, the survey data highlights several key barriers that contribute to the under-representation of women in the field. Gender bias remains the most significant challenge. Women often face stereotypes and preconceived notions about their abilities in the technology sector, particularly in cybersecurity, which has historically been male-dominated. This bias can lead to women being undervalued, overlooked for leadership roles, and subject to micro-aggressions, making it harder to succeed or advance. Discrimination, both overt and subtle, continues to be a major issue. Women in cybersecurity may face unequal treatment in terms of pay, responsibilities and professional opportunities compared to their male counterparts. This can include discrimination in hiring practices. Furthermore, women often experience limited opportunities for career advancement in cybersecurity. This may be due to a lack of mentorship, exclusion from professional networks, or fewer leadership and growth opportunities compared to men.

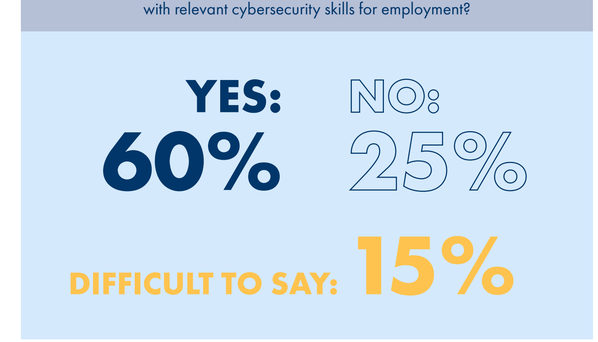

Figure 30: Difficulty in finding female employees

Survey data showing that 60% of companies struggle to find female employees in cybersecurity highlights a major challenge for organisations trying to diversify their workforce. A significant majority of companies report difficulties in hiring women for cybersecurity roles. This aligns with the challenges women face in the field, which include gender bias, discrimination, limited opportunities and educational barriers. Since fewer women pursue careers in cybersecurity due to these obstacles, the pool of qualified female candidates is smaller.

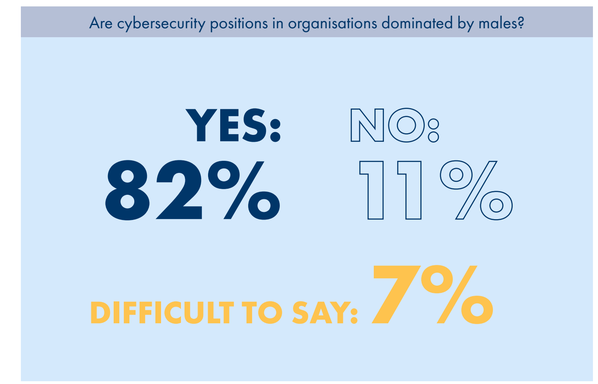

Figure 31: Male dominance in the cybersecurity domain

Survey data indicating that 82% of cybersecurity positions in organisations are dominated by men underscores a significant gender imbalance in the field. This overwhelming majority reveals that cybersecurity remains a male-dominated profession. Factors such as gender bias, discrimination and limited opportunities for women (as outlined previously) contribute to this imbalance.

CONCLUSION

Many organisations within South Africa have recognised the strong need for cybersecurity skills and have invested in building and maintaining the capability. A few organisations choose not to invest in cybersecurity as their business may be too small or they lack the finances to focus on cybersecurity; other companies are starting to look into the need for cybersecurity. Many cybersecurity positions remain unfilled, especially security managers, individual contributors and senior managers or directors of security. There is also a challenge in finding candidates with the necessary skills.

The most sought-after qualifications by employees and organisations are CISSP, CISA, CISM and CIPP. This shows that organisations are looking for critical skills to ensure security management, auditing and data privacy.

In general, organisations have a strong tendency for organisations to face challenges with both recruiting and retaining cybersecurity employees.

A growing requirement for cybersecurity workers will be the ability to work from home. After Covid-19 many members prefer to work from home. However, many organisations in South Africa require members to be in the office at least once a week. Thus, hybrid working conditions are currently the most popular approach.

For more information, visit **www.csir.co.za**

science & innovation
Department:
Science and Innovation
REPUBLIC OF SOUTH AFRICA

CSIR
Touching lives through innovation