Bridging the Gap

Identifying Challenges in Cybersecurity Skilling and Bridging the Divide

An action research study by

DSCI
PROMOTING DATA PROTECTION

Powered by

Microsoft

Knowledge provider

EY
Building a better working world

Abbreviations and acronyms

Abbreviation	Description
CS	Cybersecurity
PWD	Persons with Disabilities
CAGR	Compound Annual Growth Rate
Cert-In	Computer Emergency Response Team
CSR	Corporate Social Responsibility
NGO	Non-Governmental Organisation
DDOS	Distributed Denial of Service
SQL	Structured Query Language
MI	Machine Learning
IoT	Internet of Things
Ai	Artificial Intelligence
AR/VR	Augmented Reality/Virtual Reality
NFT	Non-Fungible Token
Sops	Standard Operating Procedure
KRA	Key Responsibility Areas
CSP	Cloud Service Providers
IITs	Indian Institute of Technology
NIT	National Institute of Technology
CEH	Certified Ethical Hacke
OSCP	Offensive Security Certified Professional
CISM	Certified Information Security Manager
CRISC	Certified in Risk and Information Systems Control

Abbreviation	Description
VMDR	Certification on Vulnerability Management, Detection and Response
OSCP	Offensive Security Certified Professional
CISSP	Certified Information Systems Security Professional
CRISC	Certified in Risk and Information Systems Control
TTPS	Tactics, Techniques, And Procedures
CTF	Capture the Flag
MOU	Memoranda of Understanding
CDAC	Centre for Development of Advanced Computing
ISACA	Information Systems Audit and Control Association
DSCI	Data Security Council of India
Isc2	International Information Systems Security Certification Consortium
CIS	Critical Security Controls
Fair	Factor Analysis of Information Risk
PCI DSS	Payment Card Industry Data Security Standard
GDPR	General Data Protection Regulation
MeitY	Ministry of Electronics and Information Technology
DGT	Directorate General of Training

Foreword

Vinayak Godse,
Chief Executive Officer
Data Security Council of India

Cybersecurity is becoming a board-level priority, given the diverse nature of cyber threats and rising monetary costs associated with data breaches. Globally, 88% of organizations report that their board now asks cybersecurity-specific questions. Heightened concerns of security and volume and complexity of challenges, demand of security skills is rising year by year. Cybersecurity is still formative profession. The challenges of the contemporary cybersecurity landscape, shaped and defined by geopolitical and macroeconomic turbulence make it different than other technology professions. The global cybersecurity workforce is expanding, but it is often met with acute shortage of skills. Efforts are witnessed to fill the worldwide gap of 3.4 million cybersecurity workers to protect cross-industrial enterprises from increasingly complex modern threats.

To comprehensively ascertain the current state of cybersecurity talent, we put together the effort of this study to examine it from multiple lenses, focusing on the experience level between 0 and 5 years. At the enterprise level, the executive spotlight is directly focused on the cybersecurity teams tasked with adapting to and protecting their organisations from escalating threats while adhering to emerging technological and regulatory requirements. A nuanced picture of the values and motivations driving Cybersecurity careers is derived from cultural, emotional, and educational perspectives.

Addressing the Diversity issue in the cybersecurity ecosystem, which appears to be lagging in the area, is another focus area of this study Diversity is incredibly potent, especially in Cybersecurity, where multiple perspectives are required to ensure a multifaceted and nuanced defence. The best defence against new and dangerous threats is the collaboration of teams from various regions, cultures, and backgrounds, as well as of varying genders. The field of Cybersecurity requires concentrated efforts to increase diversity. The Data Security Council of India, with industry support led by Microsoft, is making efforts to close gender and regional diversity gaps. One of the key purposes of this report is to create a diverse and equitable Cybersecurity workforce in the country. The report explores numerous facets of the Cybersecurity workforce. It examines the subject's evolution and its impact on employment creation, with a primary emphasis on early-stage careers. Through this report, we would also like to urge the industry to give diversity in its Cybersecurity workforce due consideration.

Foreword

Ashutosh Chadha
Director and Country Head Government Affairs & Public Policy
Microsoft India

Cybersecurity continues to be a significant threat for governments, businesses, society, and individuals around the world. From supply chain disruptions, ransomware attacks, phishing, and other, cybercrimes have become increasingly sophisticated. Furthermore, the threat landscape has become more diverse & challenging. These cybersecurity challenges are compounded by a workforce shortage; there simply aren't enough people with the cybersecurity skills needed to fill open positions across the cybersecurity spectrum & this remains a global problem. By 2025, there will be 3.5 million cybersecurity jobs open globally, representing a 350% increase over an eight-year period, according to Cybersecurity Ventures.

Microsoft has been laying significant emphasis on augmenting skilling ecosystem towards equipping young women and men in India to build career pathways in Cybersecurity. Further, we aim to catalyze the collaborative approaches viz., partnership with Non-Profits, Academic Institutions and with government organizations. Our interventions like CyberShikshaa has been working towards fulfilling two broad objectives: (1) creating & equipping youth from underserved and disadvantaged segment of society to build career in Cybersecurity (2) to address the diversity gap and lack of participation of young women in this domain, Cyber Shikshaa aims at fulfilling the both the objectives.

With the goal of more strategic and systematic approach towards Cybersecurity skilling, the research on "Bridging the Cybersecurity Skills Gap: Fostering Workforce Readiness through CSR and Partnerships" undertaken by Data Security Council of India, in knowledge partnership with Ernst & Young, and powered by Microsoft, will pave a definitive roadmap. The research shall further direct various stakeholders towards collaborations and designing targeted interventions to foster Cybersecurity skilling ecosystem. The research report highlights the specific need and targeted interventions for skills building & workforce readiness for young women in Cybersecurity. Further, we will strengthen programs with government organizations viz., DGT and NIELIT, to achieve broader scale & replication of the initiative across India. The research report shall further enable private sectors, academia and non-profit organizations to collaborate, design and deploy effective training models in this important domain.

Acknowledgement

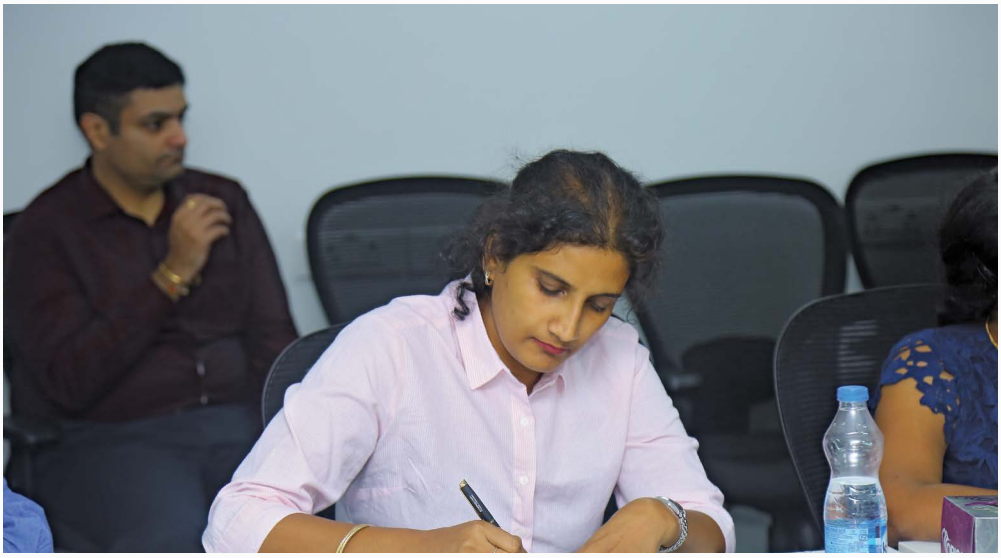
DSCI would like to express its sincere gratitude to the partners and stakeholders that supported and contributed to the action research on the Cybersecurity skill gaps. Their invaluable assistance and resources made this study possible and significantly enhanced its quality and impact.

We extend our heartfelt appreciation to Microsoft for their unwavering commitment in powering this study, recognizing the importance of addressing the skill gaps in the domain and addressing the same through their CSR programs. Their dedication to bridging the gaps between skills, opportunities, and social exclusion and their belief in the significance of this study are greatly acknowledged and appreciated.

We would also like to extend our thanks to EY, who served as a knowledge partner throughout the research process. Their expertise, insights, and guidance were instrumental in shaping the study, and ensuring its relevance. Their collaboration and commitment to knowledge sharing made a significant contribution to the overall success of this research.

Lastly, we express our gratitude to all the individuals and organizations who participated in interviews, shared their experiences, and provided valuable inputs for the research. Their willingness to contribute their time and knowledge was essential in capturing diverse perspectives and enriching the findings.

The completion of this research would not have been possible without the support and contributions of all those mentioned above. Their involvement has had a lasting impact on the quality and depth of this study, and we extend our heartfelt thanks to each and every one of them.




ORIGAMI
So..Soft

Table of Contents

Executive Summary

The global cybersecurity landscape is experiencing a growing concern due to the increasing number and severity of cyber threats. India, as a nation undergoing rapid digitization across various sectors, is not immune to these threats. The cybersecurity industry in India has gained significant importance and is expected to grow rapidly in the coming years. However, there is a noticeable gap between the demand and supply of skilled cybersecurity professionals.

This study aims to analyse the demand and supply of skilled cybersecurity professionals in India, identify technical and social factors contributing to the shortage of skilled professionals, and explore solutions to address these gaps through CSR and multi-stakeholder approach.

The methodology employed a mixed-methods approach, utilizing existing reports, articles, papers, and related resources from private and government agencies in the cybersecurity and skill development domains as well as primary data through stakeholder interactions. The sample size included companies employing cybersecurity professionals, employed professionals, representatives from NGOs and training providers, academic institutions, trainers, and students/aspirants enrolled in cybersecurity courses. The study involved an extensive literature review, identification of key stakeholders, preliminary consultations, development of data collection tools, and data collection through interviews and questionnaires. The collected data was analysed to identify patterns, trends, and gaps in the skilling ecosystem within the cybersecurity sector.

Findings of the study

- More than 70% of the Cybersecurity professionals covered in the study revealed that the top three attacks that are expected to see substantial rise in the near future are phishing, smishing, and vishing attacks, followed by ransomware attacks and zero-day exploit. Furthermore, respondents stated that the three major trends that will catalyse the demand for Cybersecurity are a) use of AI, ML and IoT by hackers resulting in increasing Cybersecurity attacks, b) growing regulatory liabilities and c) excessive usage of digital platforms resulting in exchange of large amount of data. This highlights the needs for organizations to perform risk assessments at regular intervals and have robust security measures.
- Almost half (47%) of the corporates stated that Cybersecurity professionals constitute less than 5% of their company's overall workforce. This indicates that Cybersecurity professionals are relatively scarce in the workforce at present. However, 47% of respondents also mentioned their goal to increase these professionals in next 5 years by more than 30% of the current Cybersecurity workforce.
- Presently, 43% corporates have women participation between 21%-40% of the overall Cybersecurity workforce. However, in next 5 years, 82% corporates have plans to increase the participation of women by at least 5% of the existing workforce, with 35% stating that they plan to increase the participation by at least 15% in the same period. Furthermore, only 12% corporates responded that they have onboarded PwDs in the Cybersecurity workforce.In the same period, while majority of respondents have defined their goals to recruit PwDs in their workforce, around one-third of the corporates stated they still don't have any plans and policies to onboard PwDs. It is also important to highlight that while companies may have planned their targets for inclusion of PwDs, the inclusion of PwDs in Cybersecurity skilling programmes and courses offered by training providers/NGOs and academic institutions remains considerably low at 0.12% and 4%. This may lead to a gap in social inclusion of diverse groups within the workforce. Considering these findings, there is a need for training providers/NGOs to promote inclusion of diverse groups and formulate strong inclusive programs that can specifically cater the needs of PwDs.
- Cybersecurity Risk Analyst, Cybersecurity Analyst, and Penetration Tester are the most prevalent job roles at present, as identified by more than 50%

Cybersecurity professionals. In the next 5 years, job roles that are expected to surge include DevSecOps Engineer, IoT Engineer, Analyst IoT Security and Analyst Operations Technology.

- Over the next 5 years, there will be an increased demand for specific technical skills and competencies. Skills and competencies that will be given high prominence, as identified by the professionals are Artificial Intelligence (56% as compared to 0% present), Data Forensics (44% as compared to 17% at present) and Hacking Wireless Networks (28% as compared to 0% at present) followed by Cloud Security, Compliance and Regulatory Knowledge and Security Auditing. Furthermore, these have also been identified as skills in which gaps exist among early talent. To meet future demands, there is a need for multi-stakeholder collaboration to map industry-relevant skills, design and deliver skilling programs as per industry standards, promote corporates driven training initiatives and ensuring validation of content to avoid disparity.
- 75% students from Cyber skilling programs driven by CSR who participated in the study have not enrolled or completed any certification on Cybersecurity for which they are eligible. Considering the growing demand, it's important to sensitize students and academic institutes about the value added by these certifications in their career. Corporates can play a pivotal role in addressing these certification gaps by incorporating and sponsoring Cybersecurity certification as a part of their skilling initiatives.
- Out of the NGOs interviewed for the study which are providing training in cybersecurity, more than half reported a placement rate of 50% in the domain. However, to mitigate the gap and to ensure increase in the placement percentage of students NGOs/Training providers can pool in resources and expertise to create large-scale programs, re-define implementation strategies with multi-stakeholder partnerships, ensure active involvement and participation of students in hackathons.
- Academic institutes and training providers/NGOs have expressed a desire to strengthen the existing partnerships and collaborate with each other and with government stakeholders for development of content, capacity building of trainers etc. Furthermore, government organizations are looking forward to collaborating as well, where they can support in designing training frameworks, developing, and curating of content and getting approved from National Council for Vocational Education and Training (NCVET).
- Corporates contribute to skilling initiatives by providing financial resources, bringing the technical expertise and resources to develop the comprehensive programs, fostering partnerships, and promoting collaborations among different stakeholders. It has been identified that all the CSR professionals interviewed as a part of the study stated that they want to collaborate with other stakeholders in the ecosystem for strengthening the Cybersecurity landscape. CSR professionals showed interest in implementation and expansion of interventions in Cybersecurity, collaborate for development of content, organizing mentoring sessions for faculties and students, and supporting in employment opportunities.

About the Study

Cybersecurity dates back to the early days of computing and network development when the need for security measures grew more apparent as computers and networks became increasingly interconnected. As technology evolved, so did security challenges, leading to the development of more sophisticated protective measures such as firewalls, intrusion detection systems, and threat intelligence platforms. In recent years, new approaches such as identity and access management and cloud security have emerged to address evolving security challenges. The global Cybersecurity scenario is one of increasing concern and importance, as the number and severity of cyber threats continue to rise. Cyber-attacks are becoming more sophisticated and frequent and can result in significant financial and reputational damage for individuals and organizations alike.

India, as a nation, is rapidly digitizing across various sectors, and as a result, is not immune to cyber threats. The Cybersecurity industry in India has gained importance in recent years and is expected to grow at a significant pace in the future. Key threats like the rise of ransomware, growth of IoT and cloud security, and shortage of skills have compelled organizations to increasingly invest in Cybersecurity technologies and services. Governments and industry groups are also working together to improve Cybersecurity standards and best practices, and to raise awareness about the importance of Cybersecurity among individuals and organizations.

The Cybersecurity sector in India is driven by various factors such as the growing use of digital technologies, rising cybercrime, and an escalating need for Cybersecurity in various sectors including finance, healthcare, and education. According to a report by NASSCOM, the Indian Cybersecurity market is expected to reach $35 billion by 2025, growing at a compound annual growth rate (CAGR) of 15.6%. The surge in demand for Cybersecurity services and solutions is fuelled by the growth of e-commerce, the rise of cloud computing, and the increasing use of mobile devices and social media. However, despite the sector's growth potential, the Cybersecurity industry in India faces several challenges. One of the primary problems is the shortage of skilled Cybersecurity professionals. This gap between demand and supply of such Cybersecurity talent has become a major concern for the industry. The lack of awareness about the importance of Cybersecurity is another major challenge confronting the Cybersecurity sector. Many businesses and individuals do not fully understand the risks associated with cyber threats and do not take adequate measures to protect themselves. This has led to a high incidence of cybercrime in India, and a large number of incidents are reported each year.

To address these challenges, stakeholders in the ecosystem have implemented several initiatives to promote Cybersecurity in the country. These include the Indian Computer Emergency Response Team (CERT-In), set-up by the Government of India, to provide guidance and support in the event of cyber incidents; programs like Cyber Shikshaa, implemented by Microsoft and Data Security Council of India, to skill professionals in the Cybersecurity domain and to generate awareness of cyber- security among people. However, there is still a deficit of skilled workforce to cater to the ever-expanding horizon and demands of the sector and there is a strong need to identify these gaps and opportunities in the Cybersecurity domain.

This study was conceptualised to map the gaps that may exist in the companies' expectations from professionals entering the Cybersecurity domain and the skills and knowledge possessed by these professionals. It was designed to encompass a multi-stakeholder perspective mapping across the skilling supply chain. The goals of the study were to:

- Analyse the demand and supply of skilled Cybersecurity professionals in India and identify the factors contributing to the shortage of skilled professionals.
- Identify the skills and knowledge gaps in the Cybersecurity workforce in India and explore potential solutions to address these gaps.
- Examine the impact of external stakeholders to identify areas of opportunities in bridging the skill gaps through CSR.

The study is primarily descriptive in nature and uses mixed methods based on secondary and primary data and information. It used existing reports pertaining to Cybersecurity, articles, papers and related books, as well as websites of private and government agencies working for Cybersecurity and skill development through CSR.

Approach of the study:

- **Secondary research:** Extensive literature review and secondary research to gather information on the Cybersecurity sector, job requirements, industry trends, and existing skill gap studies. Academic journals, industry reports, government publications, and other relevant sources to gain insights into the current state of the sector were reviewed. This included mapping industries offering roles for Cybersecurity professionals, suitable job profiles for professionals with 0-5 years of experience, and challenges faced by professionals, trainers, and employers in the sector. Secondary research also included assessing the existing training landscape for Cybersecurity professionals.
- **Stakeholder mapping:** Key stakeholders involved in the Cybersecurity sector and skilling of professionals were identified. The mapping included Cybersecurity professionals, employers, trainers in NGOs and training centers, management of training institutes/ academic institutions, candidates being trained on Cybersecurity skills, and students - to understand their perspectives, needs, and contributions to the sector.
- **Preliminary consultations:** After identifying stakeholders, preliminary consultations were conducted with a small sample of each stakeholder group to understand their perspective on the Cybersecurity sector as well as gaps in their respective area of work.
- **Development of survey tools:** Data collection tools for interviews tailored for each stakeholder group were developed. The tools captured relevant information related to opportunities, job requirements, skills, competencies, challenges, and training offerings in the Cybersecurity sector, among other aspects.
- **Data collection:** Primary data was collected from stakeholders through one-on-one interviews a digital questionnaire. Telephonic/Virtual interactions with companies/employers to understand the available opportunities, job profiles, and required skills were held. In-person interactions were also held with training providers/NGOs/academic institutions to understand their course offerings, content, and trainer competency. Further, data was collected from candidates to assess their existing skills, knowledge, and awareness of career prospects in Cybersecurity.
- **Data Analysis:** Collected data was analysed to identify patterns, trends, and gaps across the skilling ecosystem in the Cybersecurity sector. The requirements of employers were compared with the skills and competencies possessed by existing Cybersecurity professionals. Finally, gaps were identified in training offerings, curriculum, and the skill level of candidates.
- **Recommendations:** Based on the research findings, recommendations are provided for bridging identified gaps in the Cybersecurity sector, enhancing training programs, improving industry-academia collaboration, promoting awareness among candidates, and aligning skill development with industry requirements.

Chapter 1

Key insights about the importance of Cybersecurity; Latest trends and technology that will grow the demand for Cybersecurity.

This Chapter provides a holistic view of the increasing significance of Cybersecurity among corporates. It also highlights the expected rise of cyber-attacks and their impact on the Cybersecurity landscape. It delves into the trends that will drive the demand for the domain and discusses the technology contributing to its challenges.

Background

Digital electronics is among the most disruptive technological developments that the world has experienced in the last century. Globally, organizations and individuals produce and consume colossal quantities of digital data every day. The World Economic Forum estimates that in 2020, the digital universe would have measured 44 zettabytes (44,000,000,000,000,000,000,000) and this must only have increased since then.

With rising digital literacy, improved connectivity, and technology becoming easier to use, we are seeing a massive proliferation of data. The world is also experiencing a corresponding increase in cyber-attacks. Adversaries have devised sophisticated methods to access and steal confidential or personal information, compromise the integrity of information systems, harm businesses and government services, and execute other forms of cyberattacks.

The importance of Cybersecurity in today's hyper connected world cannot be overstated. Artificial intelligence (AI), machine learning (ML), cloud computing, data analytics, and the internet of things (IoT) are examples of digital technologies that are gaining currency and highlight the need for sophisticated defences against cyberattacks that could seriously undermine governments, businesses, other organizations, and people.

What is Cybersecurity?

The main goal of Cybersecurity is to safeguard data and all its essential components, including the hardware and software used for data generation, use, storage, transfer, and destruction. It is used to prevent unauthorised users from accessing, using, disclosing, disrupting, altering, or destroying data. Using appropriate precautions, Cybersecurity measures assist individuals and organizations to secure confidentiality of information, preserve its integrity, and enable authorized users to access and use it when required. Thus, Cybersecurity measures help organizations and people protect assets such as information, business functions, technology, financial standing, and reputation among others.

Cybersecurity can be described in different ways, for example:

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, Cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization. (What is Cybersecurity? | IBM)

Cybersecurity is a set of processes, best practices, and technology solutions that help protect your critical systems and network from digital attacks. (What is Cybersecurity? | Microsoft Security)

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

However, a single underlying theme is common to all definitions, i.e., using digital technology to shield sensitive information, electronic devices, and networked IT systems against digital attacks.

The Need for Cybersecurity

Cyberattacks can take many different forms and often make use of malware. Short for malicious software, malware is a term used to describe destructive software that hackers use to gain access to sensitive information. Malware is characterized by the adverse use for which it is intended, rather than by the technology used to develop it.

The most common types of cyberattacks are briefly described below.

Phishing: an act in which a target person/group receives an email, phone call or text message from a sender pretending to be a legitimate entity, luring them into disclosing sensitive information such as personal details, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

Hacking: an attempt to take advantage of a private network or computer system. Hacking involves unauthorised access to or control over computer network security systems for illegal purposes.

Hacktivism: a combination of the word's hacker and activism, hacktivism is a form of hacking that is typically not motivated by monetary gain; rather it is done to promote a cause or hinder opposition. For example, a religious, environmental, or other activist may gain access to a system to promote their own cause or create disruption for the opposition.
SQL Injection: this is a commonly used web hacking technique to steal, delete, modify data etc. to compromise websites that use SQL databases e.g., online stores, forums, or blogs.

Ransomware Attack: a type of malware attack in which the target's data is encrypted or locked until a ransom is paid to the attacker.

Denial of Service Attack: in a denial-of-service (DoS) attack, a computer or other device is rendered unavailable to its intended users by interfering with the device's regular operation. A targeted machine is usually flooded with requests until normal traffic cannot be processed, and additional users are denied service.

Man in the Middle Attack: man-in the middle (MitM) attacks are those in which a cyber attacker is positioned between communicating parties and intercepts or passively listens to communication with the intention of stealing sensitive information, spying, corrupting data etc.

Data Leakage: unlawful electronic data communication from within an organisation to a receiver or location outside of it. Threats of data leakage typically include the internet and email, but they can also involve portable data storage devices like optical media, USB keys, and laptops.

According to the Annual Threat Report 2022, by Quick Heal Technologies Ltd., 398 million[1] malwares were detected worldwide among their customers with Windows operated systems while among customers with Android systems, 56% of detections comprised malware.

The enhanced risk of cyberattacks is also evident in the large number of incidents addressed. In 2020, the Computer Emergency Response Team, CERT-In handled 1,158,208 incidents which spanned a variety of activities such as website intrusion and malware propagation, malicious code, phishing, distributed denial of service (DDoS) attacks, website defacements, unauthorized network scanning/probing activities, ransomware attacks, data breach and vulnerable services.

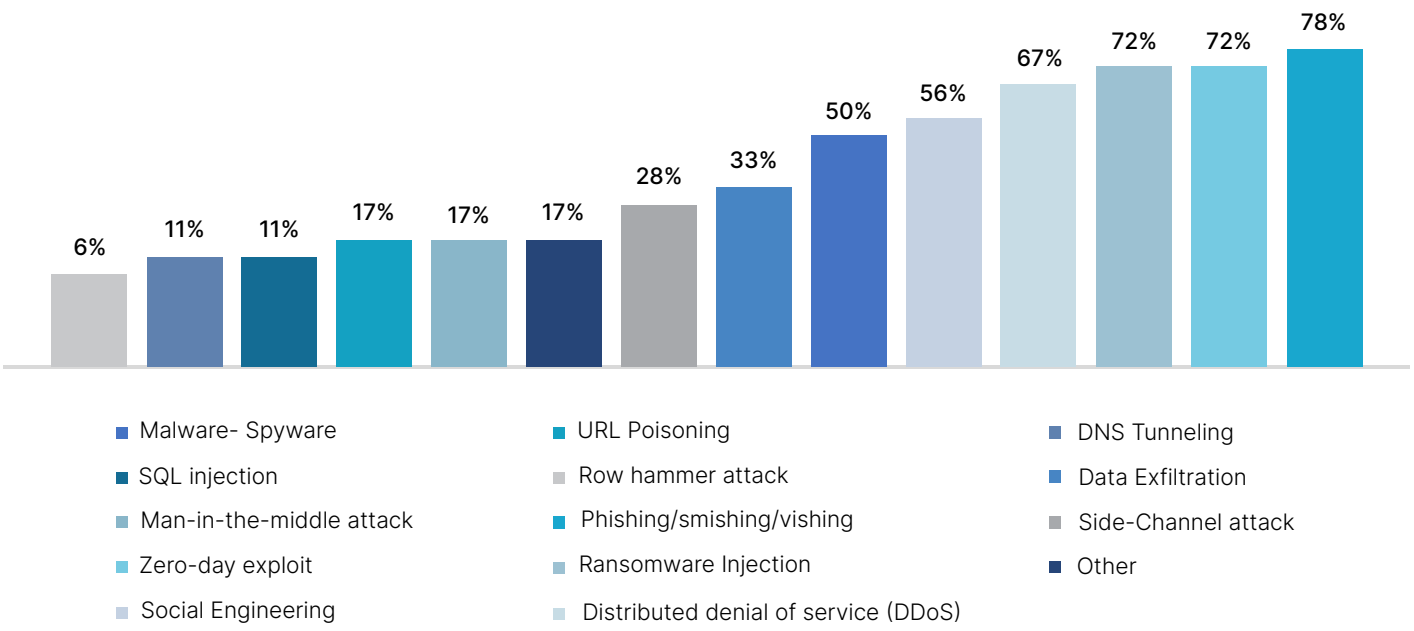
As per the figures reported by CERT-In, the number of cyber-attacks has increased from 41,378 attacks in 2017 to 14,02,809 attacks in 2021. However, in November'2022 12,67,564 attacks were reported by them.

In recent times, several cybersecurity breaches have occurred in India leading to huge financial loss and data breaches. Online payment gateway Razorpay experienced a loss of INR 7.3 crore in just three-month period. Another incident, where Juspay, faced a cyber-attack, led to leakage and sale of customer data of 100 million users of Amazon, Flipkart, Airtel, and Jiomart.

In another incident, Tech Mahindra faced a loss of INR 35 crores due to a ransomware attack while handling the Smart City project for the Pimpri Chinchwad Municipal Corporation. Mobikwik, the mobile wallet and payments application also experienced security breach which included details like KYC details, Aadhaar card information, signatures of nearly 100 million users, the data for which was available for sale on a hacker forum on the dark web. These incidents emphasize an urgent need for and importance of robust cybersecurity measures in India for mitigating the risks associated with it.

[1]QH Annual Threat report 2023 (quickheal.co.in)

Figure 1: % Increase in cyber-attacks in next 5 years



Cybersecurity professionals who participated in the study were asked about threats that they expect will rise in the near future.

More than **70%** professionals indicated that phishing, smishing, and vishing attacks, followed by Zero-Day exploit and ransomware attacks, are projected to increase significantly.

These findings are a major concern for businesses and individuals, as the financial and operational implications can be severe. Additionally, DDoS attacks are expected to surge as indicated by 67% respondents.

Other types of cyber-attacks, such as data exfiltration attacks, SQL injection, man-in-the-middle attacks, DNS tunnelling, URL poisoning, side-channel attacks, and row hammer attacks, are also predicted to increase in varying levels, but to a smaller extent. As evident from stakeholders' perceptions, vigilance, proactive defence strategies, and investment in Cybersecurity infrastructure and skills are crucial to mitigate the risks posed by these emerging threats.

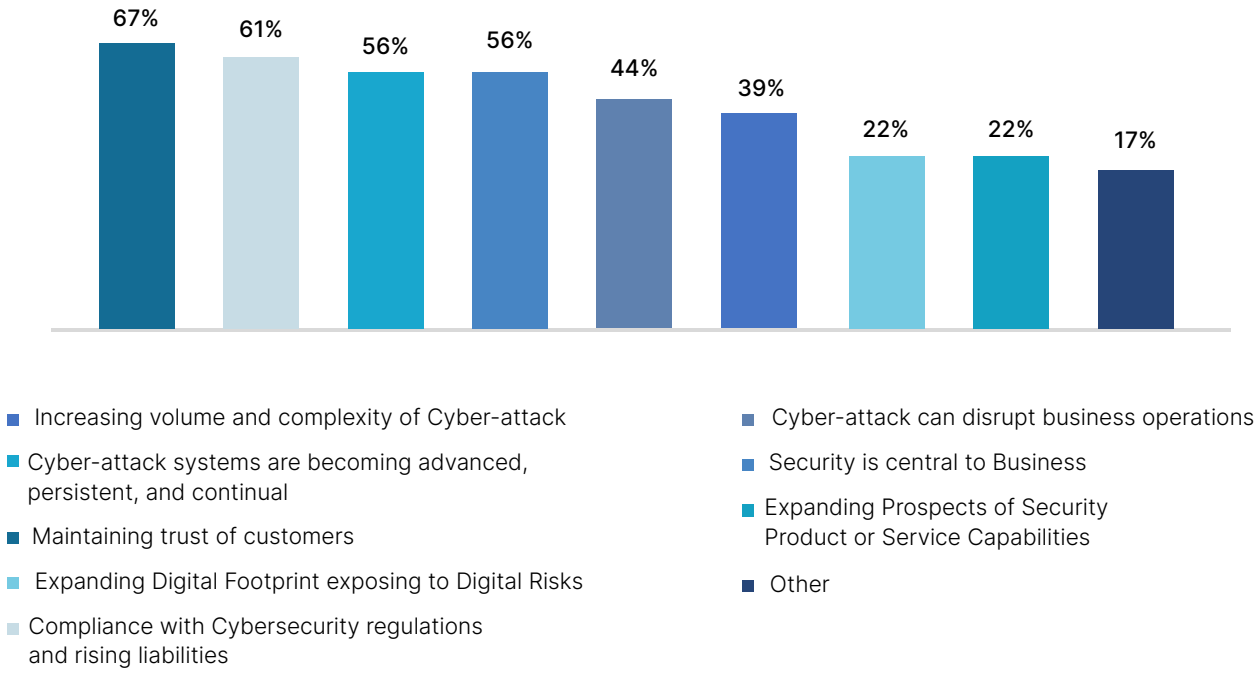
Importance of Cybersecurity for corporates

Governments, businesses, and other organizations are accelerating the adoption of digital processes and society is becoming more digitally savvy and reliant on technology in many aspects of daily life. The internet has impacted life in ways few could have imagined; not only is it integral to how businesses operate, but social media has also revolutionized social and professional interactions. Technology underpins financial transactions and wealth creation as well as the way goods and services are made available; it has also generated learning platforms that are changing the education landscape.

As a result of these advances, the availability of new technologies and the digitization of sensitive information, the environment has become more fertile for cyberattacks. Simultaneously, the types and numbers of threats and attacks are also on the rise. Consequently, cyber attackers, also known as threat actors, have tremendous opportunity to inflict harm in a variety of ways and to varying degrees.

Cybersecurity thus assumes a highly significant role. Key among the reasons for emphasizing security and protection is that the harm inflicted can be costly – financially as well as in intangible terms - for those impacted. According to IBM's Cost of a Data Breach 2022 Report, the average total cost of a data breach in India touched Rs. 17.6 crores in FY 2022, an increase of 6.6% from Rs 16.5 crores the previous year and 25% higher than Rs. 14 crores in 2020.[2]

Figure 2: Importance of Cybersecurity for Corporates



Interactions with Cybersecurity professionals clearly revealed the growing importance of Cybersecurity for businesses. 67% of respondents acknowledged that Cybersecurity is important to maintain the trust of customers. While 61% stated that compliance with Cybersecurity regulations and rising liabilities are significant concerns. Over half of the respondents (56%), also indicated that security is central to their business, Cyber-attacks are becoming advanced, persistent, and continual, and hence, it is essential to maintain a secure digital environment.

[2]India's average cost of a data breach touched all-time high in FY22: IBM - The Hindu

Other factors that make Cybersecurity important for corporates include:

- Cyber-attacks have the potential to disrupt business operations
- Increasing volume and complexity of cyber-attacks
- Higher vulnerability to digital risks arising from improved security product or service capabilities, and expanding digital footprint

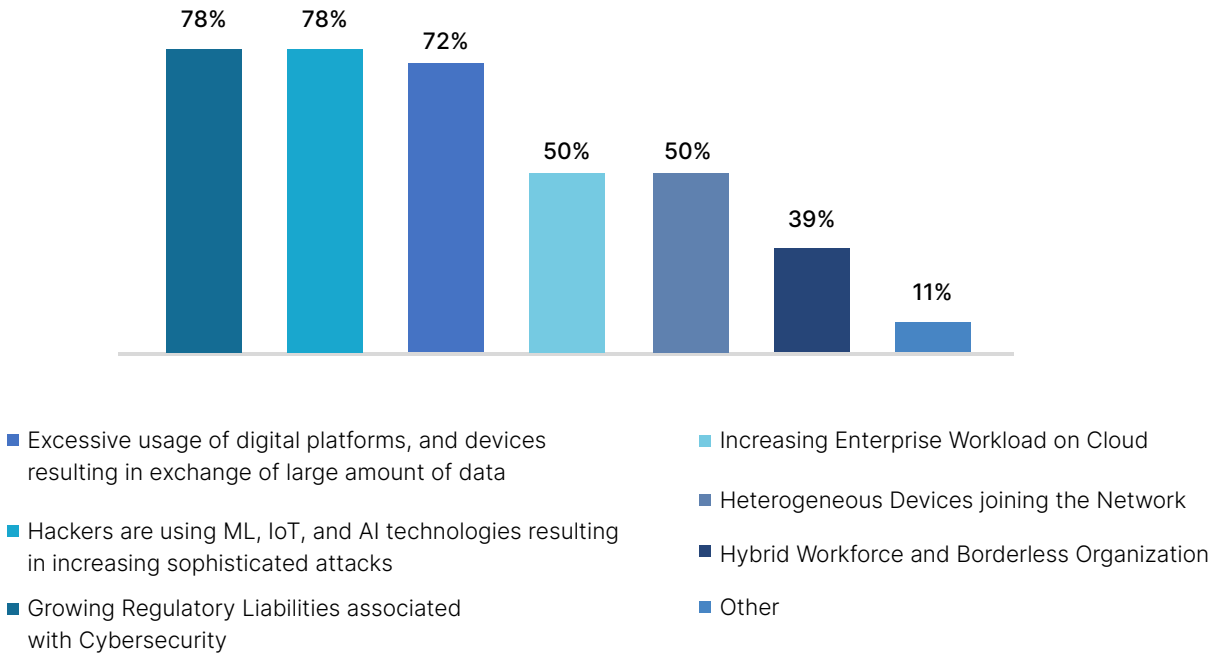
Overall, the findings demonstrate the multifaceted importance of Cybersecurity for companies, encompassing factors such as the increasing threat landscape, customer trust, digital risks, compliance, operational continuity, and business prospects.

Trends that will grow the demand for Cybersecurity

As the digital landscape continues to expand at an unprecedented rate, so does the scope and complexity of cyber threats. The importance of robust Cybersecurity measures has become increasingly evident, with organizations across industries grappling with sophisticated attacks and data breaches. In this ever-evolving landscape, staying ahead of the curve is crucial to safeguard sensitive information and maintain trust in digital infrastructure. To that end, understanding the emerging trends that will shape the future of Cybersecurity becomes imperative.

Interactions with professionals revealed that 78% of them recognize that hackers utilize emerging technologies such as machine learning (ML), Internet of Things (IoT), and artificial intelligence (AI) to carry out increasingly sophisticated attacks. The same percentage (78%) of respondents have also identified growing regulatory liabilities as the key emerging trend. Further, the high use of digital platforms and devices, resulting in the exchange of large amounts of data, is another significant trend that was identified by 72% of the respondents.

Figure 3: Trends that will grow the demand for Cybersecurity

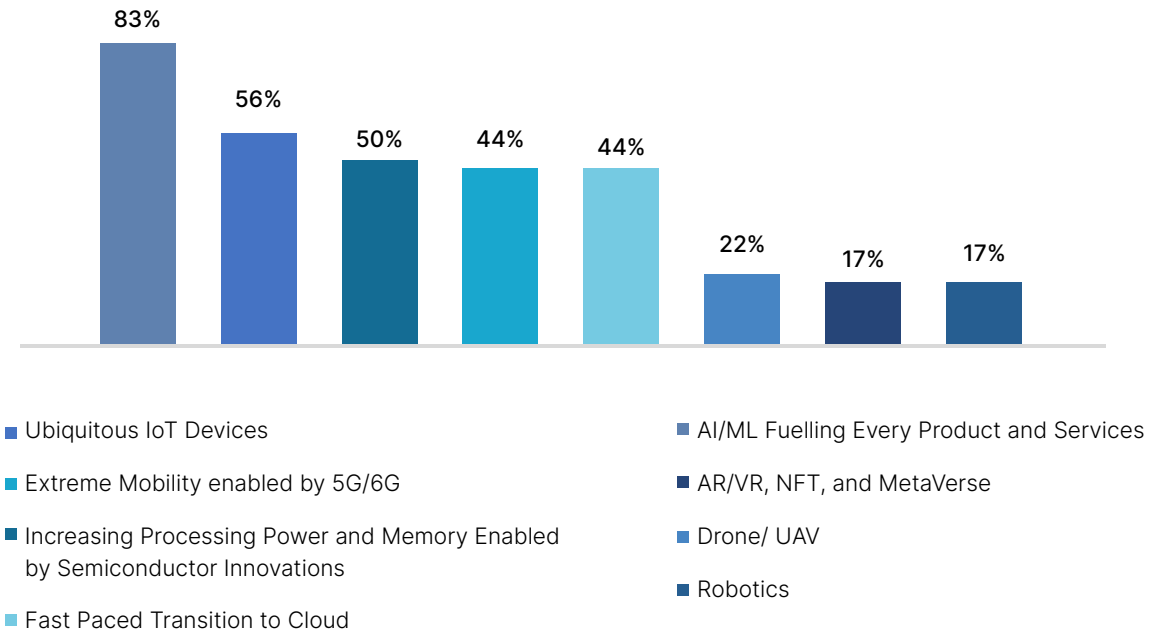


The proliferation of heterogeneous devices joining the network, and increasing enterprise workload on cloud platforms, identified by 50% of the respondents, poses significant Cybersecurity challenges. With the advent of the Internet of Things (IoT) and the interconnectedness of various devices, securing these devices and the data they generate becomes crucial to prevent potential breaches. The rise of hybrid workforces, prevalence of remote work, and borderless organizations were acknowledged by 39% of the respondents as factors that will drive the demand for Cybersecurity.

Technology that will lead to significant Cybersecurity challenges

The convenience that technology brings are accompanied by an increasingly complex array of cyber threats. The connectivity, automation, and efficiency that empowers businesses and individuals may also create vulnerabilities that can be exploited by malicious elements.

Figure 4: Technology that would lead to Cybersecurity challenge

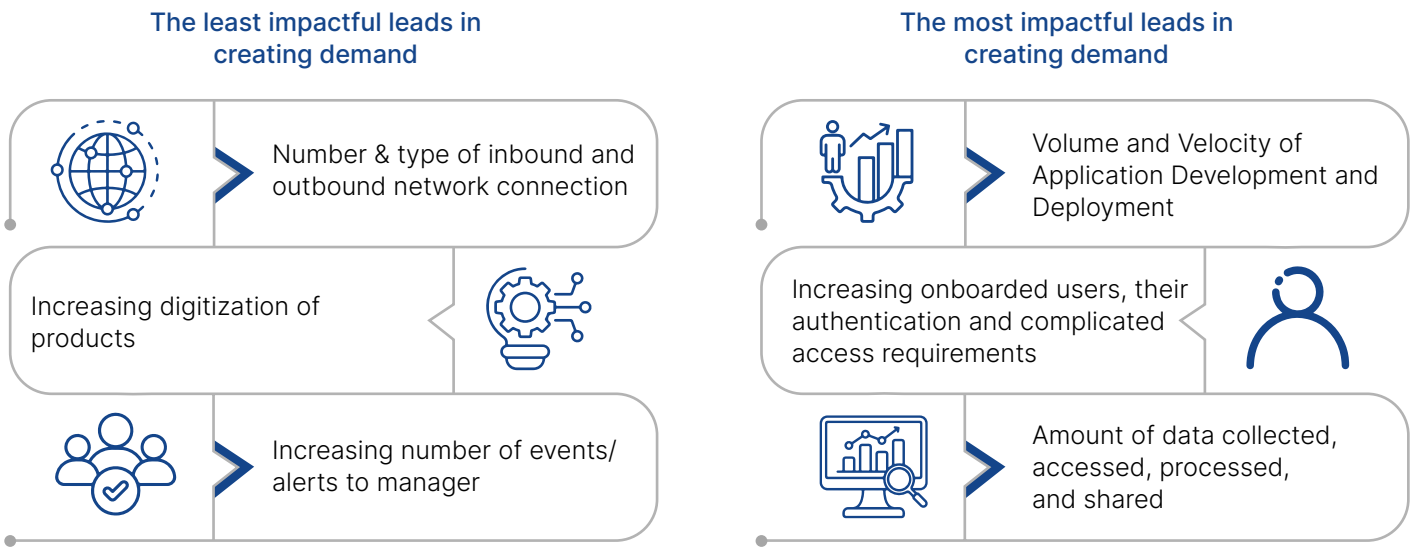


When asked about the technologies that may lead to Cybersecurity challenges, artificial intelligence, and machine learning (AI/ML) fuelling several products and service emerged as the most prominent concern among Cybersecurity professionals as 83% of respondents recognized their potential threats. The threats arising from ubiquitous Internet of Things (IoT) devices were mentioned by 56% respondents while 50% identified increasing processing power and memory enabled by semiconductor innovations as areas of concern Extreme mobility enabled by 5G/6G networks, and the fast-paced transition to cloud computing were considered significant Cybersecurity challenges by 44% of respondents each.

Additionally, 22% viewed drone/UAVs as posing Cybersecurity challenges. Further, (17%) of respondents perceived AR/VR, NFT, and metaverse technologies and robotics as threats Cybersecurity due to their potential vulnerabilities and privacy concerns associated with them.

Leads in creating demand for Cybersecurity skills

Figure 5: The most & the least impactful factors in creating demand for Cybersecurity skills



In today's digitally connected world, the demand for Cybersecurity has grown exponentially. With the increasing frequency and complexity of threats, organizations are in need for robust security and protection measures, resulting in greater demand for solutions and Cybersecurity skills.

Cybersecurity professionals who participated in the study were asked about the leads that will create the demand for Cybersecurity skills. As shown in Figure 5, the most impactful lead as opined by the respondents which is going to create a demand for Cybersecurity is a) volume and velocity of application development and deployment, followed by b) Increasing onboarded users, their authentication and complicated access requirements and c) amount of data collected, accessed, processed, and shared.

Chapter 2

Key insights about the present state of affairs and tracking the growing demands for Cybersecurity professionals in different cyber job roles

This chapter explores the present state of the Cybersecurity workforce and the goals defined to strengthen the workforce in the next 5 years. It sheds light on the most relevant job roles within the Cybersecurity ecosystem, emphasizing the diverse skill sets and competencies required as per industry standards. The chapter also shed lights on the job roles that are expected to be in greater demand in Cybersecurity landscape.

Trends in Onboarding Cybersecurity Professionals

Cybersecurity services in India have potential for immense development given the rising role of the digital economy, the rapid adoption of digital payments, and internet based financial transactions, among other factors. In addition, the adoption of contemporary technologies such as AI, ML, cloud computing, IoT, data analytics in business functions points to the need for Cybersecurity as an essential function in all organizations.

The Cisco Annual Internet Report estimates that India will have over 907 million internet users by 2023.[3] As digitalization gains momentum, Indian governments have acknowledged the expanding Cybersecurity risk environment and have taken various measures to address and mitigate it.

With India having assumed presidency of the G20 in 2023, the Ministry of Electronics and Information technology (MeitY) has launched the G20 Digital Innovation Alliance (G20-DIA). This aims to showcase innovative solutions and bring together innovation ecosystem players, (including start-ups, investors, mentors, and institutions who are building digital public goods/innovations) with a view to growing economies and benefitting communities. MeitY has selected various themes to focus on and secured digital infrastructure including Cybersecurity are among these.

In the private sector, several Indian companies have established their own security operations centres (SOCs) to monitor, and address cyberattacks. Further, businesses continue to deploy advanced Cybersecurity solutions to protect their networks and data.

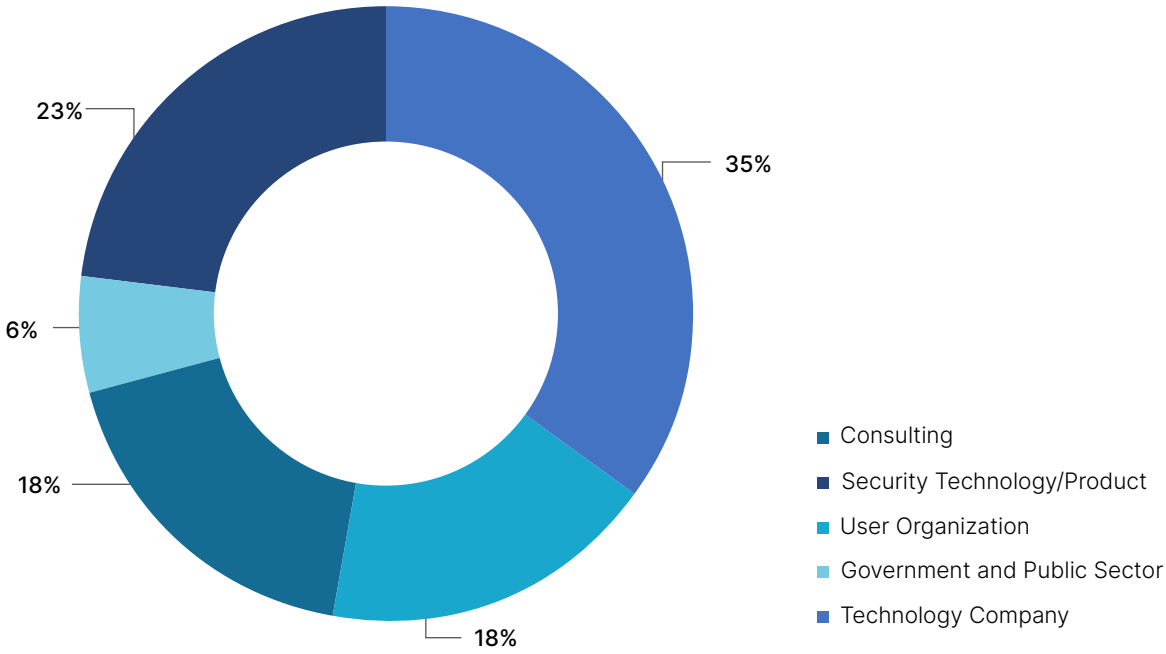
While India has taken steps in the right direction, managing Cybersecurity risks, and protecting the country's infrastructure, businesses, and people against them is a herculean task. With technology becoming accessible, threat actors are using it in more sophisticated ways to inflict serious harm to organizations and individuals. Appropriate responses to the expanding threat environment require to be equally or more sophisticated and require affordable solutions and a growing pool of skilled professionals to implement them. Unfortunately, Cybersecurity professionals are in short supply the world over and according to Microsoft, there will be 3.5 million open Cybersecurity roles globally by 2025.[4]

In India, 66% of corporates reported at least one cyberattack in 2021 and the demand for Cybersecurity professionals has grown by ~ 51% since then. The country's Cybersecurity workforce is about 135,000 strong and an additional 68,000 are required to meet the sector's requirements.[5] This is corroborated in a joint study by the Data Security Council of India and Future skills Prime (a MeitY -NASSCOM digital skilling initiative) which estimates that the country needs 53 million trained professionals (excluding fresh hires) to effectively contain cyber threats that emanate from a rapidly expanding digital environment. Considering the growing need for skilled Cybersecurity professionals in India, it is critical that this workforce is be developed urgently and key challenges addressed to meet this objective.

The study covered a range of organizations representing different sectors and industries. The purpose was to assess the trends in onboarding Cybersecurity professionals across these organizations. Among them, technology companies formed the largest group, representing 35% of the participants. This category included companies in IT/ITES, Quantum Computing, BPO, and Technology Consulting. Security technology/product companies accounted for 23% of the participants, covering industries such as Cybersecurity, IoT security, and Transportation and Logistics. User organizations and consulting firms both comprised of 18% of the respondents inclusive of finance, and BFSI (Banking, Financial Services, and Insurance) companies. The rest were government/public sector companies represented by the banking sector.

[3]India will have over 907 million internet users by 2023: Report | Technology News,The Indian Express
[4]Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries - The Official Microsoft Blog
[5]Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries - The Official Microsoft Blog

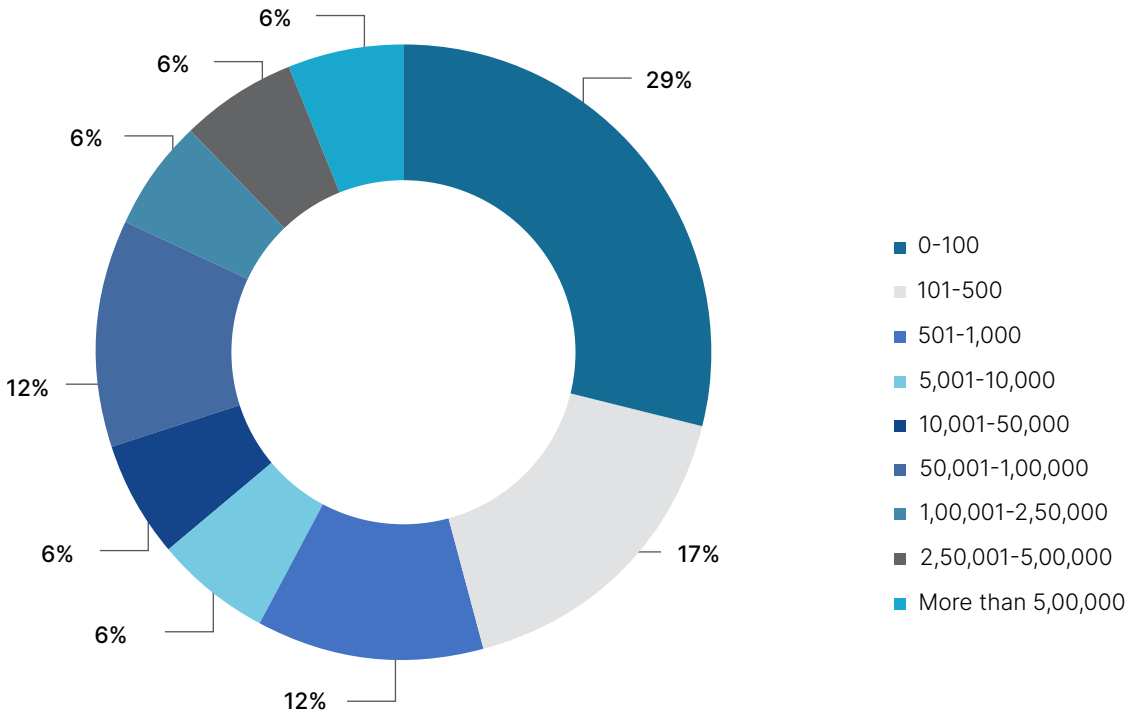
Figure 6: Types of organizations covered



Overall workforce

The majority of respondents (58%) shared that their company's current strength in India is 1,000 employees, indicating a relatively small workforce. The sample also comprised of large companies with 18% respondents having a workforce of more than 100,000.

Figure 7: Organization overall workforce



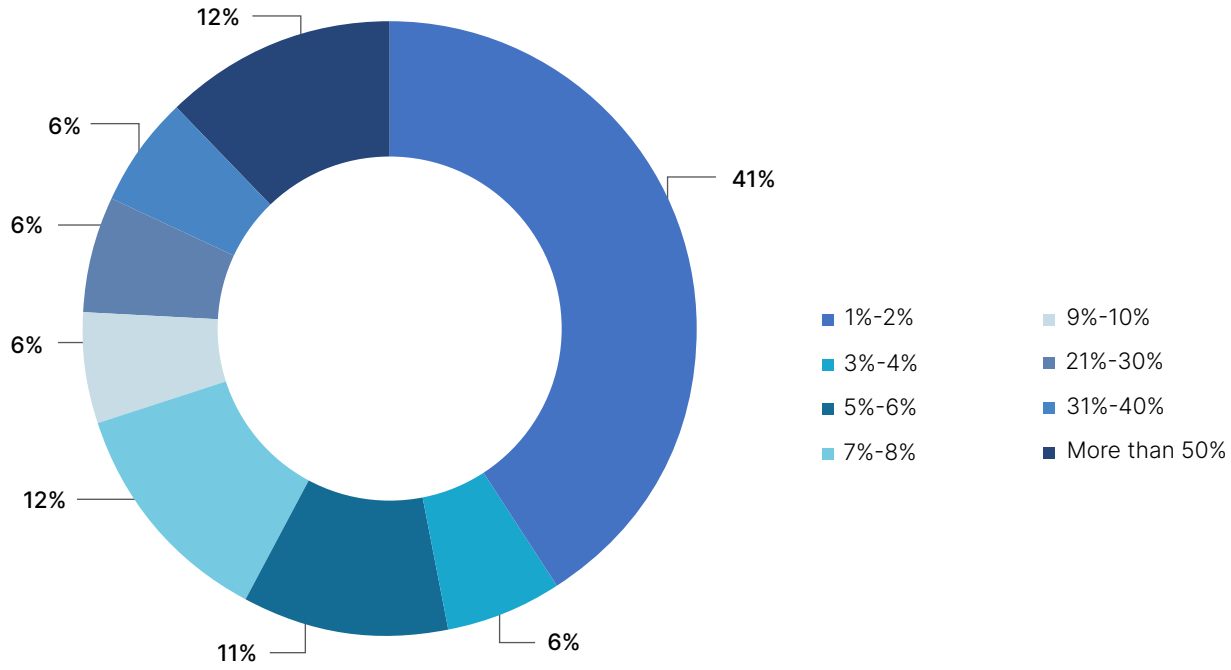
Cybersecurity workforce at present

The demand for Cybersecurity professionals has surged in recent years, reflecting the growing importance of securing digital assets and protecting sensitive information. The current Cybersecurity workforce is characterized by a highly dynamic landscape and a persistent shortage of skilled professionals to meet the rising demand. As organizations across various sectors face increasingly sophisticated cyber threats, the need for a robust and qualified workforce has become paramount. However, the demand for Cybersecurity expertise far exceeds the available talent pool, leaving many companies vulnerable to potential breaches and data compromises.

Figure 8 shows: Almost half of the respondents (47%) stated that Cybersecurity professionals constitute less than 5% of their company's overall workforce. This indicates that Cybersecurity professionals are relatively scarce within organizations, with a smaller proportion allocated to this specific role compared to other functions.

29% of corporates, Cybersecurity professionals' range between 5%-10% of their employee strength, while about 24% recruit these professionals in higher numbers. Among them, 12% are Cybersecurity service providers with Cybersecurity personnel making up over half their total workforce.

Figure 8: % of Cybersecurity Workforce



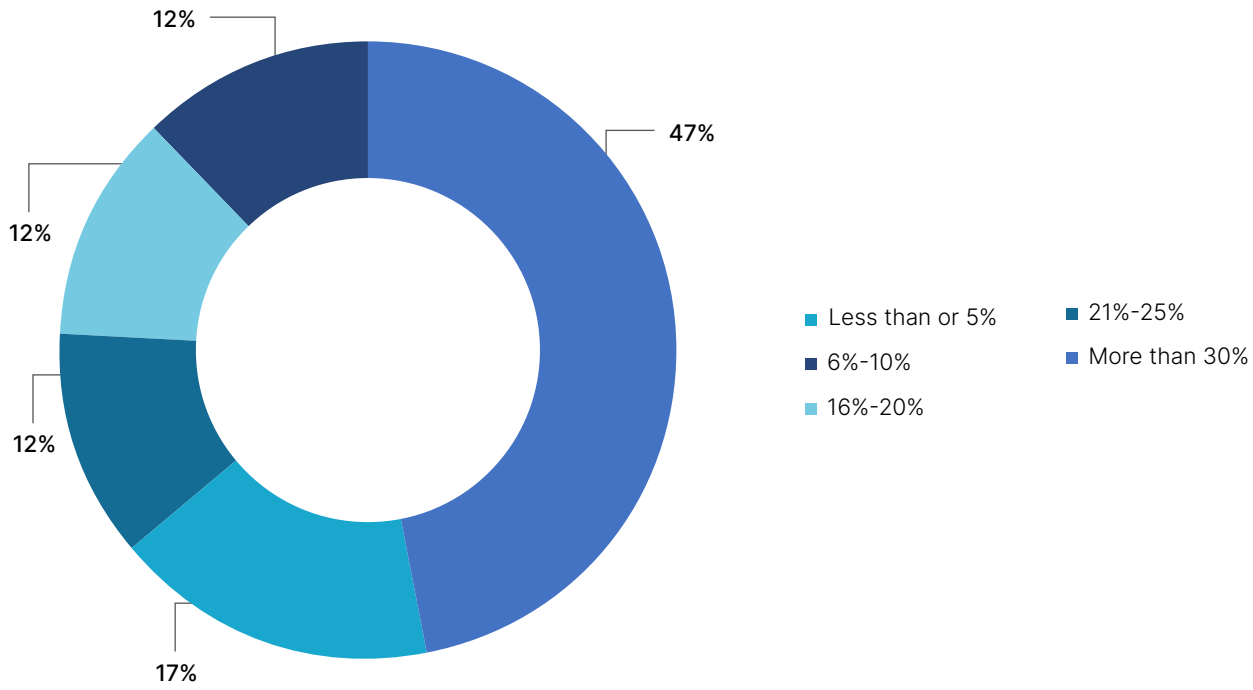
Goal of increasing the Cybersecurity workforce in next 5 years

By 2025, it is expected that the Cybersecurity sector will have an estimated 1.5 million job vacancies and 42% talent shortage, even before considering the projected 32% growth in Cybersecurity jobs over the next 6 years. To address the increasing number of Cybersecurity attacks and growing complexities of maintaining a secure digital environment, corporates need skilled Cybersecurity professionals. Corporates that participated in this study have shared goals for increasing their Cybersecurity workforce in next 5 years.

As seen in Figure. 9, the majority of participants (47%) advocated for a significant expansion of more than 30% on the current Cybersecurity workforce. A smaller group (24%) aimed for a 16%-25% growth. 29% respondents expressed a desire to achieve a conservative growth of less than or equal to 10% of the existing Cybersecurity workforce. These findings demonstrate varying perspectives on addressing the Cybersecurity skill gap.

47% of respondents mentioned that the goal is to increase the number of Cybersecurity professionals by more than 30% of the current workforce, indicating a significant increase in the demand for skilled professionals in Cybersecurity domain.

Figure 9: % increase in Cybersecurity Workforce in next 5 years



Cybersecurity Job Roles

The evolving environment of cyber threats has led to the emergence of various specialized job roles in Cybersecurity. From analysts and architects to incident responders and consultants, each role plays a crucial part in safeguarding organizations from cyber risks. By building a diverse and skilled Cybersecurity workforce, organizations can better protect their digital assets, maintain customer trust, and stay resilient in the face of changing cyber threats.

Interactions with Cybersecurity professionals show that presently, the most prevalent job roles available in the organizations for individuals with 0-5 years of experience, are Cybersecurity Risk Analyst, Cybersecurity Analyst, and Penetration tester.

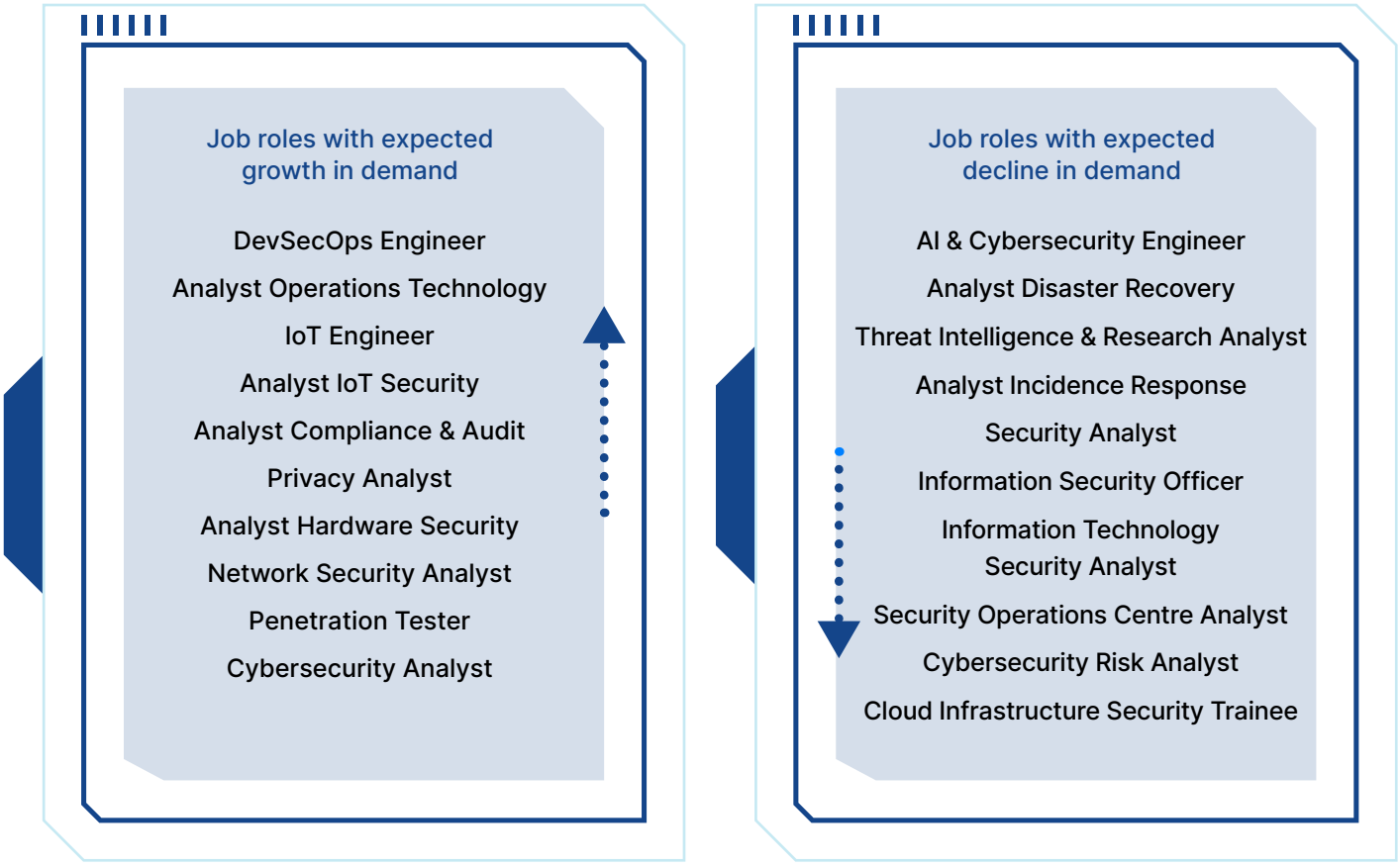
Other job roles that are in demand include Cloud Infrastructure Security Trainee, Security Operations Centre Analyst, Security Analyst, and Application Security Analyst (39% each), Cloud Engineer, Information technology Security Analyst, Network Security Analyst, and AI and Cybersecurity Researcher (33% each). These roles represent a diverse range of Cybersecurity functions, highlighting the multidimensional nature of the field.

To mitigate the growing demand Cybersecurity professionals identified job roles that are likely to increase within their organizations as shown in Figure 10.

Other job roles that will are expected to grow in next 5 years includes Analyst Compliance & Audit, Privacy Analyst, Analyst Hardware security, Network Security Analyst, Penetration tester and Cybersecurity Analyst.

Job roles that are expected surge in the next five years include DevSecOps Engineer, Analyst Operations Technology, IoT Engineer and Analyst IoT Security with a significant growth rate (100 %) or more)

Figure 10: Cybersecurity job roles with expected demand in the next 5 years



Chapter 3

Illuminating the path to inclusion: Identifying gaps in Diversity and Inclusion

This Chapter provides the overview about the Diversity and Inclusion (D&I) within the cybersecurity workforce. It assesses the present status of D&I within the cybersecurity workforce, exploring the representation and participation of women and PWDs. The chapter highlights the existing gaps and challenges leading to underrepresentation of Diverse and Inclusive workforce. It also discusses about the future goals set by organizations to improve D&I in the cybersecurity workforce.

Trends in Diversity & Inclusion (D&I) in Cybersecurity Workforce

Diverse teams in Cybersecurity can offer a range of different perspectives and experiences, enabling professionals to approach challenges from different angles. Diversity fosters creativity, innovation, and problem-solving skills, which are crucial in staying ahead of the curve. By incorporating diverse backgrounds, cultures, and viewpoints, organizations can tap into a broader pool of talent and expertise, enhancing their ability to effectively identify and address vulnerabilities in systems and networks. Diversity and inclusion may also contribute to the development of more robust and comprehensive Cybersecurity strategies. By including individuals with diverse backgrounds, organizations can better understand the unique risks faced by different user groups or communities and develop security measures and practices that cater to the needs of a broader range of stakeholders.

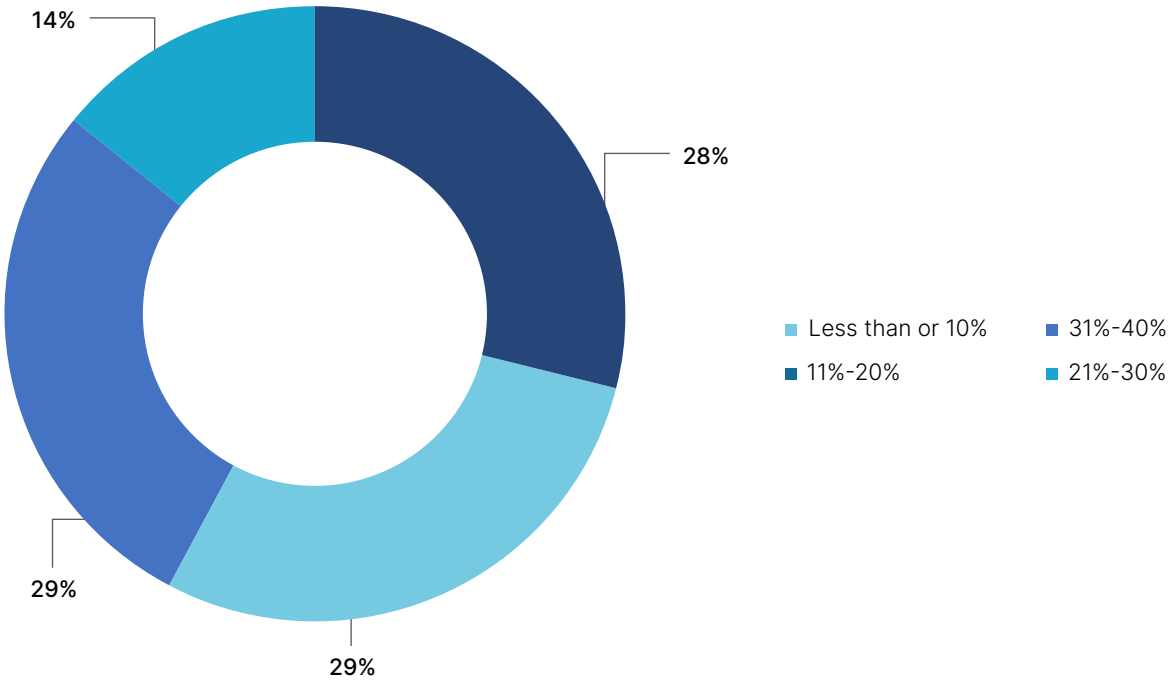
Women in Cybersecurity workforce

There is a growing recognition of the need to increase gender diversity in this field. Women have traditionally been underrepresented in technology-related professions, and cybersecurity is no exception. However, efforts are underway to bridge this gender gap and create a more inclusive and balanced workforce.

Increasing the participation of women in cybersecurity taps into a vast pool of untapped talent, skills, and perspectives. By fostering diversity, organizations can enhance their ability to think creatively and find innovative solutions to security challenges.

Further, promoting gender diversity in Cybersecurity is essential for creating a more inclusive and equitable industry. It offers women equal opportunities for career advancement, professional growth, and leadership roles. By breaking down barriers and biases, organizations can create a work environment that nurtures and supports women in Cybersecurity, encouraging them to thrive and make significant contributions. 82% of the corporates in this study mentioned that they have been onboarding women in Cybersecurity job roles. Figure 11 shows, 43% respondents have workforce ranging from 21%-30% to 31%-40%. 57% of the participants have a lower representation of women in Cybersecurity i.e., less than 20%.

Figure 11: % women in Cybersecurity workforce



Inclusion of Women in the Cybersecurity Workforce in the next 5 years

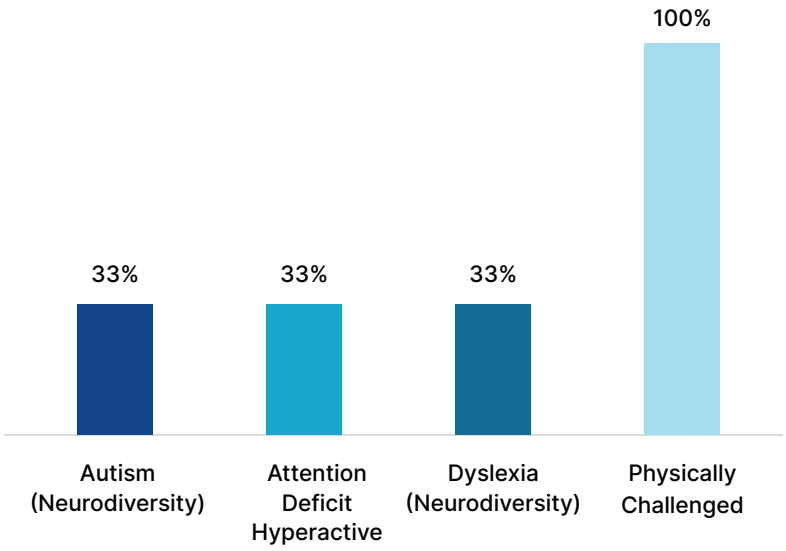
To bridge the D&I gap, corporates have defined goals to increase the participation of women in Cybersecurity in the next five years. 82% corporates have plans to increase the participation of women by at least 5% and out of these, 35% of respondents want to increase the participation by at least 15% in next 5 years.

Persons with Disabilities (PwDs) in Cybersecurity workforce

Currently, there is a lack of Cybersecurity representation and inclusion of persons with disabilities (PwDs) in the Cybersecurity workforce. Despite advancements in technology and a growing emphasis on diversity and inclusion, PWDs remain underrepresented in the field.

Cybersecurity roles require a range of skills beyond physical capabilities, such as critical thinking, problem-solving, and analytical skills, which can be carried out by PWDs efficiently

Figure 12: % PwDs in Cybersecurity workforce



The study findings show that only 12% of the corporates onboarded PwDs into the Cybersecurity workforce. All of these corporates hired professionals who are physically challenged while 33% each recruited PwDs diagnosed with Autism, Attention Deficit Hyperactive Disorder (ADHD) and Dyslexia. The overall representation of PwDs in the participating organizations is between 1%-2%.

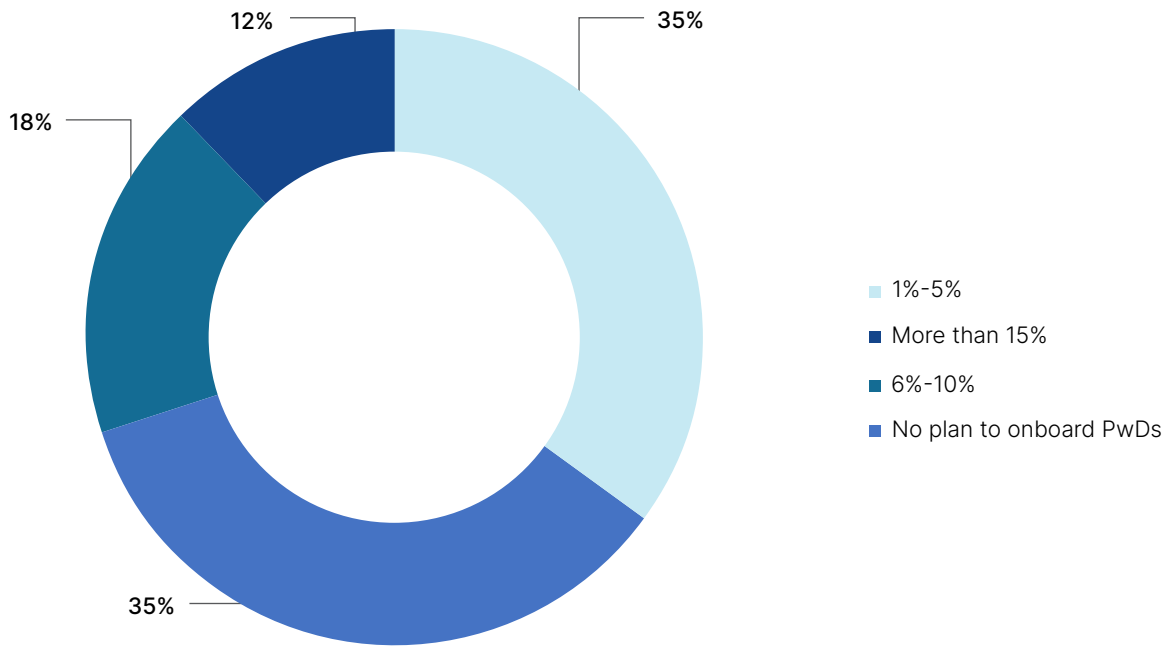
Goal for Increasing PwDs in Cybersecurity workforce

To empower PwDs to pursue and excel in Cybersecurity careers, it is important for the industry to address this disparity by implementing inclusive hiring practices and build, create a more resilient Cybersecurity workforce that leverages the strengths and contributions of diverse individuals with diverse strengths and abilities.

However, as per the study, a considerable portion (of the respondents, (35%) indicated that they do not have any plans to onboard PwDs in next 5 years as shown in Figure 13.

While 35% of the respondents have goals ranging from 1%-5% PwDs in their workforce, 18% have set a goal of having them comprise 6%-10% of the workforce. Only, 12% respondents have plans to onboard PWDs to make up more than 15% of their workforce. It is important to note that the companies' goals and plans regarding PwD inclusion may vary based on individual responses and organizational strategies.

Figure 13: % increase in participation of PwDs in Cybersecurity workforce



Gaps identified in Diversity & Inclusion (D&I) in Cybersecurity Skilling Programs

The low representation of women and PwD in the sector extends to skilling programs as well, which reflects the broader diversity gaps within the industry. Cybersecurity Cybersecurity Addressing this challenge requires proactive measures to promote gender equality and inclusion for PwDs in the Cybersecurity ecosystem.

Encouraging and supporting women and PwDs to pursue training opportunities, providing scholarships or financial assistance, and creating mentorship programs are some of the steps that can be taken to bridge the diversity and inclusion gap. Additionally, raising awareness about the exciting and rewarding aspects of Cybersecurity careers and debunking myths can help attract more women and PWDs to training programs.

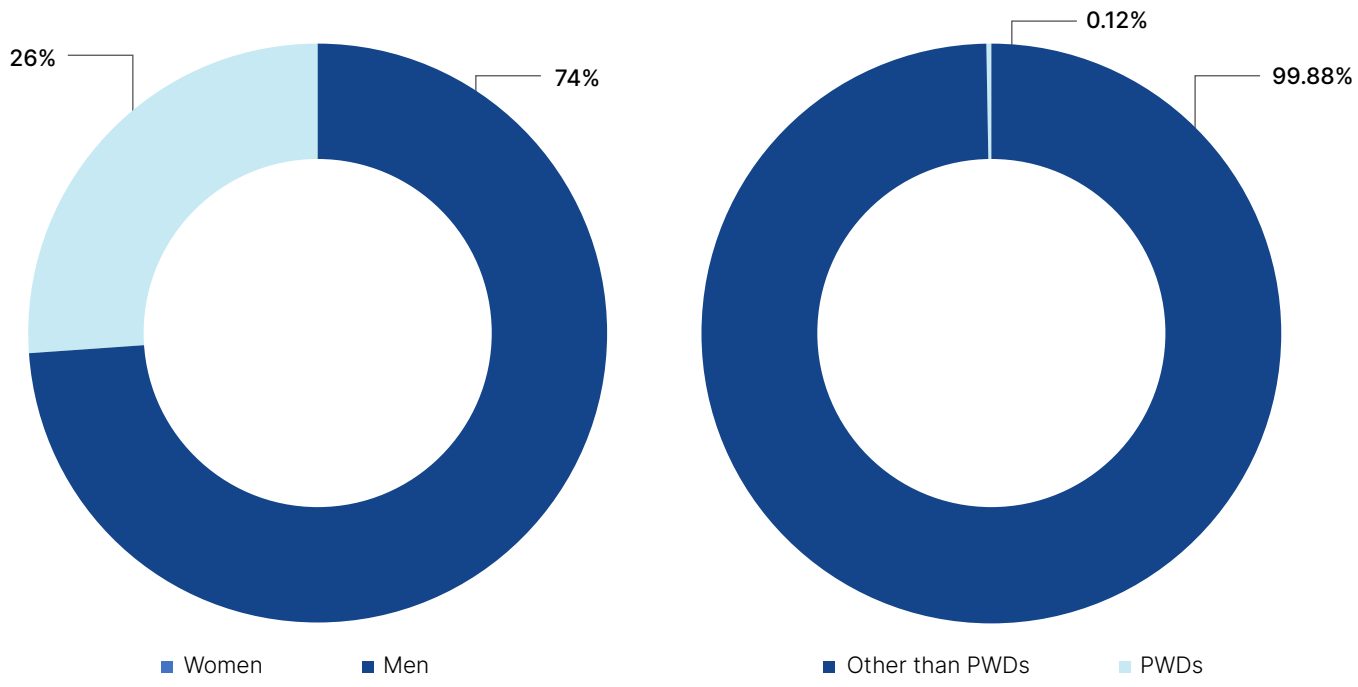
PARTICIPATION OF WOMEN

Only 26% women completed Cybersecurity skilling program organized by training providers/ NGOs

PARTICIPATION OF PWDS

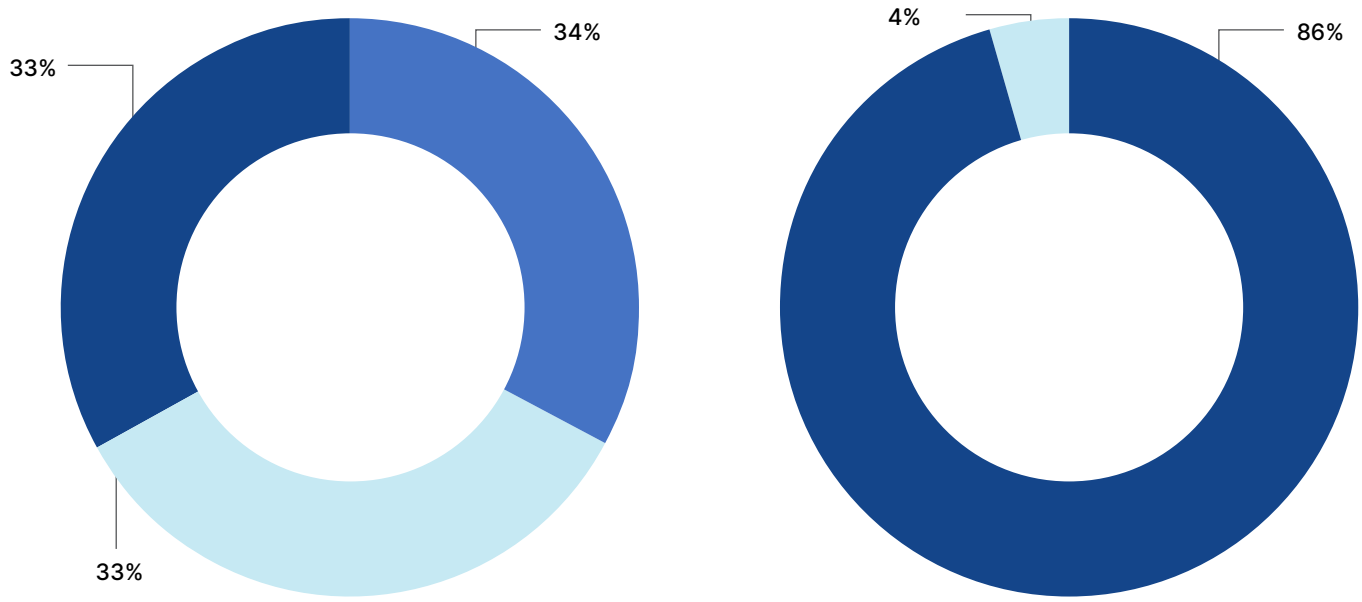
Only 0.12% Persons with Disabilities (PwDs) completed the Cybersecurity skilling program

Figure 14: Participation of women and PwDs in Cybersecurity skilling program of training providers/NGOs



As reported by training providers/NGOs, representation of women in Cybersecurity skilling programs is 26%. Moreover, participation of PwDs in skilling program is quite low i.e., 0.12%

Figure 15: Participation of women and PwDs in Cybersecurity skilling program of academic institutions



67% academic institutions included in the study mentioned that less than 25% women participate in Cyber Security programs in their institutes Among these institutions, about half have 5%-10% women. Additionally, the participation of PwDs in the academic institutes is just 4%.

Chapter 4

Anticipating Future Skill Demand and Identification of Gaps in the Cybersecurity Ecosystem

This chapter provides an overview of the relevant skills and competencies sought by corporates in Cybersecurity professionals and highlights skill gaps they have identified. It also summarizes the preferred academic qualifications for hiring freshers in Cybersecurity. The chapter also explores the surge in demand for Cybersecurity certifications and discusses the low awareness about the domain among students. The chapter also provide valuable insights about the relevant soft skills in the Cybersecurity landscape.

Growing demand for technical skills and Competencies

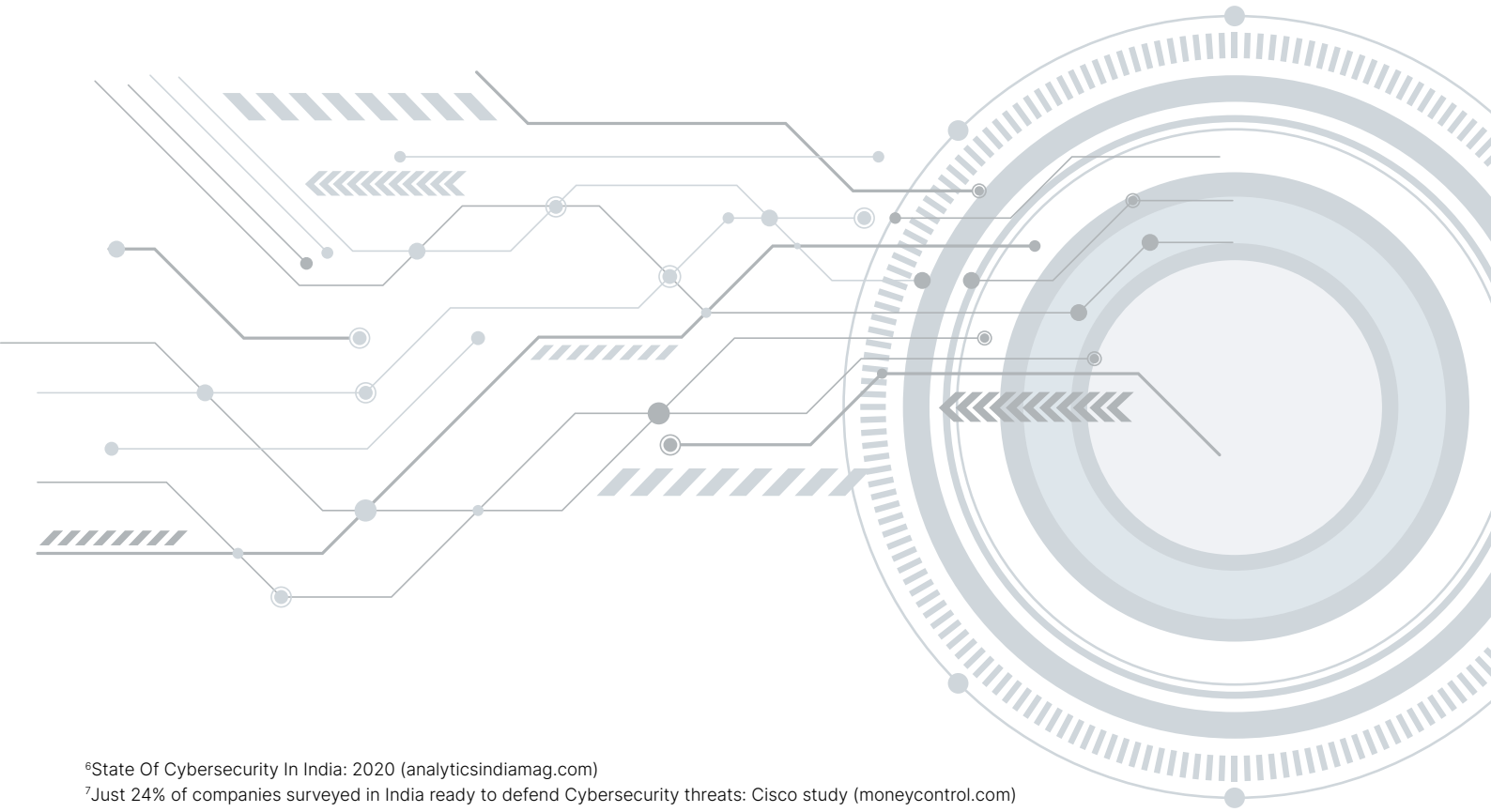
Cybersecurity professionals employed in India constitute 3% of the global Cybersecurity jobs. In addition, there is a dearth of specialized professionals in the country, with 19% holding post graduate degrees and 1% with doctorate or equivalent degrees.[6] The shortage in India is estimated to be 9% higher than the global average.

The paucity of a skilled Cybersecurity workforce has a major impact on the security of data housed by governments, corporates, and other organizations. A multi-market study with 6,700 respondents conducted by Cisco shows that only 24% of companies surveyed in India are prepared to fend off Cybersecurity threats while 38% are in the early stages of readiness. The impact of not being well prepared is also financially significant; 80% of the study participants reported a Cybersecurity incident within the previous year and 53% said each event cost them USD 500,000 at a minimum.[7]

According to a report titled, ISACA State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources, and Cyber efforts, the largest skill gaps among trained Cybersecurity professionals lie in: soft skills (54%), cloud computing (52%), and security controls (34%).

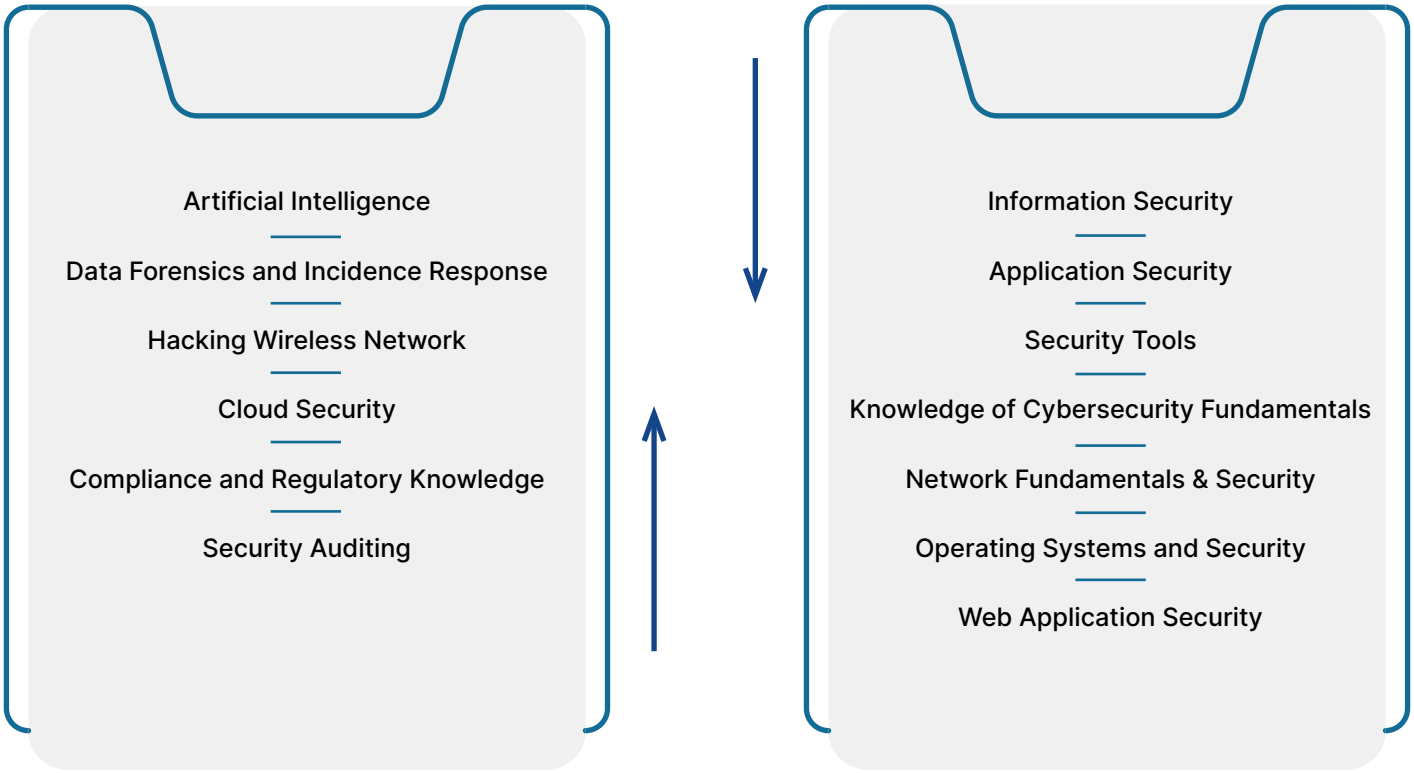
Professionals who participated in the study were asked about the most relevant technical skills and competencies that are required at present for Cybersecurity job roles for professionals with 0-5 years of experience. The findings in Figure 16, reveal that knowledge of Cybersecurity Fundamentals (78%), Networking Fundamentals and Security (67%), Information Security (61%), Application Security (61%), Web application Security (61%), Security Tools (61%) and Cloud Security (56%) are in high demand among organizations.

However, when seen from a lens of future demand, the most highly recognised skills when compared with their demand currently were Artificial Intelligence (56% as compared to 0% present), Data Forensics (44% as compared to 17% at present) and Hacking Wireless Networks (28% as compared to 0% at present).



[6]State Of Cybersecurity In India: 2020 (analyticsindiamag.com)
[7]Just 24% of companies surveyed in India ready to defend Cybersecurity threats: Cisco study (moneycontrol.com)

Figure 16: Demand for Technical Skills & Competencies



Looking ahead, technical skills and competencies that are expected to experience significant growth and will be highly recognized in the next five years include Artificial Intelligence, Data Forensics and Incidence Response, Hacking Wireless Network, Cloud Security, Compliance and Regulatory Knowledge, and Security Auditing

Gaps identified in technical skills and competencies by industries

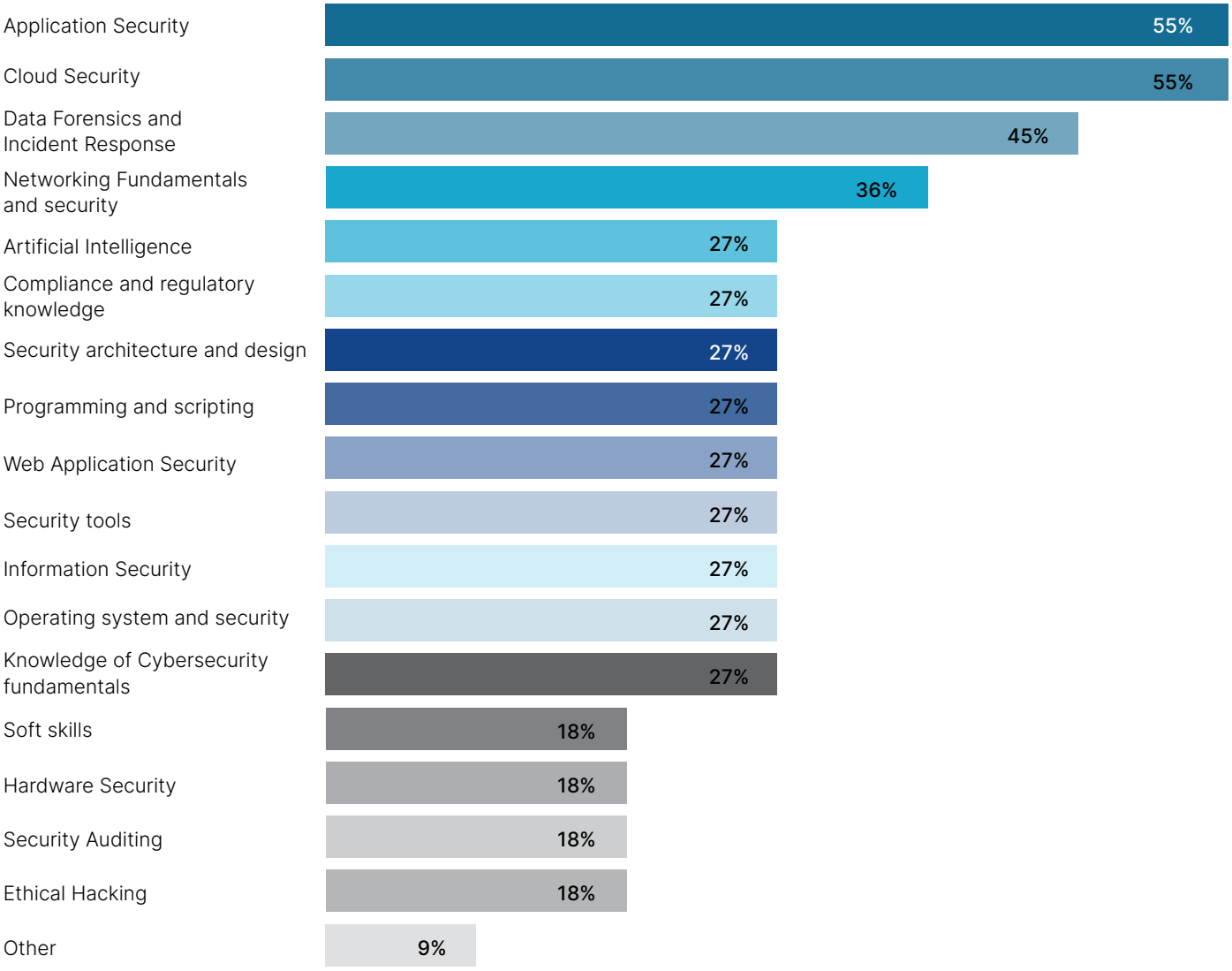
The gap between training content and industry demand can hinder the ability of Cybersecurity professionals to effectively navigate the complex Cybersecurity landscape. It is important to assess these gaps and bridge them through content validation, targeted training programs, curriculum enhancements, and industry collaboration.

61% companies have identified gaps in current skills and competencies level of Cybersecurity professionals with 0-3 years of experience.

The top four skills where the gaps have been identified include, cloud security, application security, data forensics and incident response and networking fundamentals and security.

Other skills where gaps have been identified as shown in Figure 17, include security architecture and design, programming and scripting, Information security, compliance and regulatory knowledge, security tools, operating system and security, knowledge of Cybersecurity fundamentals, web application security and artificial intelligence. These skills are critical for managing organizations' Cybersecurity infrastructure and operations.

Figure 17: Skill Gaps observed by corporates



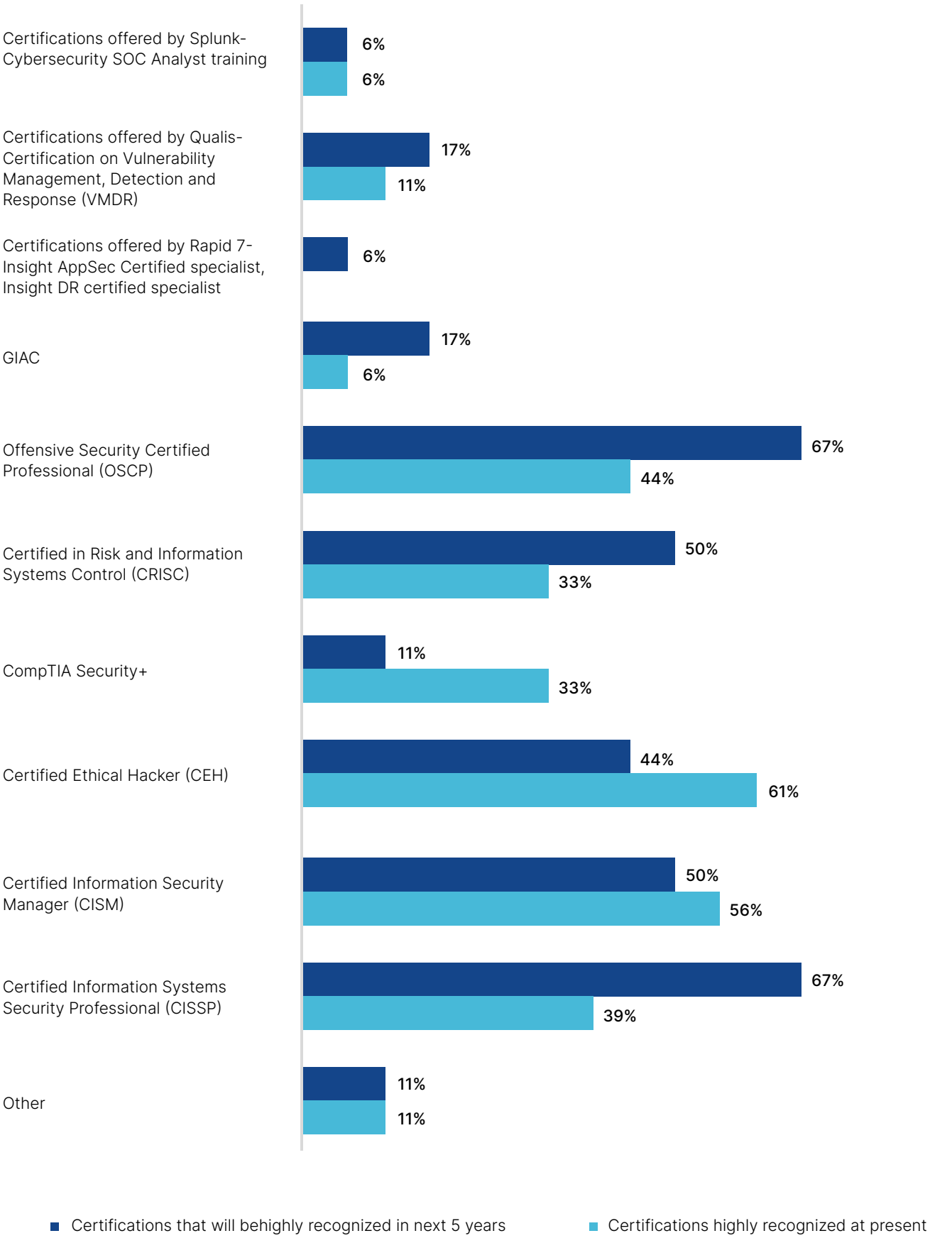
Surging demand for Cybersecurity certifications

The demand for Cybersecurity certifications reflects the growing importance of a skilled and certified workforce in combating evolving cyber threats. Organizations across various industries are recognizing the need to strengthen their security postures and protect sensitive data from sophisticated cyber-attacks. As a result, employers are placing greater emphasis on hiring professionals with recognized certifications that demonstrate their knowledge and expertise in the field of Cybersecurity.

Figure 18 shows, The most in-demand certification at present for professionals with 0-5 years of experience is Certified Ethical Hacker, with 61% of respondents mentioning it as a requirement. Next in importance are the Certified Information Security Manager (CISM) and Offensive Security Certified Professional (OSCP) certifications mentioned by 56% and 44% of the respondents respectively. Certified Information Systems Security Professional (CISSP), CompTIA Security+ and Certified in Risk and Information Systems Control (CRISC) certifications follow thereafter. Only 11% of respondents require the Certification on Vulnerability Management, Detection and Response (VMDR) offered by Qualis, and 6% require GIAC and Cybersecurity SOC Analyst training offered by Splunk.

In the next 5 years, Cybersecurity certifications which will be given high prominence as mentioned by professionals include, Offensive Security Certified Professional (OSCP) (67%), Certified Information Systems Security Professional (CISSP) (67%), Certified in Risk and Information Systems Control (CRISC) (50%), GIAC (17%), Certifications offered by Qualis- Certification on Vulnerability Management, Detection and Response (VMDR) (17%), Certifications offered by Rapid 7- Insight AppSec Certified specialist, Insight DR certified specialist (6%).

Figure 18: Demand for Cybersecurity certifications

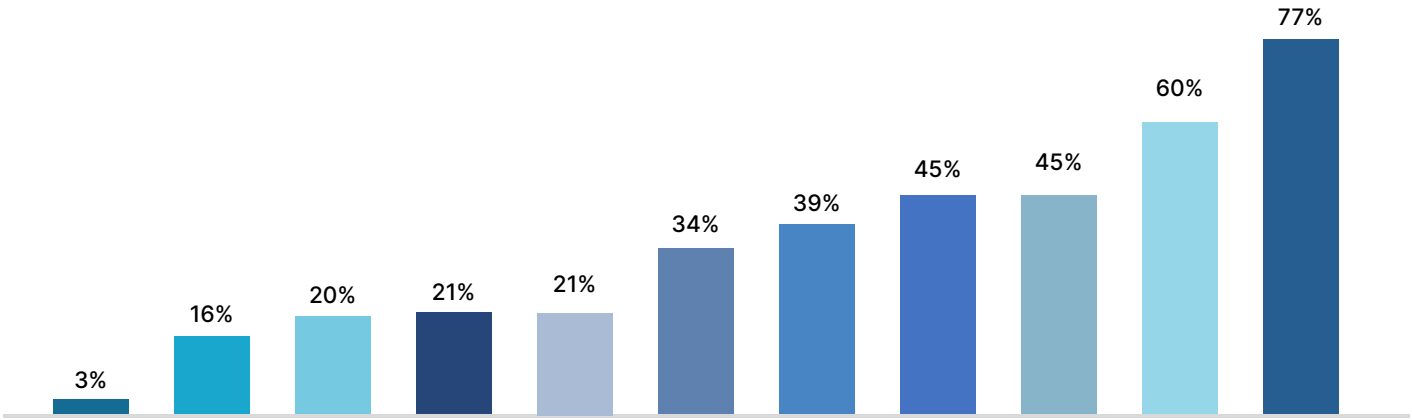


Gap in students' awareness of Cybersecurity

Despite the increasing demand for professionals in this field, many students are unaware of the career opportunities available in Cybersecurity and the critical role it plays in safeguarding organizations' digital assets. This lack of awareness can be attributed to several factors, which the study sought to capture.

Cybersecurity training providers who were the part of the study have rated the awareness level as 2.13 out 5 (1 being the lowest and 5 being the highest). Additionally, it has been observed that 70% students were aware about different Cybersecurity certifications, out of which not even 50% of students were aware about certifications such as Vulnerability Management Detection and Response (VMDR), Insight AppSec Certified specialist, Insight DR certified specialist, GIAC, Offensive Security Certified Professional, Risk and Information Systems Control, CompTIA Security+, Certified Information Security Management as shown in Figure 19.

Figure 19: Awareness of students on Cybersecurity certifications



- Cybersecurity SOC Analyst training (Offered by Splunk)
- Certification on Vulnerability Management, Detection and Response (VMDR) (Offered by Qualis)
- Insight AppSec Certified specialist, Insight DR certified (Offered by Rapid 7)
- Certification- GIAC
- Certification- Offensive Security Certified Professional (OSCP)
- Certification- Certified in Risk and Information System Control (CRISC)
- Certification- CompTIA Security+
- Certification- Certified Ethical Hacker (CEH)
- Certification- Certified Information Security Manager (CISM)
- Certification- Certified Information Systems Security Professional (CISSP)
- Others

Academic Qualifications

Another key factor that influences a company's decision to hire a professional is their academic qualification and its alignment with the work they may be tasked with.

Figure 20: Education qualification in order of respondent's preference in hiring freshers

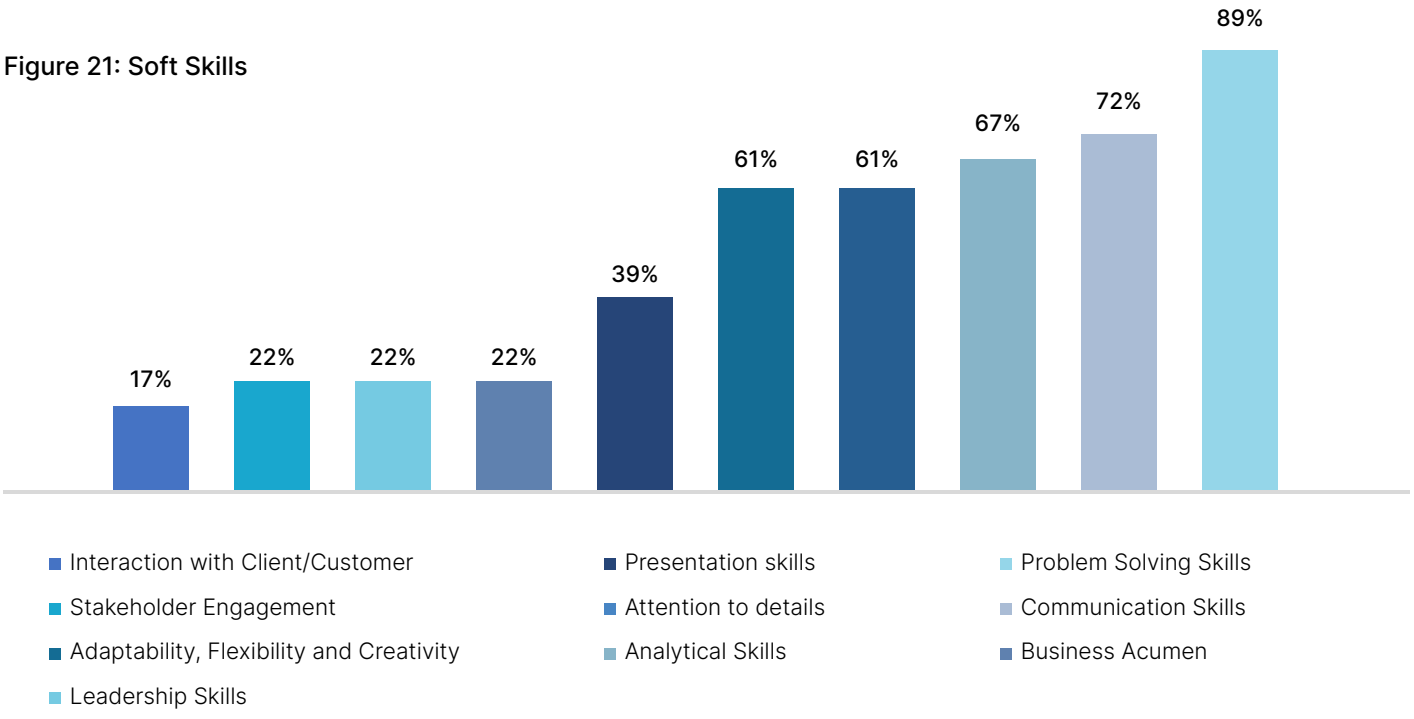
As shown in Figure 20, corporates first preference in onboarding Cybersecurity professionals is computer science graduates/ post-graduates with specialization in Cybersecurity, second preference given to graduates/ post-graduates with project/internship in Cybersecurity, followed by Graduates/ Post-Graduates with courses in Cybersecurity and last preference is given to Computer Science Graduates/ Post-graduates

Soft skills

While technical proficiency is crucial for addressing cyber threats, the ability to effectively communicate, collaborate, and think critically is equally vital as these professionals often find themselves working in cross-functional teams, engaging with stakeholders, and communicating complex technical concepts to non-technical audiences. The demand for professionals who can combine technical prowess with strong soft skills is growing, as organizations recognize the need for holistic Cybersecurity strategies that encompass both technical solutions and effective communication with stakeholders.

Figure 21 shows that the most relevant soft skills that are required for Cybersecurity job roles in the organizations (who participated in the study) are Problem Solving Skills (89%), Communication Skills (72%), Analytical Skills (67%), Adaptability, Flexibility and Creativity (61%) and Attention to details (61%). Other soft skills required are Presentation Skills (39%), Business Acumen (22%), Leadership Skills (22%) and Stakeholder Engagement (22%) and Interaction with Client/Customer (17%).

Figure 21: Soft Skills



Chapter 5

Current landscape: Training and Placements

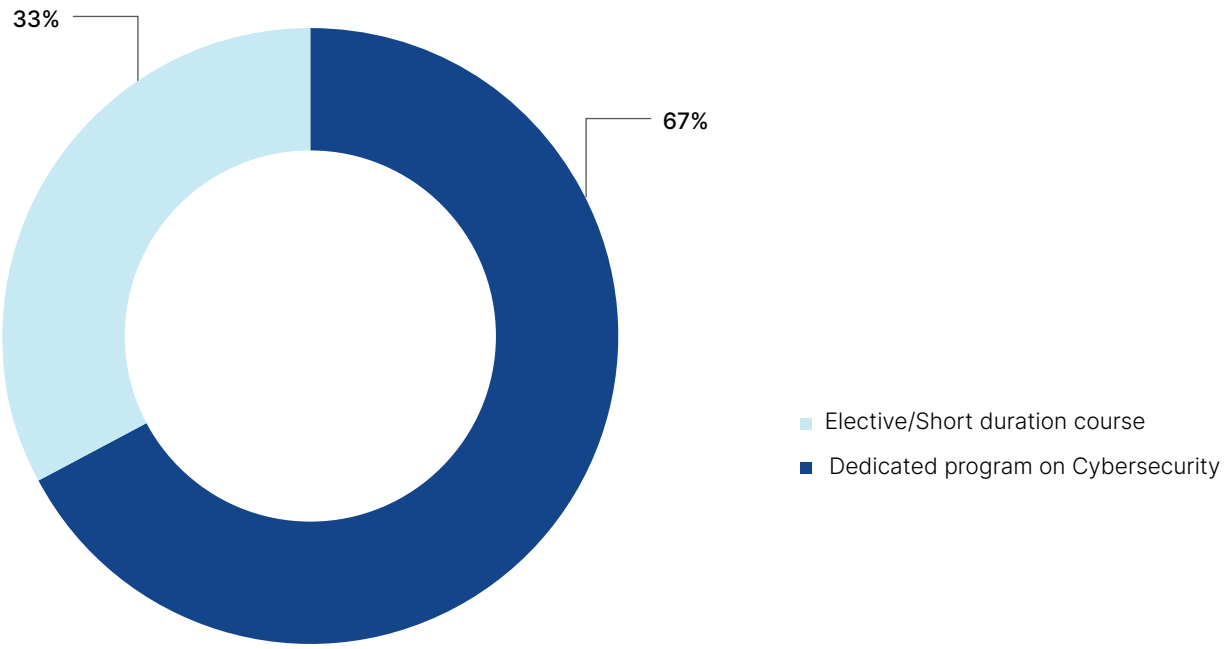
This chapter explores the current landscape of training and placement of Cybersecurity skilling program. It delves into the difficulties and gaps identified with respect to program design, content validation and skills learned by the students. It also explores the domain of training and capacity building of trainers. The chapter also sheds light on the placement landscape of the Cybersecurity skilling program.

Cybersecurity Program Design and Structure

Cybersecurity is a vast and rapidly evolving field that requires a comprehensive understanding of various concepts, technologies, and methodologies. While a long-term training program offers students a solid foundation and in-depth knowledge of fundamental principles, network security, cryptography, ethical hacking, incident response, and other essential areas, short-term training modules that focus on specific skills, emerging threats, and industry trends can address rapidly evolving topics to help students stay up-to-date with the latest advancements and gain practical experience in handling contemporary Cybersecurity challenges.

When asked about the kind of training program they would seek, 67% of students opted for dedicated skilling programs on Cybersecurity, while 33% opted for an elective/ short duration program.

Figure 22: Program Design

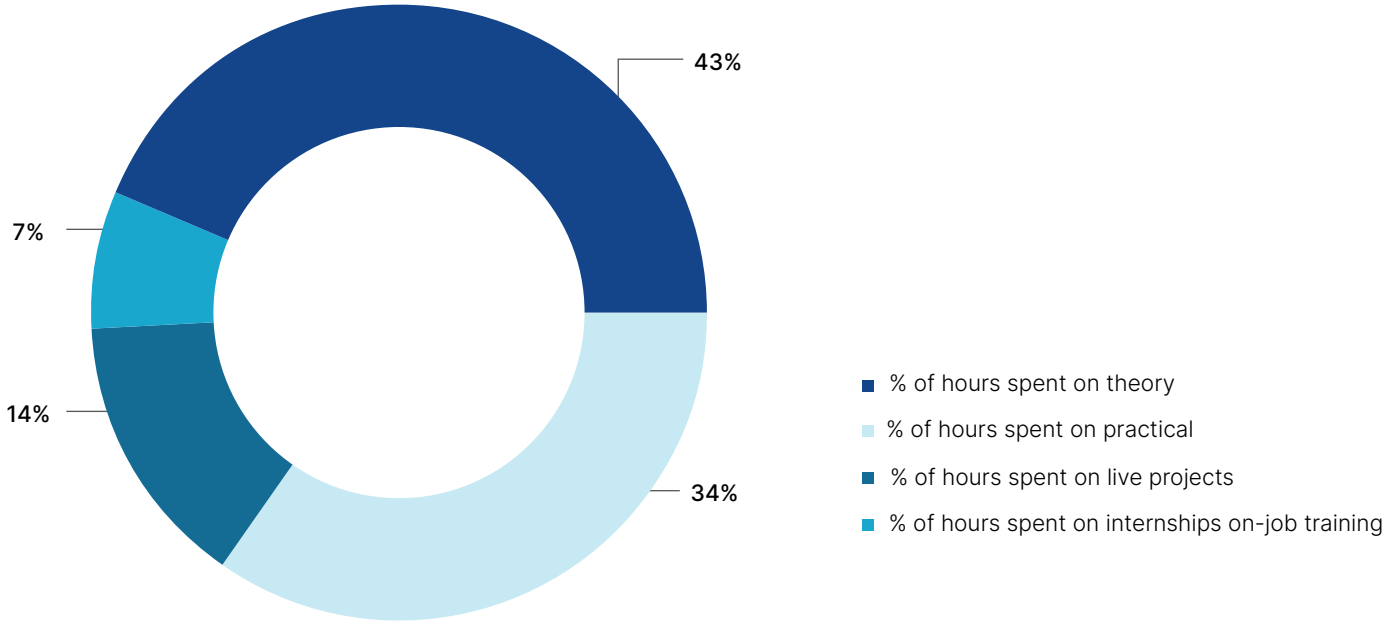


Dedicated program on Cybersecurity

During discussions with students who have been placed in jobs and have more than 6 months of work experience, it was noted that they face difficulties while transitioning to the role of Cybersecurity professional. This stems from challenges in practical application of Cybersecurity concepts.

67% of the students who opted for dedicated programs on Cybersecurity mentioned that on average, training providers spend 43% of the total hours on teaching theoretical concepts and 34% hours on practical application of those concepts as shown in Figure 23. As a result, students do not get adequate hands-on-experience in the practically applying the concepts they have been taught about. This in turn leads to a gap between the students' knowledge and understanding and expectations of corporates.

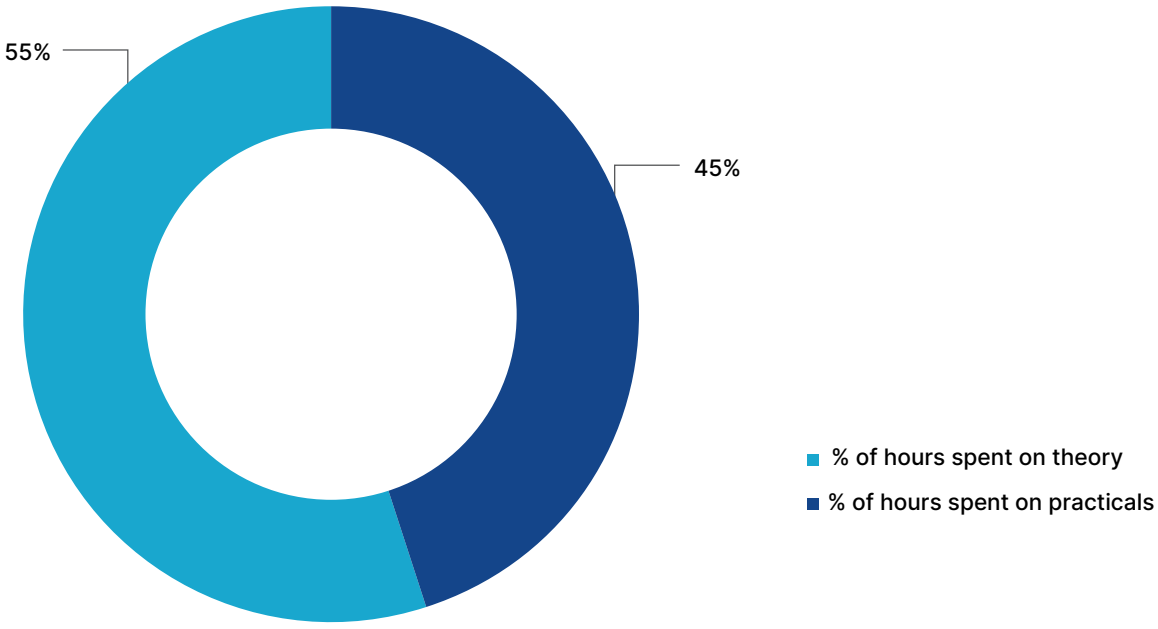
Figure 23: Dedicated program on Cybersecurity



Elective/Short Duration program on Cybersecurity

Figure 24 shows, among those students who have opted for an elective/ short duration program, mentioned that on average 55% of total hours of the program are spent on learning theoretical aspects of the program, and 45% of total hours are spent are hands-on-experience or practical application.

Figure 24: Elective/Short duration program on Cybersecurity



Content Validation

Content validation is critical for driving skilling initiatives in Cybersecurity. It ensures that content designed is in alignment with industry standards and expectations of the Cybersecurity ecosystem. Validated content also provides credibility to the skilling program,

Content development and curation are essential components of Cybersecurity training programs. Effective training content can aid in providing students with the skills and knowledge required to counter Cybersecurity risks. Curation also makes sure that the training content is relevant and engaging thereby improving the program's effectiveness over time.

The lack of content validation in cybersecurity training programs contributes to a significant disparity between the technical skills and competencies required by corporates and what students learn through the skilling program.

100% academic institutions and 56% training providers/ NGOS driving Cybersecurity skilling programs have not got the content validated, whereas 44% of the training providers have got the content validated by organizations such as Data Security Council of India, CISCO, and technical experts from academic institutes.

Comparative analysis- Technical Skills and Competencies: Corporates and Students

As the field of cybersecurity continues to evolve at a rapid pace, it is also crucial to identify and address the skills gaps that exist between the current training content available and the future skills demand from the industry. With emerging technologies, growing threats, and changing regulations, cybersecurity professionals need to be well prepared to effectively defend organizations from cyber risks.

The illustration below shows the technical skills and competencies that are learned by students in training programs at present as well as the technical skills and competencies which companies expect will gain importance. The ranking is on the basis of % of respondents choosing the options.

Figure 25: Gaps identified in Technical Skills & Competencies

Ranking	Technical skills and competencies that will be given high prominence in next 5 years	Technical Skills and Competencies learned by Students
1	Artificial Intelligence	Knowledge of Cybersecurity fundamentals
2	Data Forensics and Incident Response	Networking Fundamentals and Security
3	Hacking Wireless Network	Information Security
4	Cloud Security	Operating system and security
5	Compliance and Regulatory Knowledge	Security tools
6	Security Auditing	Ethical Hacking
7	Hardware Security	Social Engineering
8	Security architecture and design	Application Security
9	Programming and scripting	Web Application Security
10	Ethical Hacking	Hacking Wireless Network
11	Social Engineering	Data Forensics and Incident Response
12	Web Application Security	Security Auditing
13	Operating System and Security	Cloud Security
14	Networking Fundamentals and Security	Security architecture and design
15	Knowledge of Cybersecurity Fundamentals	Programming and scripting
16	Application Security	Hardware Security
17	Security Tools	Compliance and regulatory knowledge
18	Information Security	Artificial Intelligence

*Ranking developed based on the % of respondents who stated the option

The comparison highlights differences in the skills sought by companies and the topics learned by students as part of the Cybersecurity skilling program. As shown in Figure 25, Companies have given high priority to Artificial Intelligence, Data Forensics and Incidence Response, Hacking Wireless Network, Cloud Security, Compliance and Regulatory Knowledge and Security Auditing as mentioned by Cybersecurity professionals. However, these skill ranks lower in the topics learned by students, indicating a potential gap that might arise when they start working as a Cybersecurity professional.

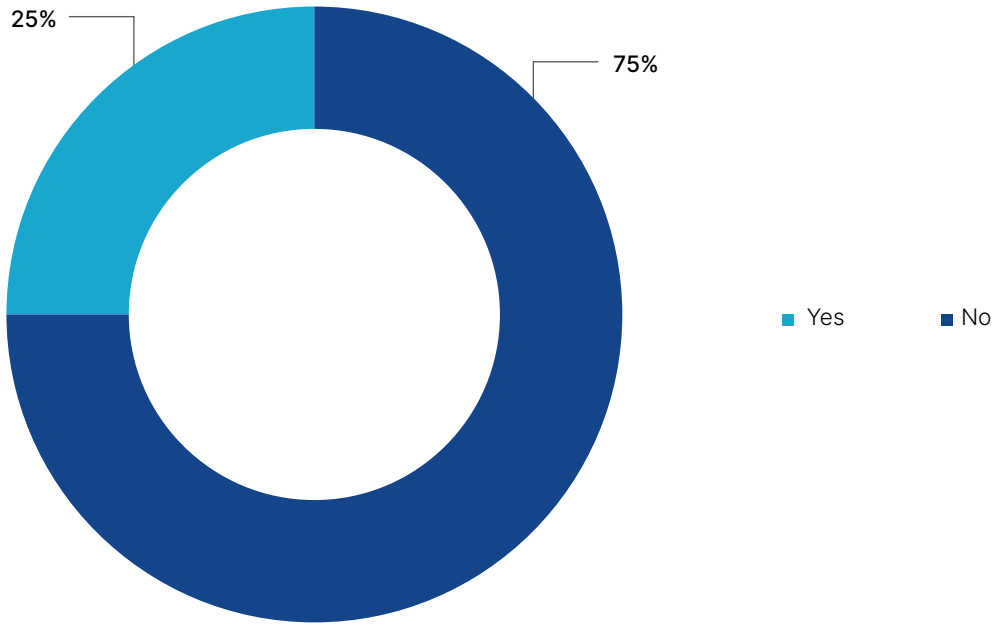
This disparity underscores the need for students to be regularly trained and upskilled in the latest Cybersecurity trends and requirements to ensure that they have adequate skills to address demands of different industries.

Certification status of students

Certifications play a crucial role in substantiating an individual's expertise and knowledge in specific Cybersecurity areas, providing employers with a guarantee of their competence and skills.

Out of the students who participated in the study, the majority of respondents admitted to not having pursued any professional certifications in the field of Cybersecurity. The lack of certifications among students highlights a potential gap between the skills and qualifications expected by employers in the Cybersecurity industry and the readiness of the student workforce.

Figure 26: Certification status of students in Cybersecurity



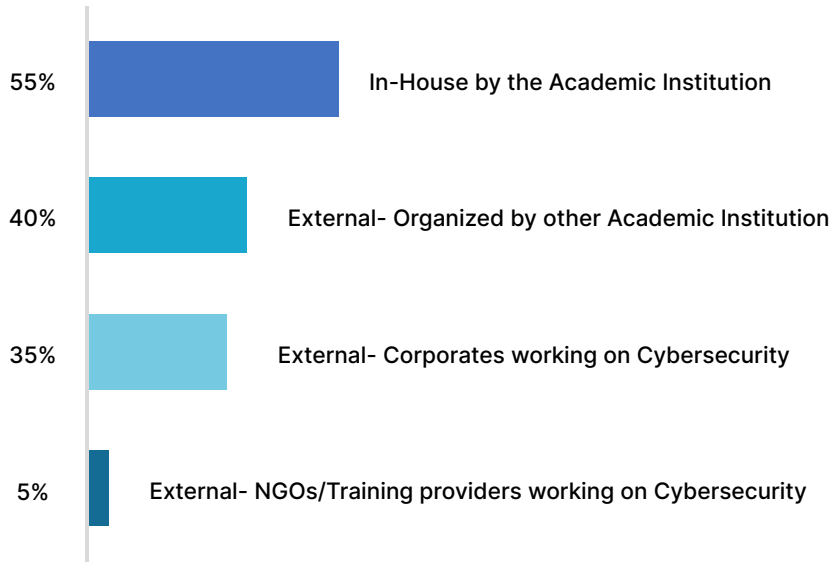
Training and capacity building of trainers

While the demand for well-trained professionals in the domain is undeniable, there is a crucial but often overlooked aspect that deserves attention: the training needs of trainers and faculties themselves. While much has been said about the technical skills and knowledge required in the Cybersecurity domain, The needs of those who play a pivotal role in shaping the future cyber defenders remain equally significant. An examination of these needs of trainers and faculties can tap into the hidden layers of expertise, adaptability, and pedagogical prowess required to effectively train the next generation of Cybersecurity professionals.

The study sought to highlight some of these needs and the responses provide key insights into the gaps in catering to these needs. The study shows that 54% trainers mentioned that they have attended the refresher training on Cybersecurity, while the remaining respondents did not undergo any refresher training.

As shown in Figure 27, 55% of the respondents mentioned that the training was organized in-house by the academic institution, while 40% of the respondents stated that their refresher training was organized externally in collaboration with other academic institutions. 35% of the respondents, reported taking refresher training that was organized in collaboration with corporates working in the Cybersecurity industry. Additionally, 5% of the respondents stated that the training was organized in collaboration with NGOs or training providers working in the Cybersecurity domain.

Figure 27: Stakeholder involved in training faculties

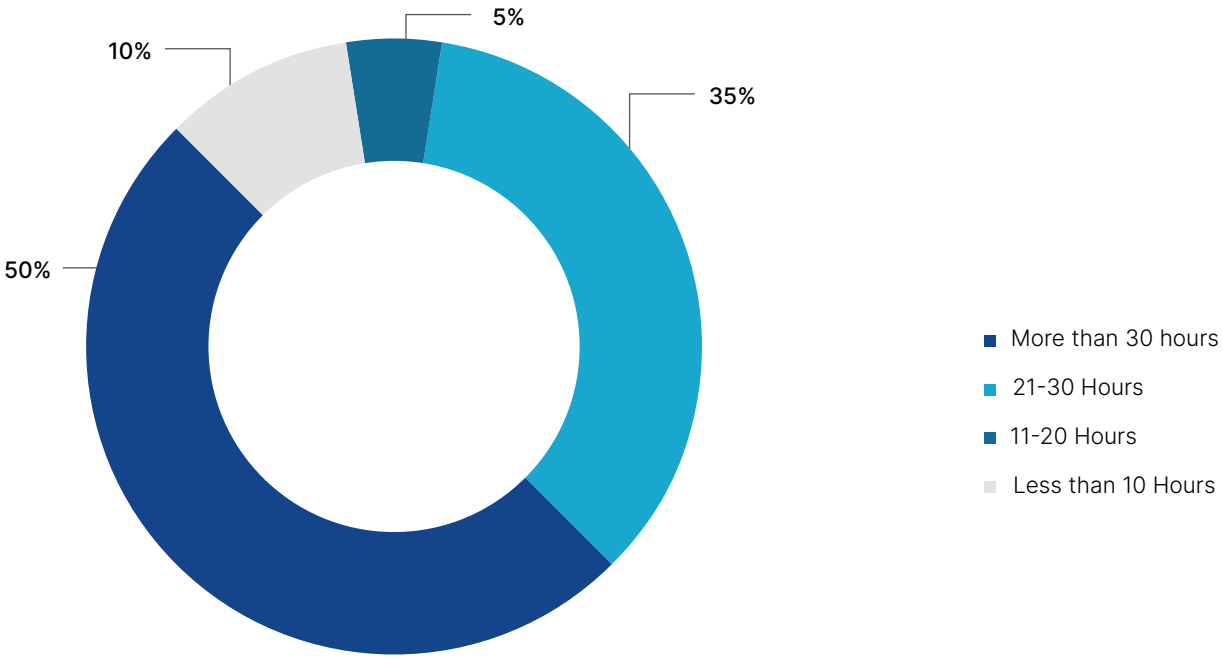


Duration of training

The duration of refresher trainings is a key aspect as it determines the extent to which trainers can enhance their expertise and remain updated with rapid changes in the Cybersecurity domain. Short, sporadic trainings may not provide sufficient time for trainers to delve deep into emerging topics or acquire comprehensive insights into evolving cyber threats. On the other hand, well-designed and adequately timed refresher trainings offer trainers the opportunity to explore advanced concepts, engage in hands-on exercises, and collaborate with industry experts to broaden their understanding.

Figure 28 shows that 10% of the respondents invested less than 10 hours in refresher training on Cybersecurity, 5% of the respondents invested around 11 to 20 hours in their training, whereas 35% of the respondents invested around 21 to 30 hours in their refresher training. The remaining 50% of the respondents invested more than 30 hours.

Figure 28: Duration of the training

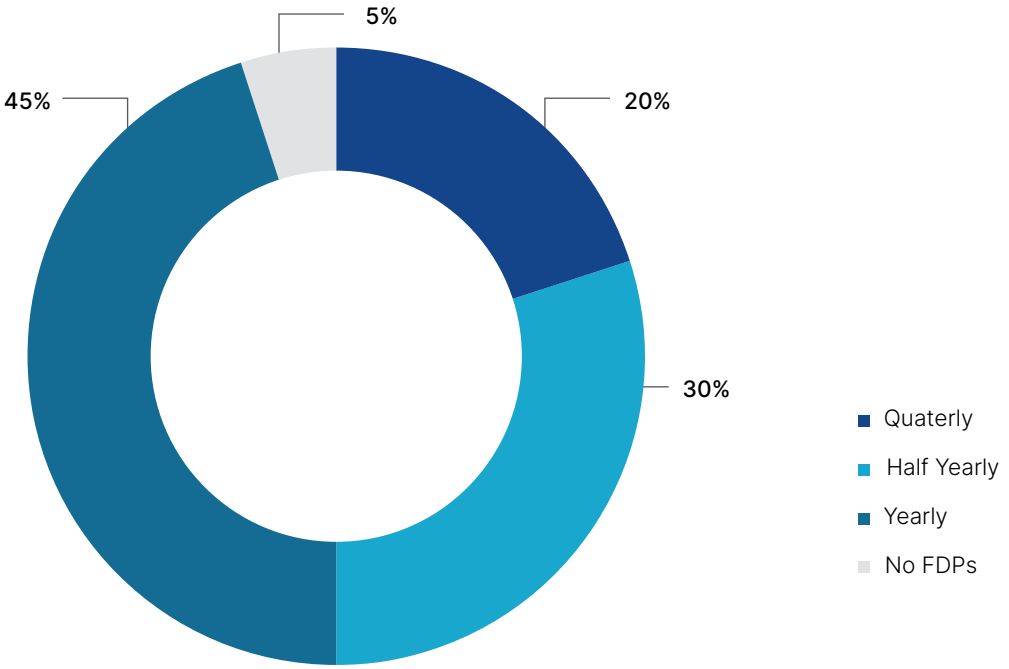


Frequency of Refresher Training for Faculties/Trainers

As new threats and vulnerabilities emerge at a very fast rate, the frequency of refresher trainings becomes a critical consideration for trainers and faculties. To keep pace with these changes, trainers and faculties must engage in refresher trainings that are frequent enough to ensure they remain knowledgeable and adaptable. By adopting an agile approach with a more frequent training schedule, trainers and faculties can continuously update their knowledge, stay informed about emerging trends, and enhance their skills to effectively address the evolving Cybersecurity challenges.

Trainers /faculties stated that 45% of the training providers conduct refresher training program for faculties on a yearly basis, 30% on a half-yearly basis, while only 20% undergo a quarterly refresher training. As the domain of Cybersecurity is constantly evolving, the requirement for more frequent training of trainers is the arising to ensure they possess the necessary industry skills and knowledge and same is delivered to students covered under the skilling program.

Figure 29: Frequency of Refresher Training for Faculties

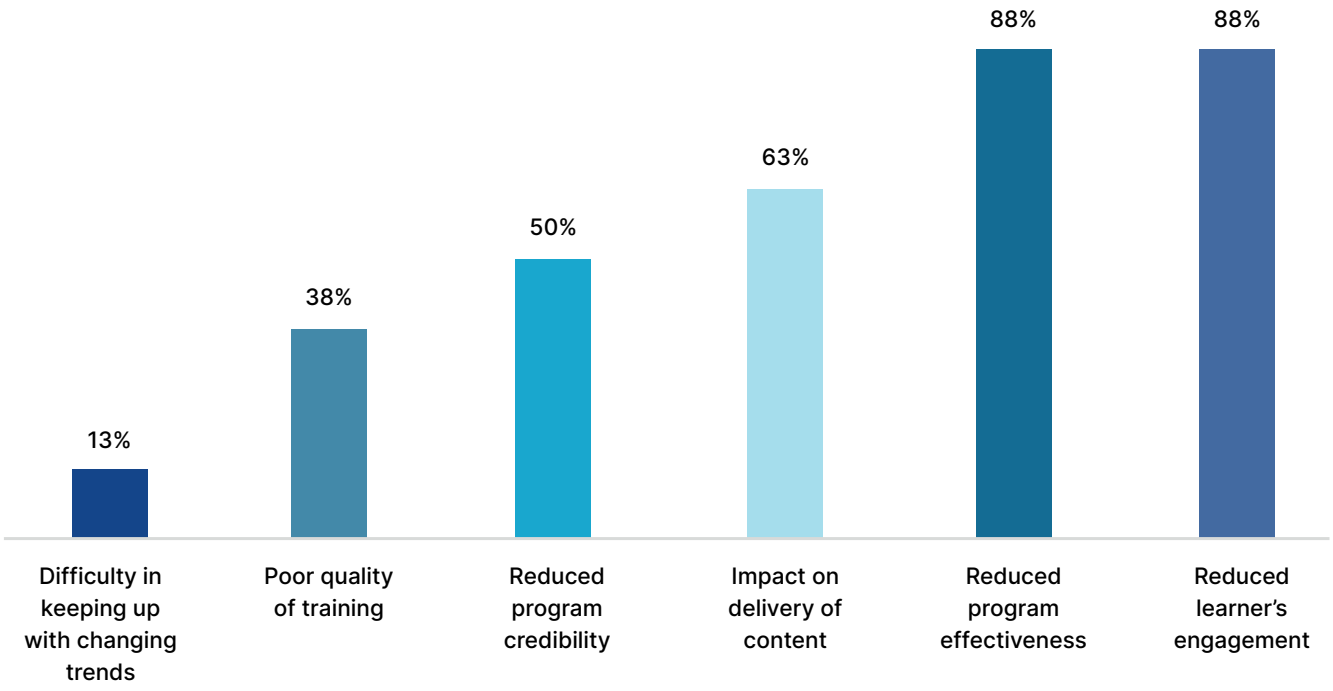


Impact on skilling programs because of lack of skilled trainers

The findings of the study indicate that it is crucial to have trained and skilled Cybersecurity trainers/faculties to bridge the gaps in the Cybersecurity skilling ecosystem.

This is evident in the opinion of a large majority (88%) of training providers who state that a lack of skilled and trained Cybersecurity trainers and faculties will result in reduced learner engagement and reduced program effectiveness. 63% of them have said it will impact the delivery of content. Further, 50% of them said that it will reduce program credibility, 38% was of the opinion that it will result in poor quality training and 13% of them said that it will lead to difficulty in aligning with the changing Cybersecurity trends as shown in Figure 30.

Figure 30: Impact due to lack of training

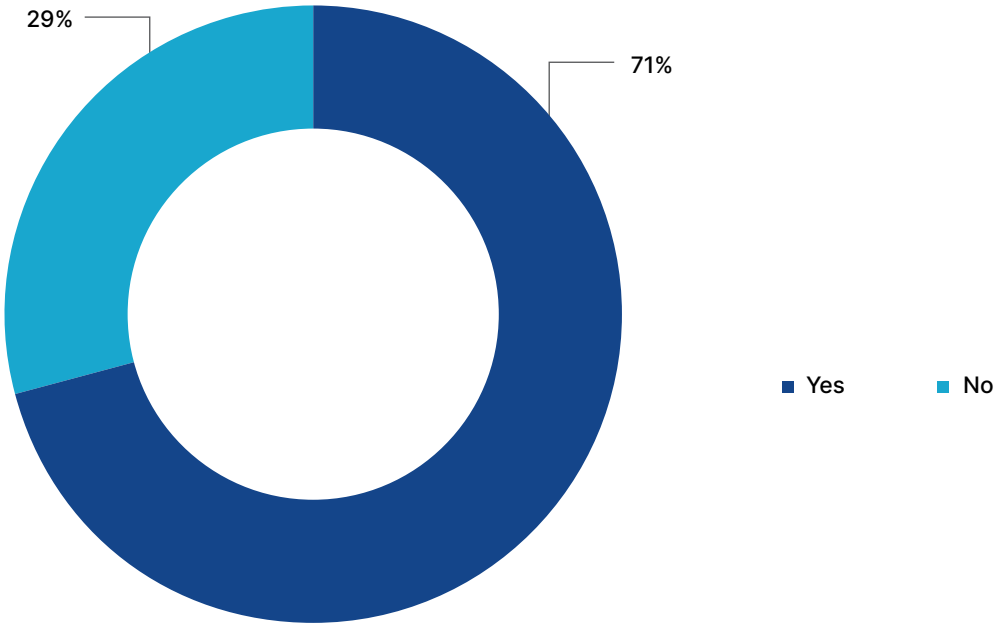


Placement scenario

Seeking the right opportunities

As shown in Figure 31, among the training providers included in the study, 86% training providers support their students with placements. Among them, most (71%) faced challenges in finding the right job opportunities for students who have completed a Cybersecurity program.

Figure 31: Challenges in finding right opportunities



Participation in Hackathons

Figure 32 shows, 73% of the students who were the part of the study have not participated in hackathon while pursuing the course on Cybersecurity. Only 27% of the students reported that they had participated in hackathon during the course duration.

During the interaction with academic institutions, it was also confirmed that there is low participation in Hackathons. Only 33% of the respondents mentioned that they participated in Hackathons. This finding indicates that a significant majority of academic institutions have limited engagement or involvement in Hackathons.

Migration Pattern

Among the most prominent challenge that training providers face in placing students is migration of students, particularly women. This challenge comes about as students are not encouraged by their families to relocate to other parts of the country for employment. 67% training providers have agreed to the same as shown in Figure 33.

Figure 32: Participation in Hackathons

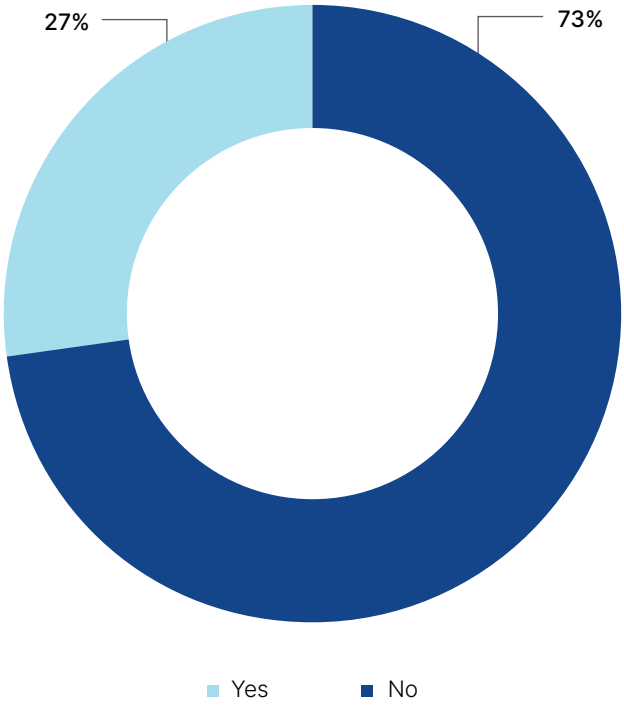
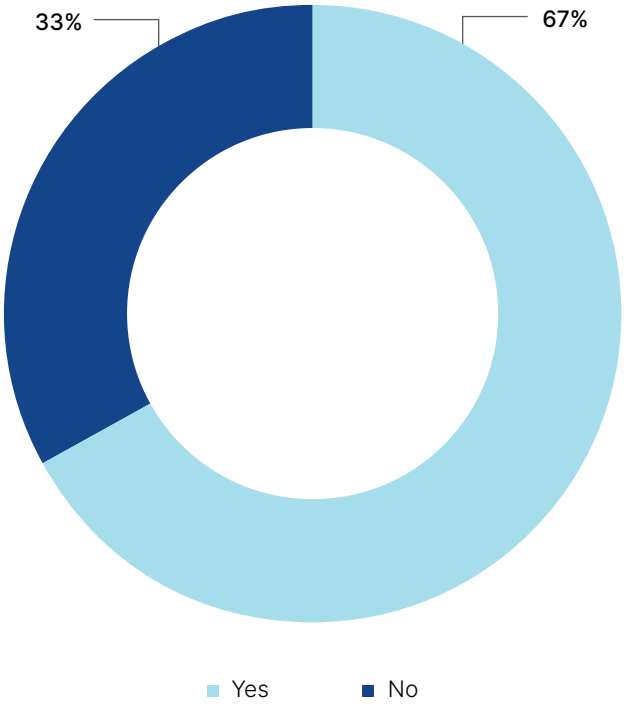


Figure 33: Challenges with respect to migration of students



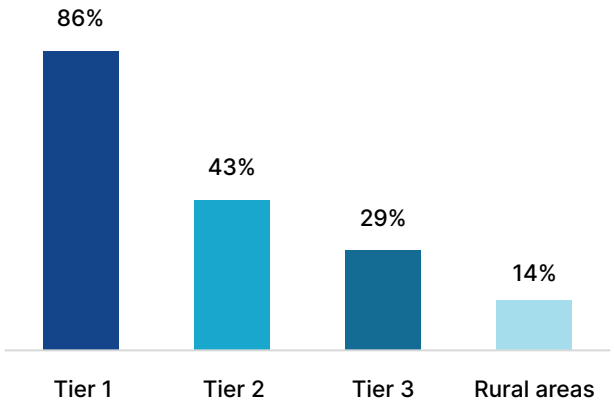
City wise distribution of placements

With respect to the locations where trained students are placed, the findings shows that most are placed in urban communities, with a higher percentage in Tier 1 cities. They also highlight a significant gap in job opportunities in Tier 3 cities and rural areas.

As shown in Figure 34, 86% of the training providers mentioned that students are placed in jobs in Tier 1 cities, 43% mentioned Tier 2 cities, and 29% responded that students are placed in employment in Tier 3 cities. Only 14% mentioned that students are placed in rural areas.

All respondents from training providers/NGOs identified Bangalore and Delhi NCR as the top cities with emerging job opportunities in cybersecurity. Hyderabad and Mumbai were mentioned by 71% of the training providers/ NGOs. Pune was reported by 57% of training providers while a similar proportion mentioned Chennai.

Figure 34: City wise distribution of placements

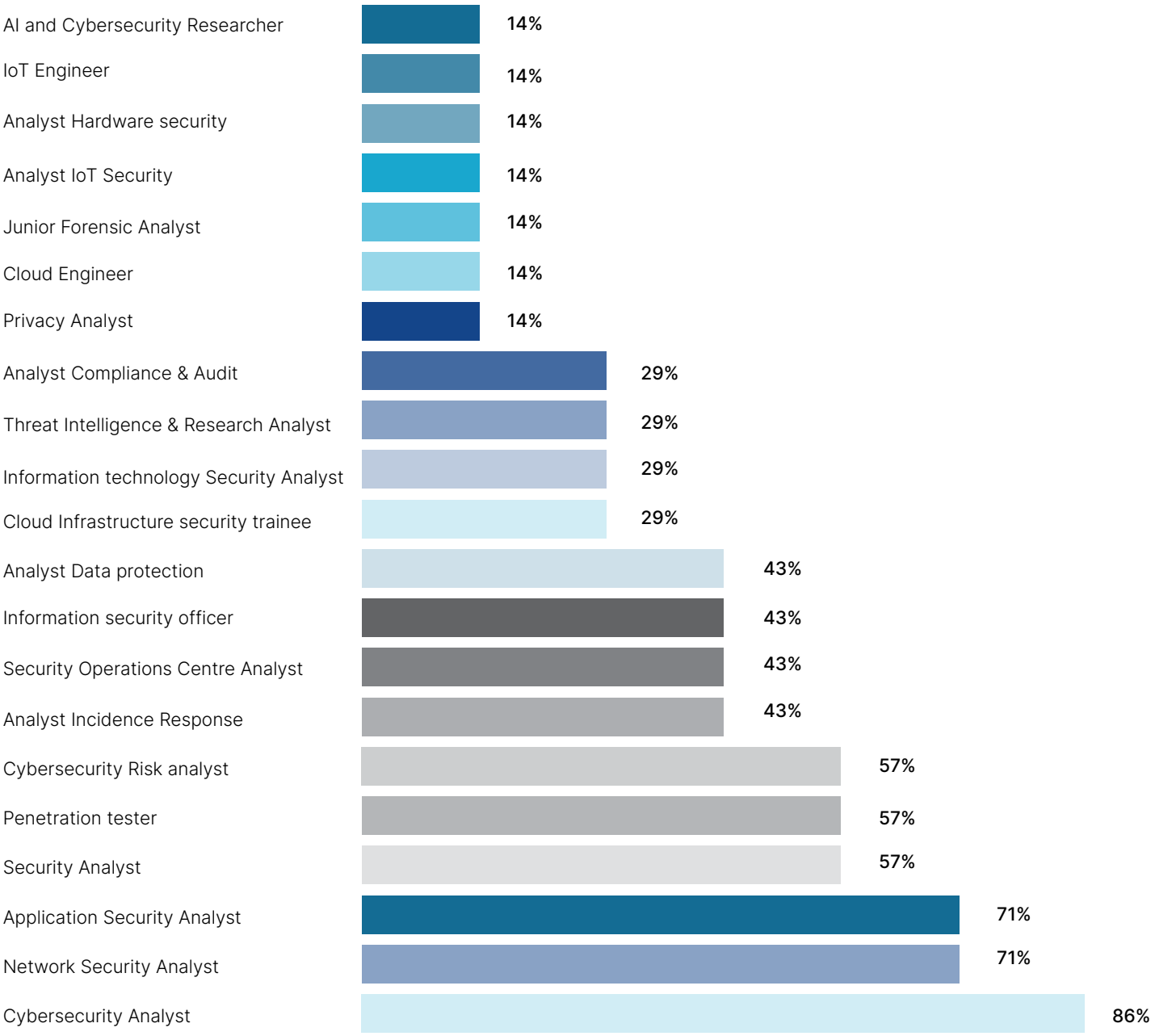


Cybersecurity Job roles offered to students

As shown in Figure 35, Cybersecurity Analyst is the most mentioned job which trained students are placed in (mentioned by 86% of training providers). This was followed by Application Security Analyst, and Network Security Analyst, which were each mentioned by 71% of the training providers.

Over half (57%) of training providers indicated Cybersecurity Risk Analyst, Penetration Tester and Security Analyst while 43% of the training providers mentioned Analyst Incidence Response, Information Security Officer, Analyst Data Protection and Security Operations Centre Analyst as jobs that students were placed in.

Figure 35: Job roles

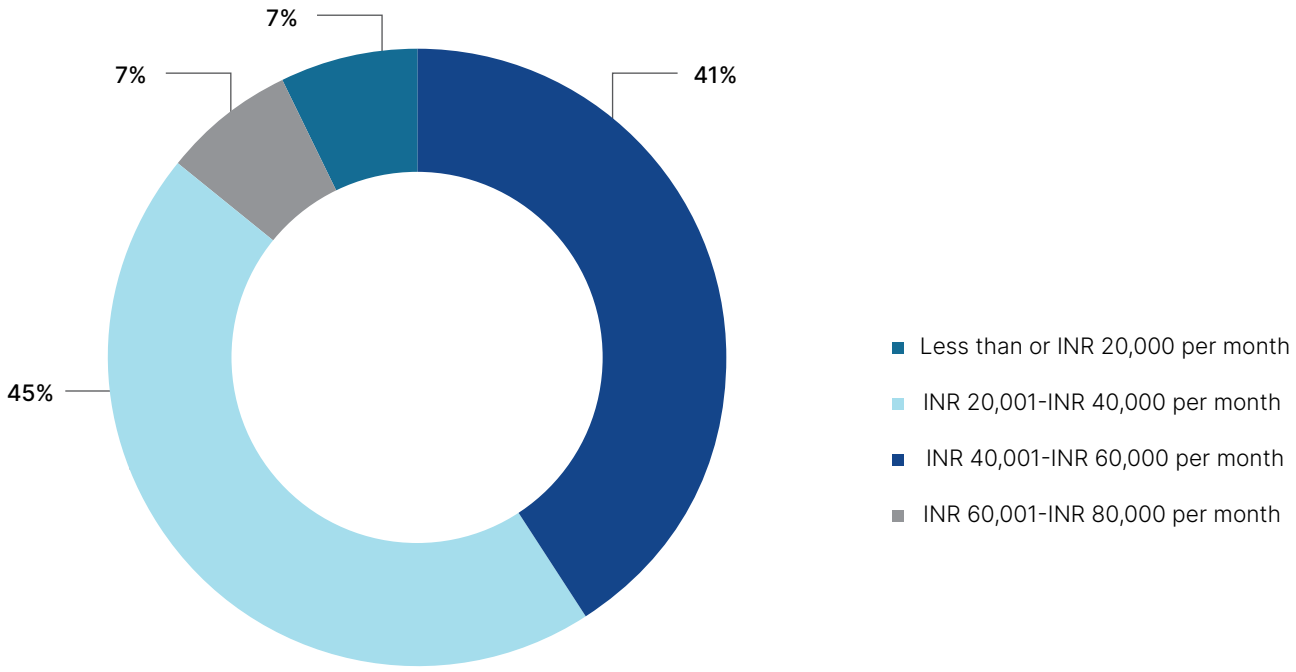


Other job roles where the students are getting placed (mentioned by 29% of training providers) are Cloud Infrastructure Security Trainee, Information Technology Security Analyst, Threat intelligence and Research Analyst and Analyst Compliance and Audit. These are followed by Cloud Engineer, Privacy Analyst, Junior Forensics Analyst, Analyst Hardware Security, Analyst IoT Security, IoT Engineer, AI and Cybersecurity Researcher and Analyst Data Protection.

Compensation offered to students

By and large, employed students earn between INR 20,001 to INR 60,000. A smaller number, (7%) draw INR 60,000 to 80,000 per month while a similar proportion of respondents earn INR 20,000 or less per month as shown in Figure 36.

Figure 36: Compensation range offered to students



Need for capacity building of professionals post placement

It is crucial for professionals to stay updated with the latest trends, techniques, and best practices to effectively protect organizations' digital assets. Refresher trainings serve as valuable opportunities for professionals to enhance their skills, expand their knowledge, and stay current in this dynamic cyber environment.
When asked about the need for refresher trainings, a vast majority of Cybersecurity professionals (78%) agreed that there is a need to provide training to professionals with 0-3 years of experience in cybersecurity, even if they have completed a relevant course or certification as shown in Figure 37.

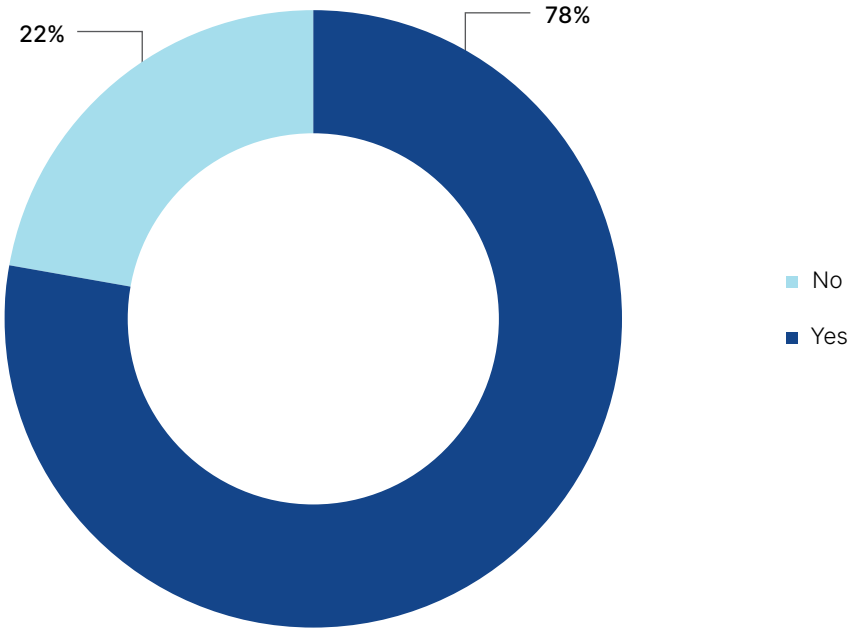
The reasons for this opinion include:

- The need to stay updated with rapid changes in the domain
- Education curricula do not cover the emerging nature of cybersecurity adequately
- The importance of practical skill training

- The vastness of the subject requiring continuous learning
- The necessity for operational knowledge and exposure
- Insufficiency of the curriculum in covering all aspects of cybersecurity fundamentals

Cybersecurity professionals emphasized that training plays a crucial role in bridging the gap between theoretical knowledge and practical application. It helps them becoming comfortable to deal with new challenges and equips them with tool-specific skills, vendor-neutral skills, and soft skills. Moreover, training ensures alignment between expertise and business requirements, protects confidential data, adapts to quantum security, and keeps professionals updated with the latest technologies. Such trainings also offer opportunities for networking, collaboration, and sharing of experiences with industry peers, and thereby foster a culture of continuous learning and improvement within the Cybersecurity community.

Figure 37: Need for refresher trainings



Chapter 6

Unveiling the obstacles: Challenges in implementing skilling programs by training providers/NGOs

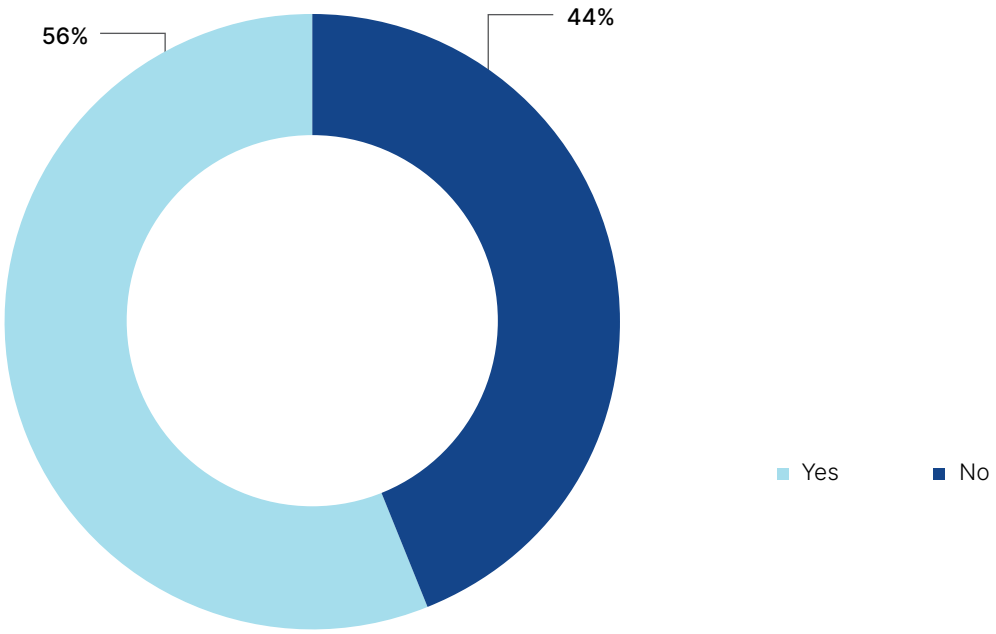
This chapter provides an overview of the challenges faced by training providers and NGOs in implementing skilling programs in the cybersecurity domain. It examines the challenges related to securing adequate financial resources and availability of digital infrastructure. The chapter also highlights the challenges with the availability of skilled and certified faculties to deliver high-quality training.

Implementing skilling programs comes with its own set of challenges. Training providers and NGOs play a crucial role in equipping individuals with the necessary skills and knowledge to thrive in today's competitive job market. However, they often face obstacles that hinder the smooth execution and effectiveness of their programmes. From limited resources and funding constraints to the need for aligning programs with industry requirements and ensuring sustainable outcomes, training providers and NGOs navigate a complex environment to successfully deliver impactful skilling programs. Some of these challenges are highlighted below.

Availability of funds with training providers

Hiring of skilled resources, support in program administration, having adequate infrastructure etc. depends completely on the adequate amount of funds received by the training providers.
The most significant challenge experienced by training providers/NGOs is the availability of funds for skilling programs in cybersecurity with 56% stating this as a major difficulty.

Figure 38: Availability of funds with Training Providers

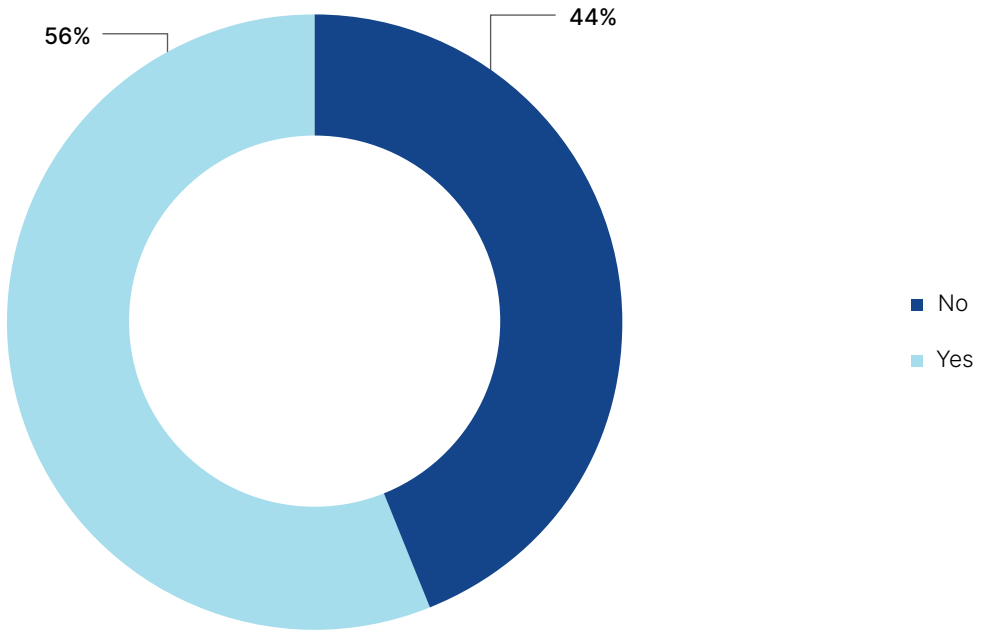


Availability of Digital Infrastructure

The availability of digital infrastructure is critical for the implementation of the Cybersecurity skilling programs. However, 56% of the training providers who were the part of the study have mentioned that they have experienced difficulties with respect to availability of digital infrastructure for Cybersecurity skilling programs.

The problems they face include unavailability of optimal computational systems, poor or no internet connectivity, and limited hardware devices like routers, access points in remote geographies. Moreover, setting up virtual labs, procuring licenced based tools, and software are expensive to procure and maintain.

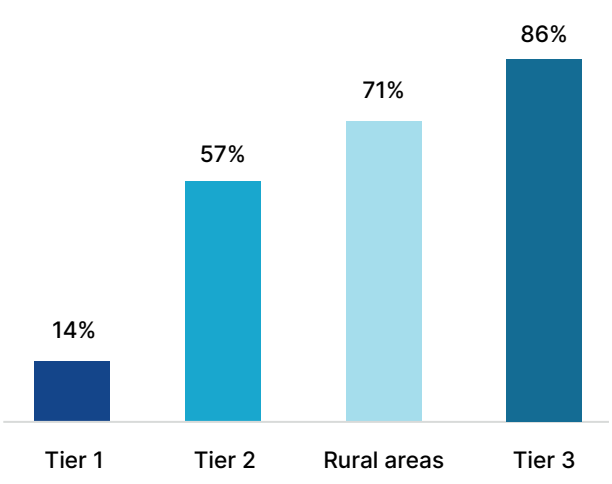
Figure 39: Availability of Digital Infrastructure



Insufficient Availability of Skilled faculties/trainers

78% of the training providers encounter challenges with respect to the availability of trained/ skilled faculties especially in remote geographies. As shown in figure 40, a majority of training providers/NGOs face difficulty in recruiting skilled faculties in tier 3 cities (86%) and rural areas (71%).

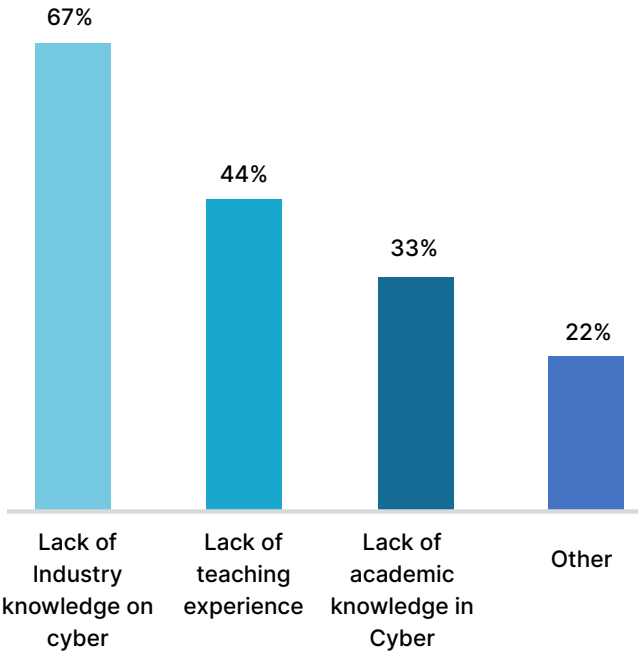
Figure 40: Availability of Skilled Faculties



Lack of Experience

67% training providers highlighted that the faculties/ trainers lack industry knowledge on Cybersecurity, while 44% mentioned that faculties lack teaching experience and 33% opined that they lack knowledge on Cybersecurity.

Figure 41: Challenges with respect to experience of Trainers



Challenges faced in upskilling

One of the main challenges faced is limited hands-on exposure to industry issues. The lack of practical experience can hinder the trainer's ability to help students understand and address real-world Cybersecurity challenges.

Another challenge is accommodating the training within the regular academic schedule, which poses a significant hurdle in providing comprehensive and effective training to students. Additionally, a major challenge lies in starting from a common point due to the diverse technical backgrounds, experience, and skills of the trainers. Bringing them to the same level of expertise for high-quality content delivery becomes a complex and demanding task.

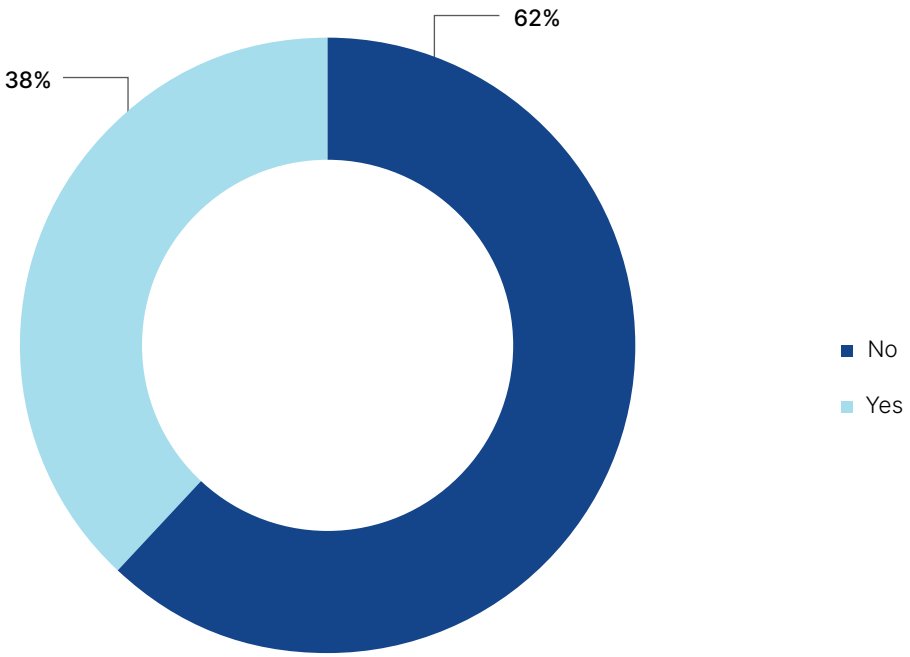
Lack of certified trainers

In a dynamic area such as Cybersecurity, it is crucial to have trainers who possess up-to-date knowledge, practical experience, and a deep understanding of the subject matter. Certifications play a vital role in validating the expertise and competency of professionals in the Cybersecurity field, provide a standardized measure of knowledge and skills, and assure training providers on the capabilities of their trainers and faculties.

During the survey, 73% of the faculties and trainers mentioned that their institute and training providers supported them with external certifications such CISSP, CEH, CompTIA Security+ while the remaining 27% of the trainers stated that no support was provided.

However, as shown in figure 42, even after support was provided, only 38% of the respondents could enrol and complete the certifications on cybersecurity. 62% of the trainers/faculties have not enrolled under any of the Cybersecurity certification.

Figure 42: Trainers certified on Cybersecurity



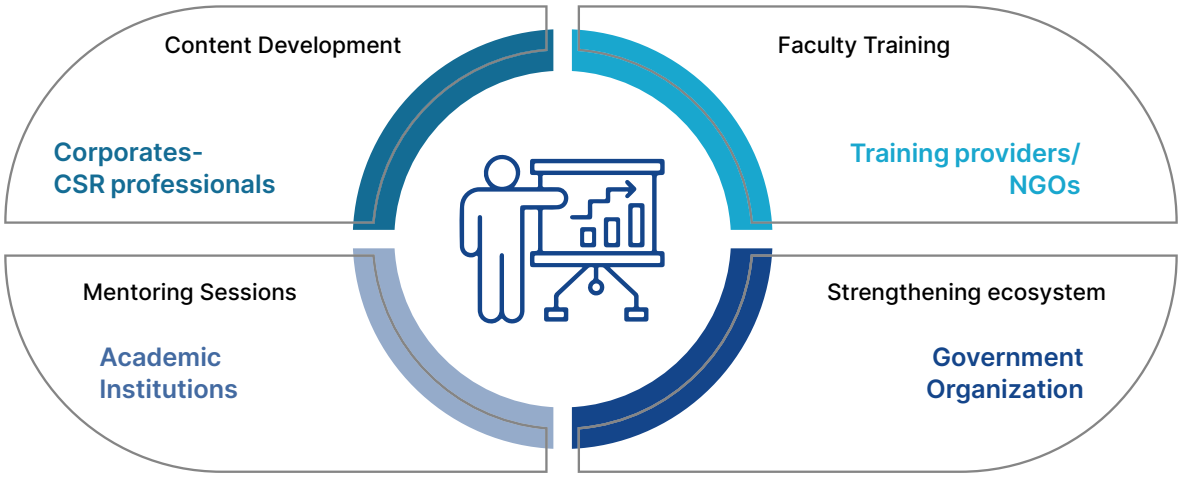
Chapter 7

Nurturing Partnerships: Exploring existing collaborations and future possibilities for collaborations

This chapter provides an overview of the importance of nurturing partnerships in the cybersecurity ecosystem. It highlights the existing collaborations between various stakeholders, such as training providers, academic institutions, industry experts, and government organizations. The chapter also explores the possibilities for future partnerships and the how it can benefit the Cybersecurity skilling ecosystem and contribute to the development of a dynamic and resilient Cybersecurity workforce.

To understand the existing partnership models and to explore the possibilities of future collaborations, interactions were undertaken with different stakeholders including corporate CSR professionals, academic institutes, training providers/NGOs, government organizations. Figure 43 shows areas that have been explored in the study for collaboration and partnership between key stakeholders in the Cybersecurity ecosystem.

Figure 43: Mapping roles and opportunities of key stakeholders



Corporates are the key drivers of the Cybersecurity ecosystem. The role of corporate is not limited to making investments in technology, digital infrastructure, designing strategies, protecting against cyber-attacks, providing services to the user organizations etc. Corporates also play a critical role in strengthening the cyber ecosystem by enabling collaborations between different stakeholders in areas such as developing academic curriculum, conducting capacity building programs for NGOs, academic institutions, and government agencies, providing mentoring sessions for students, and, most importantly, driving skilling programs on Cybersecurity.

50% of Corporates Cybersecurity professionals have agreed that presently, they have collaborated with other industries, academic institutes, sector skill council and Government agencies to strengthen the ecosystem. Going forward, 72% Corporates would collaborate with other stakeholders in the ecosystem.

Key areas of collaboration are partnership with Government bodies such as Centre of Excellence for Cybersecurity, collaborations with international organizations i.e., ISACA, NGOs like Data Security Council of India, academic institutes for incubator programs. Additionally, some of the corporates are acting as a knowledge/data bank for other stakeholders as they are supporting them with knowledge transfer on latest trends and conduct training and capacity building programs for them.

100% Corporate Social Responsibility professionals who were covered as a part of the study has committed to collaborate and partner with other stakeholders for driving Cybersecurity Skilling programs.

100% CSR professionals want to drive and implement the Cybersecurity skilling program in Academic Institutions and via. Centre of Excellence established by NGOs/Training provider. Only 50% of them want to implement the skilling program with ITI's and polytechnics.

The proportion of CSR professionals who want to collaborate with ITIs and polytechnics is lower because Cybersecurity roles demand a minimum qualification of graduation. However, the students who enrol in ITI and polytechnics lack this qualification and are those who have passed 12th standard or have dropped out of school.

Additionally, in the future, 100% CSR professionals want to collaborate with all key stakeholders to develop content and to support with mentoring sessions for faculties and students.

Opportunities for Collaboration with Training providers/NGOs and Academic Institutions

Academic institutions and training providers/NGOs play a pivotal role in driving Cybersecurity skilling programs. They support to design curriculum, implement skilling programs, conduct trainings, and provide capacity building sessions for trainers/faculty. Most importantly, they support corporates and government organizations to reach out to students from underprivileged communities in remote and aspirational geographies.

Figure 44: Development of Content and sharing of existing curriculum

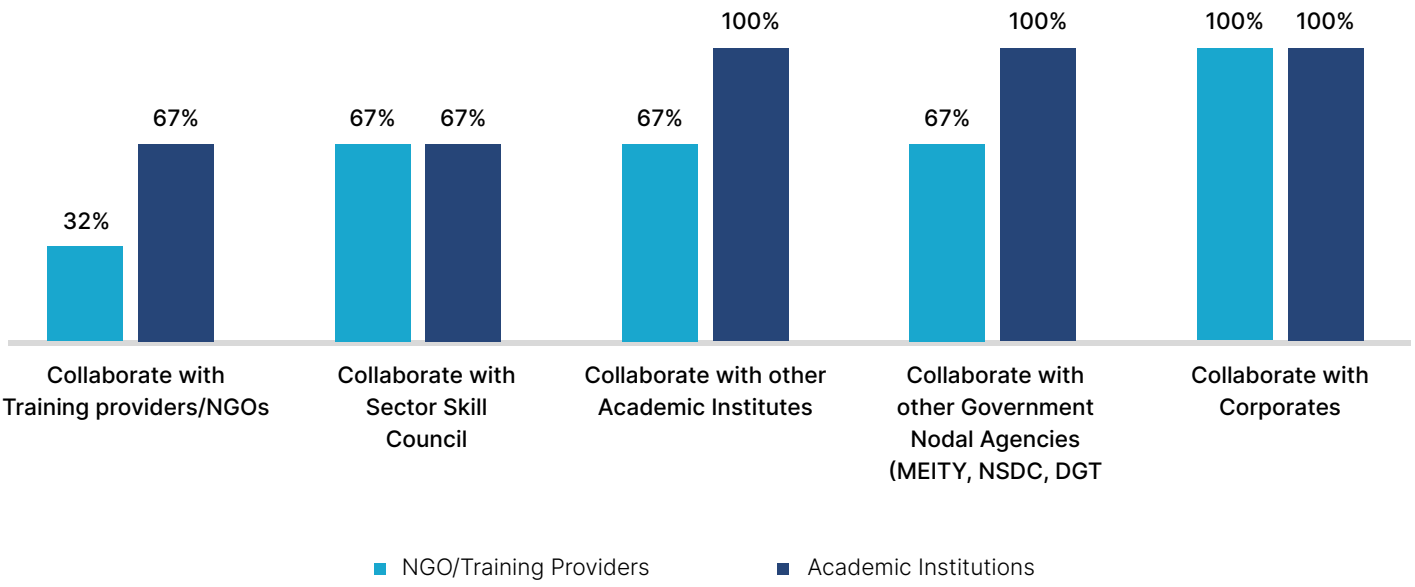
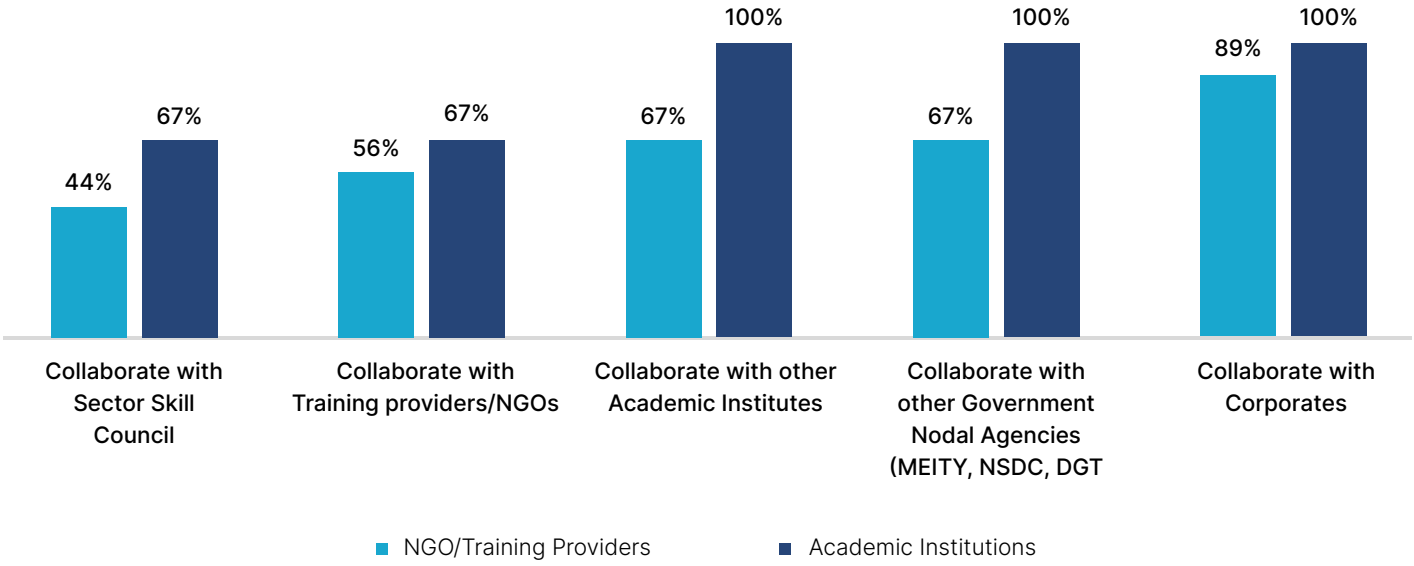


Figure 45: Training and Capacity building of Faculties/Trainers and sharing of skilled resources



Analysis: Figure 44 and Figure 45 shows the possibilities of future collaborations by academic institutions and training providers/NGOs for development of content and for training and capacity building of faculties/trainers.

Collaboration with Government agencies: Going forward, 100% academic institutions would collaborate with government nodal agencies and 67% would collaborate with Sector Skill Council for development of content and for training of faculties. A similar proportion of training providers/NGOS would collaborate with government nodal agencies and Sector Skill Council for development of content, for training & capacity building of trainers.

Collaboration with Corporates: There is a high desire to collaborate with corporates for content development training and capacity building of faculties among both groups of respondents.

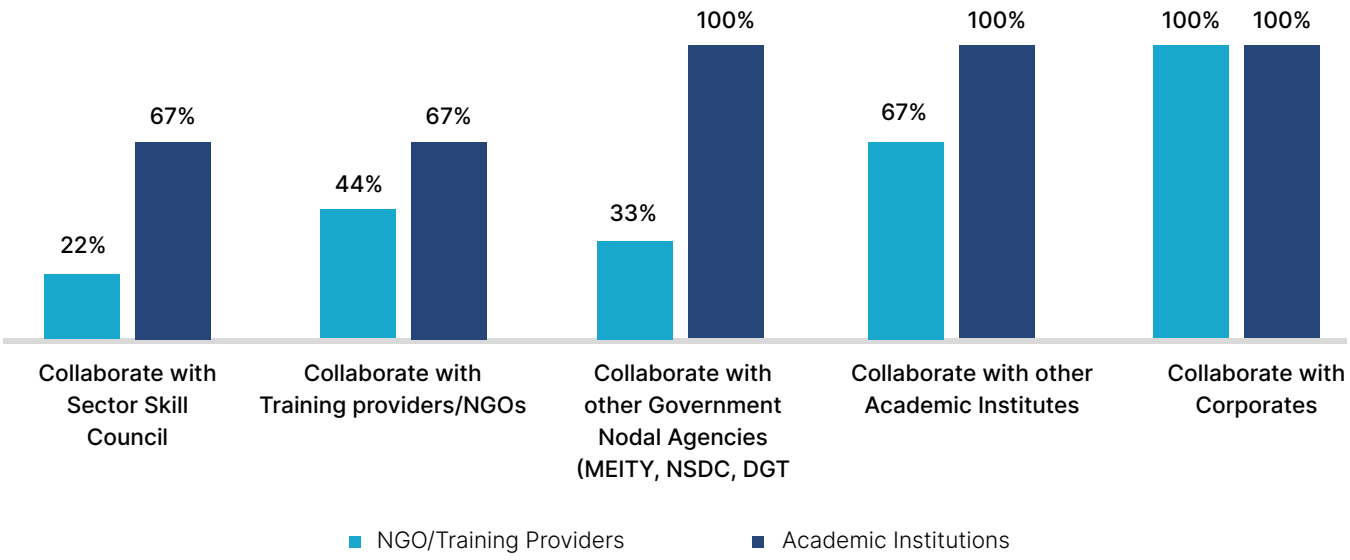
Collaboration with academic institutes: 100% Academic Institutions and 67% NGOs/Training providers would want to collaborate with Academic institutions.

Collaboration with training providers/NGOs: 67% Academic Institutions wants to collaborate with NGOs/ Training providers. Collaboration amongst training providers/NGOs is relatively low in content development. However, over half of them would be interested in collaborating with other training providers for capacity building programs.

Collaboration with government agencies: There are various opportunities where support can be leveraged from government stakeholders to improve the Cybersecurity skilling program ecosystem. These include seeking approval from NCVET, integrating the program on the Skill India portal and active participation of government stakeholders in the creation, design, curation, and advisory of the course curriculum and pedagogy. Additionally, government stakeholders can support in developing training frameworks, strengthening employment opportunities for Cybersecurity professionals, and funding and supporting private sector initiatives in the domain.

Mentoring sessions for students pursuing Cybersecurity

Figure 46: stakeholder collaboration for mentoring sessions



Collaboration among varied stakeholder groups in the ecosystem plays an important role in delivering mentoring sessions because it allows for the amalgamation of diverse expertise and perspectives, sharing of resources, expansion of networks, leveraging of strengths, and enhanced impact and reach. It can create more holistic and effective learning experiences for mentees resulting in continuous improvement and learning. Overall, collaboration enhances the benefits and potential of mentoring sessions for students and contributes to both personal and professional development.

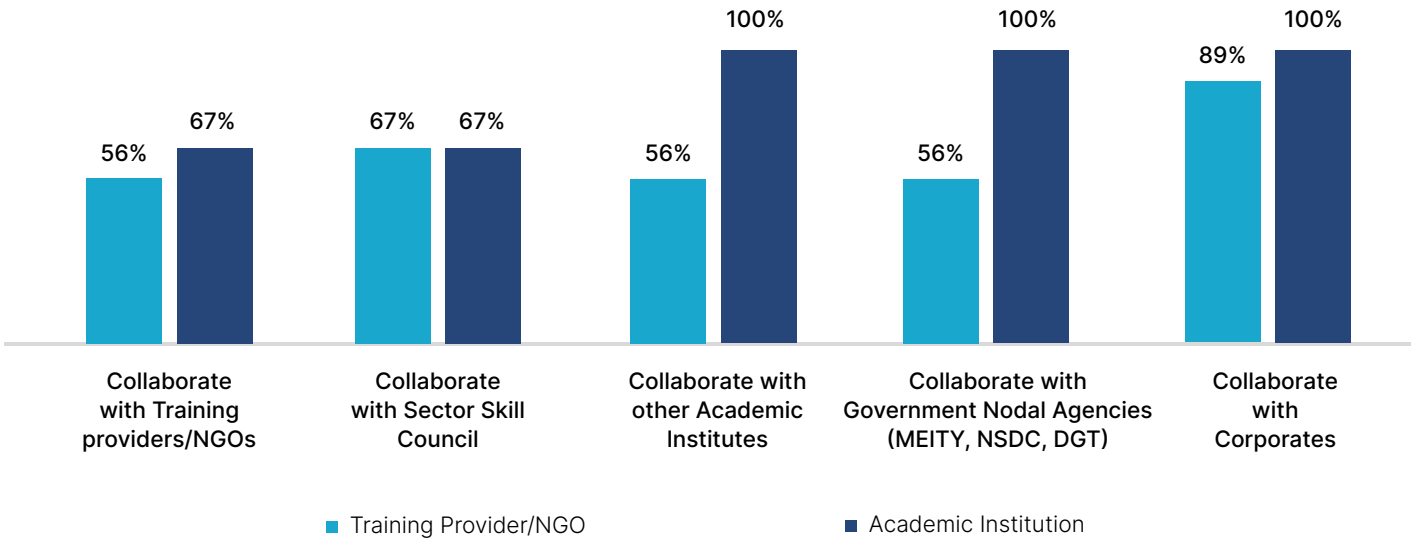
Academic institutions showed a strong interest in collaborating with other academic Institutes and government nodal agencies such as MeitY (Ministry of Electronics and Information Technology), NSDC (National Skill Development Corporation), and DGT (Directorate General of Training). 100% of the academic institutions expressed their desire to collaborate with these entities to organize mentoring sessions. Furthermore, the 67% of academic institutions also expressed interest in partnering with training providers/NGOs and Sector Skill Councils.

However, interest among training providers to collaborate with academic institutes to deliver mentoring sessions is lower. There is still lower interest in this stakeholder group to collaborate with others like themselves (44%) and with government nodal agencies and Sector Skill Councils (33% and 22% expressed interest, respectively).

As shown in Figure 46, interest among training providers/NGOs, and academic institutions in collaborating with corporates for organizing mentoring sessions is significantly high. The data indicates that all of the training providers/ NGOs and academic institutions expressed their willingness to partner with corporates, highlighting the recognition of the value that corporate collaborations can bring to mentoring initiatives.

Strengthening ecosystem of potential employers in Cybersecurity

Figure 47: Collaboration for strengthening ecosystem of potential employers



To increase the number of students getting placed and to ensure sustainable employment opportunities for students, it is crucial for academic institutes and training providers/NGOs to partner with other stakeholders to strengthen the existing ecosystem of potential employers.

Figure 47 shows, that corporates are the most desired partners for both stakeholders to strengthen the existing ecosystem. 100% academic institutes want to collaborate with corporates, government nodal agencies and other institutes. Their interest in collaborating with training providers/NGOs and Sector Skill Council is lower with 67% responding positively.

Among training providers/NGOs, 89% are interested in collaborating with corporates, 67% with Sector Skill Council and 56% each with government nodal agencies, academic institutes, and other training providers.

Impact of potential Collaborations/Partnerships

Bridging the skill gaps through partnerships and collaborations among varied stakeholders in the Cybersecurity ecosystem is essential for addressing the growing demands for skilled Cybersecurity professionals.

Collaborations among stakeholders will increase the value by creating sustainable solutions, sharing of resources and amplification of efforts that will have a positive impact on the youth perusing Cybersecurity.

Here's how partnership between Corporates, Academic Institutions, Training providers/NGOs, Government will help:

Bridging Skill Gaps through Industry-Aligned Cybersecurity Skilling Programs:

The collaborative approach will bring together stakeholders to develop a holistic training program that meets the specific requirements of the cybersecurity ecosystem. It would help in leveraging the collective expertise and resources of these stakeholders to ensure that students receive the necessary skills and knowledge to address constantly changing industry challenges effectively.

Identification of skill requirements:

The collaborative approach will allow the stakeholders to collectively assess the dynamic needs of the cybersecurity ecosystem and identify the necessary skills and competencies necessary for cybersecurity professionals contributing to the development of skilled cybersecurity professionals who are well-prepared to address the ever-evolving challenges in the field.

Sharing of resources and digital infrastructure:

Collaboration among stakeholders would enable the sharing of resources, including technology, expertise, and training facilities. This would contribute to optimizing the use of existing infrastructure, reduce costs and enhance the quality and accessibility of cybersecurity training programs. Such collaboration promotes an environment where stakeholders can collectively leverage their resources to improve efficiency and effectiveness in addressing skill gaps and delivering holistic cybersecurity training.

Leveraging network for reaching out to remote and aspirational districts:

Collaboration will help in harnessing the power of partnership to expand cybersecurity skilling programs to underserved areas, improve accessibility of training opportunities and nurture talent development in regions with limited resources. This would help to reduce the skill gap in the Cybersecurity workforce and bridge the digital divide.

Scaling up of programs:

Partnerships between different stakeholders would contribute to scaling up the cybersecurity skilling programs. Through collaboration, the stakeholders can leverage and utilize their combined resources, expertise, and networks to expand the geographic reach of the program reaching out to wider audience to access cybersecurity training and meeting the evolving demand for skilled professionals.

Monitoring and Evaluation:

Fostering partnerships between stakeholders would help in establishing a robust and strengthened monitoring and evaluation framework for cybersecurity skilling programs. Sharing of data, insights, and best practices among stakeholders would help to identify improvement areas for delivering high-quality cybersecurity training that aligns with the needs of the industry.

Recommendations

In order to effectively address the evolving threats encountered in the Cybersecurity space, it is crucial to assess the existing gaps within the Cybersecurity skilling supply chain and bridging these gaps through a multi-stakeholder approach. By identifying key areas of intervention and addressing the areas where expertise and knowledge are lacking, organizations can build a resilient workforce capable of mitigating emerging threats. The following recommendations cover the gaps assessed in this action research study and possible measure to address the same.

1. Increasing reliance on emerging technologies such as machine learning (ML), Internet of Things (IoT), and artificial intelligence (AI) is paving the way for more sophisticated cyber-attacks and leading greater demand for Cybersecurity solutions. To address these challenges, companies should have robust security measures, perform risk assessments at regular intervals that involve both internal and external risks associated, design comprehensive training programs inclusive of emerging technologies i.e., AI, ML and IoT to upskill existing employees and new hires, and educate them about risks associated with growing technologies, design comprehensive incidence response plans and engage & involve external Cybersecurity experts.

2. Over the next 5 years, an increase is expected in demand of specific technical skills and competencies, out of which the top ones are Artificial Intelligence, Data Forensics & Incidence Response, Hacking Wireless Network, Cloud Security, Compliance & regulatory knowledge, and Security Auditing. Furthermore, the research identified the gaps in the skills among early talent. To mitigate the skill gap, it is important to bring synergies between different stakeholders in the ecosystem to map industry-relevant skills, design and deliver skilling programs, promote corporates driven training initiatives, and identify opportunities for skilled professionals.

3. The participation of women and PwDs was found to be low in Cybersecurity workforce and skilling programs. To ensure equal representation of diverse groups, it's important for organizations to define and set D&I goals, formulate strong inclusive policies and practices fostering inclusion, actively seek diversity while recruiting candidates for Cybersecurity job roles, empower leaders from these groups, undertake sensitization programs for existing employees on D&I and mobilization drives in institutes, schools and communities. Additionally, it's vital to design training programs that cater to the needs of PwDs that involves customized training modules, assistive technologies such as, sign language interpreters, braille etc. considering diverse needs of students with visual and hearing impairments, mobility limitations and cognitive challenges. Furthermore, ensure accessibility to the skilling programs this includes physical accessibility such as elevators, ramps, accessible restrooms.

4. Level of awareness and number of students completing Cybersecurity certifications was observed to be relatively low among the students who are enrolled in skilling programs driven by CSR and participated in the study. To bridge the skills gaps and increase the awareness about the Cybersecurity as career pathways, it is imperative to implement effective measures and strategies such as increasing the frequency of awareness sessions on Cybersecurity, sensitizing the students about career pathways. Further, the academic institutes should aid in increasing awareness and sensitization about the career opportunities in the domain. Providing financial assistance such as scholarships and addressing the certification gaps by incorporating and sponsoring Cybersecurity certification as a part of their skilling initiatives should be considered by the CSR interventions.

5. The availability of skilled faculty members and lack of trainings/infrequency of refresher training for faculties remains to be the most significant challenges encountered by training organizations or NGOs in Cybersecurity training especially in tier 2 & tier 3 cities and rural areas.

   To effectively address the challenge, it is crucial to develop a pool of trainers. This necessitates a) development of a strong network comprising diverse stakeholder groups to establish training and skilling programs specifically designed for faculties in tier 2 & tier 3 cities and rural areas. b) Promotion of Faculty Development Programs (FDPs) for existing resources and connecting with faculties in tier 1 cities may also be taken in collaboration with academic institutions, government departments like AICTE. c) foster partnerships with industry experts; invite subject

matter experts i.e., Cybersecurity practitioners to share the knowledge and provide practical insights. d) collaborate with government and academia to imbibe the training curriculum as a part of their L&D within the institutions. e) engage retired Cybersecurity professionals and faculties in skilling programs and onboard them in geographies where there is lack of availability. f) provide access to resources such as LMS or tech-based platforms that offer the flexibility to engage and upskill, g) encourage them to pursue industry recommended certifications and gathering regular feedback to improve effectiveness of the training program is an essential requirement in a sector which is driven by innovation.

6. Only a few academic institutions have validated their content for Cybersecurity, whereas the most other training providers interviewed have not validated their content. To mitigate the gap and to ensure that the content delivered is in alignment with the industry requirements and latest trends of the ecosystem, it is important for training providers and academic institutions providing training on Cybersecurity to validate their content. Content may be validated in collaboration with industry experts, corporates, and validation bodies to ensure that it meets industry standards and best practices. This may result in reduced disparity between academia and industry in terms of knowledge requirement from candidates as well as addressing the demand and supply gap in Cybersecurity landscape.

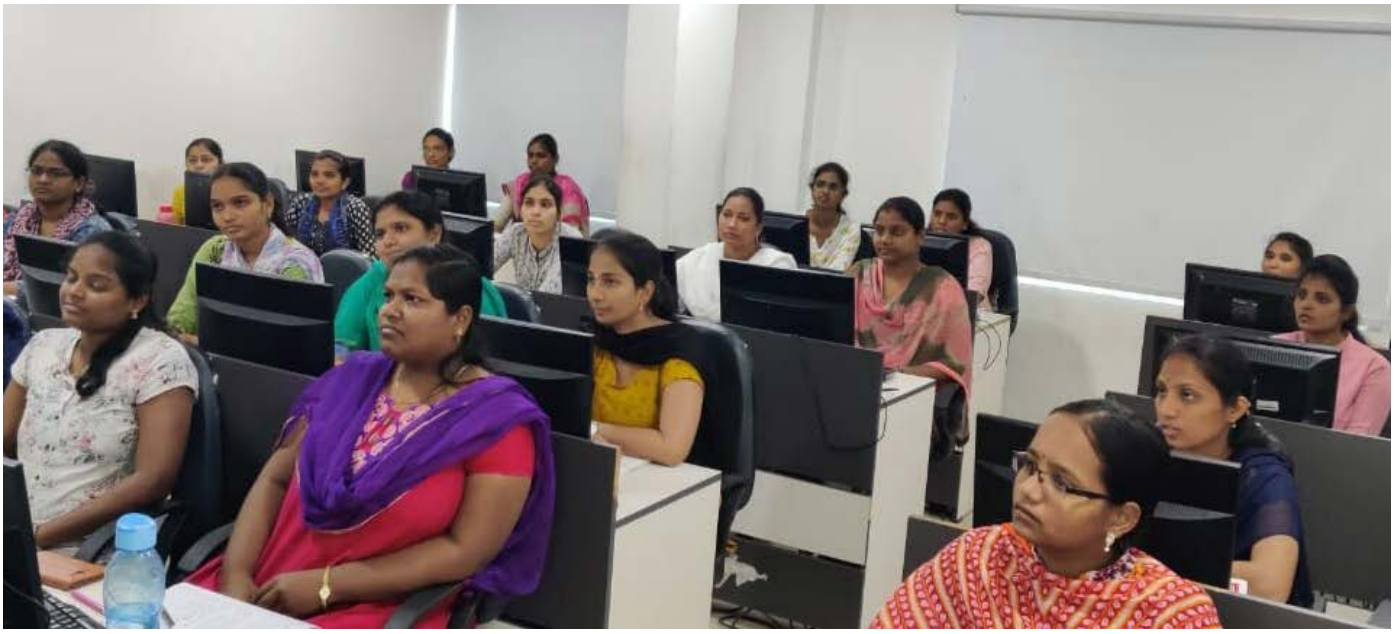
7. Another challenge faced by training providers is the availability of digital infrastructure. Building digital infrastructure is cost-extensive; therefore, training providers may undertake a comprehensive assessment of the existing infrastructure and prepare a strategic plan to ensure utilization of existing resources and development of new infrastructure as per needs. Partnership with government and private sector organizations is also crucial in funding and implementing the initiatives through improved digital infrastructure and developing skilled workforce capable of operating and maintaining the infrastructure.

8. To increase the percentage of students getting placed in cyber security from cyber skilling programs it's important- a) To effectively address the challenge, training providers should make efforts to diversify their partnerships with a wider range of stakeholders. Pooling resources and expertise can facilitate in creating large-scale programs and may help in mapping suitable opportunities for such candidates in different geographies, b) encourage employees to contribute through skill-based volunteering, evaluate outcomes of CSR driven skilling programs and identify the areas of improvement. This approach would help in refining the strategies and ensure more successful placements. c)Furthermore, active involvement and participation of students in hackathons can significantly enhances their prospects of security employment. d) Additionally, corporates may re-define their preferences to hire students who are specifically trained in Cybersecurity. This can be achieved through Cybersecurity skilling programs driven by CSR (such as Cyber Shikshaa). e) training providers can participate in Rozgar mela organized by Government to explore the possibility of employment.

9. Migration of students post placement is a major challenge experienced by the training providers. The issue of student migration is increasingly evident among women due to lack of family support in relocating for employment who were covered in the study. To mitigate this challenge and encourage students to relocate, training providers can organize awareness and career counselling sessions targeting both the learners and their families, connecting students with alumni who have successfully relocated after placement and exploring remote work opportunities in the sector.

10. Corporates can look into strengthening existing evaluation parameters like annual appraisal KRAs and billability to measure professionals' efficiency and performance in the domain, such as their ability to respond to security incidents, time taken to detect the security incident, time taken to respond and mitigate security incidents, vulnerabilities identified and mitigated, security controls ensured by the professionals and compliance with regulatory frameworks. The parameters may vary for each organization depending on the organization's category; however, more sector specific parameters are required for performance evaluation of such professionals.

Notes



CYBER shikshaa

A Joint Skills Initiative of

Microsoft DSCI PROMOTING DATA PROTECTION

DSCI in partnership with Microsoft and in support with Information Security Education and Awareness (ISEA) of Ministry of Electronics & IT (MeitY) launched CyberShikshaa in September 2018.

The CyberShikshaa flagship program 'Cybersecurity Training Program' trains women engineering graduates from tier-II, tier-III cities and rural areas in the niche field of Cybersecurity. C-DAC, NIELIT and our other premier training partners conduct the online/offline training sessions. CyberShikshaa students being placed successfully in global corporations, large technology services firms, start-ups and even law enforcement agencies is a highly satisfying outcome.

In 2021, after a successful run of the initial Cybersecurity Training Program, 'Privacy Module for Women on Break' was rolled out for women professionals who are on career break due to medical, personal or any other reasons and want to make a career in Data Privacy. This is a pioneer credentialing program which equips women professionals with necessary skills to advance their careers in the growing field of Data Privacy and has seen women successfully restart their career even after break period of seven or eight years. Additionally, a self-learning 'CyberShikshaa Fundamentals' program is also launched to introduce Cybersecurity concepts to college students so that they can aspire for careers in cybersecurity in future.

For more information visit us at : https://www.dsci.in/cyber-shikshaa/

DATA SECURITY COUNCIL OF INDIA
NASSCOM Campus, 4th Floor, Plot No. 7-10,
Sector 126, Noida (U.P.) - 201303, India
For any queries contact
P: +91-120-4990253 | E: research@dsci.in | W: www.dsci.in

DSCI_Connect dsci.connect dsci.connect
data-security-council-of-india YouTube dscivideo