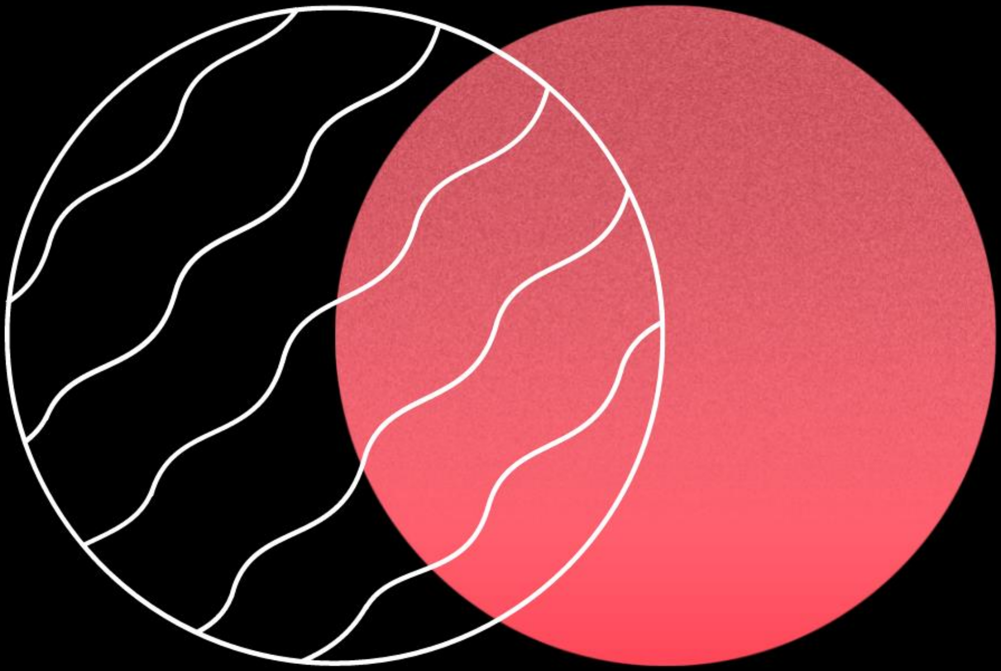
SRI LANKA
CERT|CC



Assessing the Supply and Demand of Cyber Security Professionals in Sri Lanka to Formulate a National Strategy

Final Report

December 2021

25 ipid Institute for Participatory Interaction in Development
Leading in Participatory Development

Institute for Participatory Interaction in Development

No. 23, P. Ruban Peiris Mawatha, Kalubowila, Dehiwala

Telephone: +94(011)2723225

Acronyms and Abbreviations

CSP:	Cybersecurity Professional / Practitioner
CSCx:	Cybersecurity Centre of Excellence
BPM:	Business Process Management
GoSL:	Government of Sri Lanka
NCSOC:	National Cybersecurity Operations Center
NCSI:	National Cyber Security Index
KII:	Key Informant Interview
ICTA:	Information and Communication Technology Agency of Sri Lanka
IPID:	The Institute of Participatory Interaction in Development
TVET:	Tertiary and Vocational Education Commission
SLASSCOM:	Sri Lanka Association of Software and Service Companies
SLCERT:	Sri Lanka Computer Emergency Readiness Team
SLCPA:	Sri Lanka Cyber Protection Agency

Table of Contents

List of Figures

List of Tables

Chapter 1: INTRODUCTION

1.1 Introduction

Digital Infrastructure development has been identified as one of the key areas towards achieving the national policy objective of digitization of the Sri Lankan economy. Usage of government networks and applications will be increased rapidly, and it is essential to ensure the security, availability and convenience. Cyber-attacks against businesses and government agencies are on the rise. With the vision of creating secure Digital Infrastructure, the Information and Communication Technology Agency of Sri Lanka (ICTA) together with the Sri Lanka Computer Emergency Readiness Team (CERT) has embarked on a significant and important initiative to build the National Cybersecurity Operations Center (NCSOC). The aim of it is to drive a holistic and comprehensive approach to Cybersecurity protection for the country. This will enable overcoming the barrier of identifying the cybersecurity attacks to the information systems in a proactive manner while ensuring the security and availability of government services. This will build the trust on government services which would further facilitate the usage and adoption.

In 2005 Information and Communication Technology Agency (ICTA) started the e-Sri Lanka initiatives to roll out the various electronic online services in Seri Lanka. The key initiatives such as e-revenue license, Electronic Travel Authority (ETA), e-population register etc. The web hosting for government organizations was commenced parallel to the mentioned initiatives. Due to rapid cybercrimes recorded after implementing these initiatives, there was a need to secure those systems. Based on this requirement, the Sri Lanka's National Computer Emergency Readiness Team (SLCERT) was established in 2006. It was formed by the ICTA as a fully owned subsidiary and non-profit organization. Number of incidents reported to the CERT has rapidly increased in 2010/11 approximately by 1000%. Subsequently in 2017, CERT has introduced the National Cybersecurity Strategy for Sri Lanka which was motivated to accede Budapest Cybercrime convention as the first South Asian country.

The Government of Sri Lanka has noted that electronic communication across cyber space has been recognized as a crucial factor that can directly affect national security. Hence, Sri Lanka's cabinet has recently approved Defence Cyber Command bill and a separate bill of cybersecurity laws outside the Defence purview. The prime objectives of this bills are expected to keep criminal and terrorism related activity online in check, strengthen the individual cybersecurity units, etc. The second bill is provided a provision to establish of a Sri Lanka Cyber Protection Agency (SLCPA) to work in conjunction with other agencies. Moreover, this initiative will introduction of legal provisions required for protecting infrastructure facilities related to decisive and essential information within the country, prevention of risk activities that affect the cybersecurity as well as creating a formal cyber protected environment within the country.

This report is the preliminary findings of the nation's first national level survey undertaken in Sri Lanka to assess the supply and demand of cybersecurity professionals in Sri Lanka. The report covers the findings with regard to the demand of the market for cybersecurity professionals.

Several national level studies have been carried out over the years to assess the ICT workforce and its strengths which has contributed to the success of this ever-expanding sector. However, there is a lack of data regarding the cybersecurity sector workforce and the market status quo in Sri Lanka, which falls within the aforementioned ICT workforce. The supply side of the equation has seen some action in recent years, with several private institutions now offering diplomas and degrees in cybersecurity, but there is also a gap in information regarding the employability of these diploma and degree holders. The survey hopes to feed data to the SDG Goal 9 of the Sustainable Development Goals (SDGs) dedicated for 'Industry, Innovation and Infrastructure', as well as the 3rd strategic thrust area of 'The Information and Cybersecurity Strategy of Sri Lanka 2019-2023', which is the 'Development of a Competent Workforce'.

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. IT analysts have been found that cost covering cybersecurity will be predicting five-year spending forecast about $1 trillion. Global statistics shows that cybersecurity costs have been increased from 2019 to 2020 by 24.7 %. The average global cost of cybercrime increased by over 27% in 2019. The most expensive component of a cyber-attack is information loss, which represents 43% of costs. Also Due to the COVID-19 outbreak an uptick in sophisticated phishing email schemes by cybercriminals has emerged. The cost of cybercrime is estimated to reach $6 trillion worldwide by the end of the year, and therefore the demand for skilled cybersecurity experts is higher than ever. Over an eight-year period tracked by Cybersecurity Ventures, the number of unfilled cybersecurity jobs grew by 350%, from one million positions in 2013 to 3.5 million in 2021. For the first time in a decade, the cybersecurity skills gap is leveling off. Looking five years ahead, we predict the same number of openings in 2025. Women represent 25% of the global cybersecurity workforce in 2021, according to Cybersecurity Ventures, up from 20% in 2019, and around 10% in 2011. ICT analysts expect a steady uptick in the number of women filling cybersecurity jobs over the next decade.

In 2015, Sri Lanka become a fully-fledged member of the Budapest Convention on Cybercrime. As a country it is essential to introduce an unformed mechanism and rules of procedure and evidence, while bringing all parties together under the umbrella of Budapest convention to mitigate the cybersecurity incidents. There are certain challenges that one will have to face in mitigating the cybersecurity threats in Sri Lanka such as lack of awareness among citizens on cybercrimes, Lack of readiness among the stakeholders, gaps in laws in relation to modern cybercrimes and lack of cooperation among the relevant stakeholders etc.

This survey was carried out to assess the both supply potentials and demand opportunities of the cybersecurity practitioners. Moreover, the data collection was carried out within a framework consisting of several definitions that allow for clear analysis and presentation of the findings. Some of the definitions were adopted from the ICT workforce surveys conducted by ICTA for continuity. The data presented in this report should be understood in the context of the following definitions;

Table 1: Table of Definitions

Words Used/ Abbreviation	**Definition**
ICT Workforce	The ICT workforce was defined in the survey to cover dedicated employees who undertake ICT related specialist job functions. Accordingly, any person involved in ICT related tasks or producing ICT related output as his/her primary job function is considered as a member of the ICT workforce.
Cybersecurity	Cybersecurity refers to the technologies, processes, and practices designed to protect computerized systems, networks, devices, programs, and data from cyber-attacks, or unauthorized access.
Cybersecurity Professional / Practitioner	Experts who are responsible for securing the information systems /IT infrastructure (Software and Hardware) of an organization against from web threats, malware, viruses, DoS attacks, phishing, etc.
Full-time Cybersecurity Practitioners	Sole responsibility / only job description.
Part-time Cybersecurity Practitioner	In-house staff (mostly IT) that perform Cybersecurity requirements as part of their job description apart from the main duties responsibilities that they have been assigned.
Cybersecurity related Courses	Courses / Programmes that offer a combination of computer expertise and cybersecurity education. For the study courses that contains a minimum of one third of the subject matter (Course Units/ Modules) on cybersecurity will be considered as a cybersecurity related course.

Words Used/ Abbreviation	**Definition**
ICT Companies	ICT companies offer a diverse range of ICT products that includes hardware and software products and a range of ICT-based services which provides IT and networking solutions for customers in Sri Lanka and abroad. The ICT companies include both relatively large business entities that offer their products to customers such as major companies and public sector organizations as well as small businesses that cater to retail markets or small-scale customers. The latter can be identified as an 'informal' subsector of the industry.
BPM Companies	BPM companies are either subsidiary units or independent third-party service providers to which specific business operations in supply chains of large companies have been outsourced. The BPM industry consists of, but is not limited to, many value-added services such as finance and accounting outsourcing (FAO), legal process outsourcing (LPO) and knowledge process outsourcing (KPO) have come into operation.
Non-ICT Companies	The use of ICT has become widespread in all sectors of the economy and a large number of companies that offer goods and services other than ICT related products also use ICT facilities for production and delivery of their output to customers. As a result, many non-ICT companies maintain in-house ICT facilities and recruit dedicated ICT staff.
Government Organizations	They include central government organizations, provincial councils and local government authorities. The central government organizations include ministries and line agencies dedicated to different subjects and the network of regional administration bodies comprised of 25 district secretariats and 331 divisional secretariats. The nine provincial councils include provincial ministries, line agencies and local government authorities.
ICT Training Organizations	Government universities, private degree awarding institutes, government vocational and tertiary training institutes, and private diploma and certificate awarding training institutes. The sample included all government universities, UGC recognized institutes, and other institutes that award degrees on fields relating to ICT in affiliation with foreign universities.

1.2 Rationale to the Study

The requirement of this study was initially identified by the Sri Lanka CERT and they hired The Institute of Participatory Interaction in Development (IPID) to carry out this study as a third-party consultant. Sri Lanka CERT acts as the focal point for cybersecurity of the nation which is having a mandate to protect Sri Lanka's Information and Information Systems Infrastructure. Its services range from responding to investigating information security breaches, in order to prevent security breaches through awareness, security assessments, managed services, forensics and capability building. The types of incidents received by Sri Lanka CERT include incidents related to social networks, email compromise, phishing, web site compromise, scams, malicious software issues and ransomware, privacy violations, financial frauds, compromised unique IP's extracted from the information collected by automated systems operated by international organizations.

Incidents reported to Sri Lanka CERT have increased to 16,376 in the year 2020. In the year 2019, 3566 incidents were reported. This is nearly a 460% increase in reported incidents compared to the year 2019.

1.3 Objectives of the Survey

The aim of this national cybersecurity workforce survey has been to gain an understanding on the supply and demand of the cybersecurity professionals of the country. The specific objectives of the survey were to;

1. Gather data and carry out an analysis of the supply of professionals for the information and cybersecurity related job roles.
2. Gather data and carry out an analysis of the demand for the information and cybersecurity professionals in the job market.
3. An analysis of the gap between supply and demand of information and cybersecurity professionals.
4. Use the generated findings to formulate an operational strategy to fill the gap between supply and demand of information and cybersecurity professionals in Sri Lanka.

1.4 Scope and Coverage of the Survey

The following table illustrates the different types of institutes covered by the Demand Survey. Table 1 further describes the number of institutes which have cybersecurity practitioners, average cybersecurity institutes per institute etc.

Altogether 22 institutes were covered during the Supply Survey. During the Supply Survey IPID was able to collect data from thirteen (13) Government Universities, six (6) Private

Degree Awarding Institutions, two (2) Registered Vocational Training Institutes and One (1) Professional Training Provider.

Table 2: Institutes covered by the Demand Survey

Type of the Institutes	**Total Number of Institutes**
Cybersecurity Firms	13
Other IT Firms	45
Private Sector Non-IT Firms	69
BPO	11
Banks and Financial Firms	26
Government Institutions	69
Total / Average	**233**

1.5 Overview of the Methodology

Reports published by ICTA and SLASCOM as well as international publications were reviewed when creating designing the first survey demand assessment of cybersecurity professionals targeting the cybersecurity workforce in Sri Lanka. This allows cybersecurity workforce data to be easily placed within the framework of the ICT workforce data already available. As mentioned in the Table 1, IPID was able to cover totally 233 institutes for Demand Survey and 22 institutes for Supply Survey. Semi-structured questionnaire surveying technique was used to collect field data. The purposively calculated sample size was taken for the Demand Survey. The lists of Cybersecurity firms, Other IT firms, Private Sector Non-IT firms, BPOs, Banks and Financial firms and Government institutions were taken from SLASSCOM. Then purposive samples were taken from each category and the selection of firms/ institutes was done randomly. However, for the Supply Survey, all institutes which are offering cybersecurity related courses were taken. Following chart illustrates the number of firms/ institutes covered by the survey.

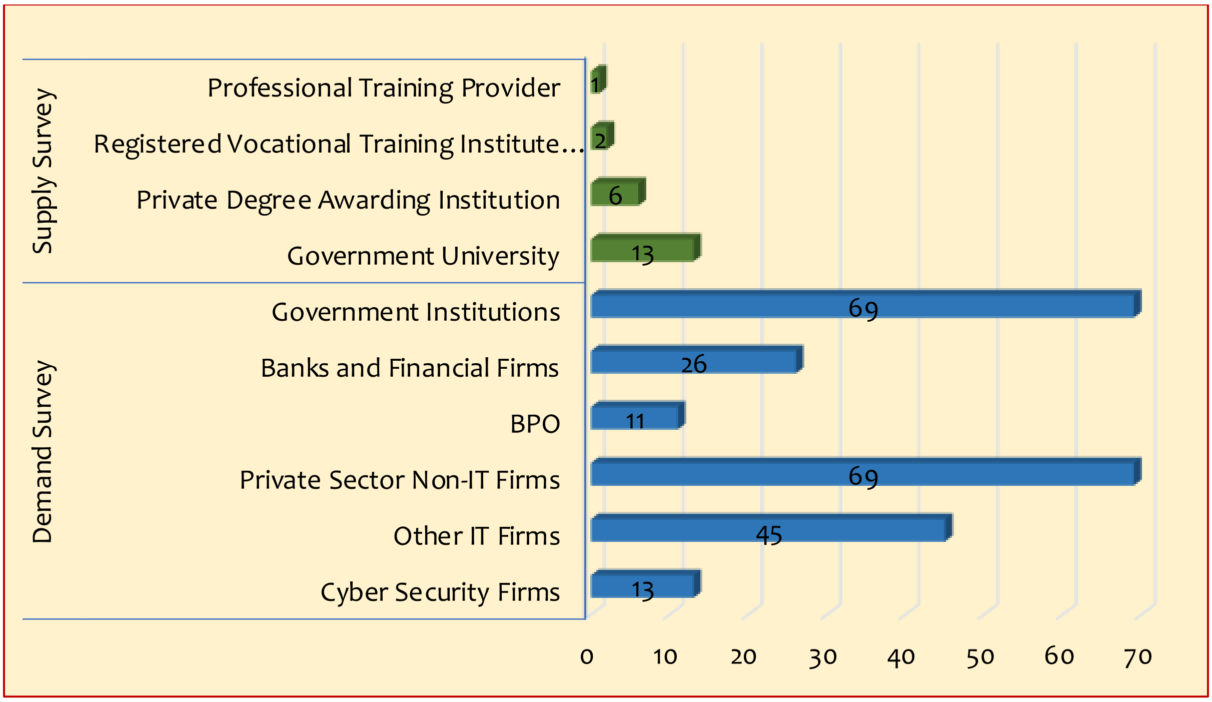


Figure 1: Number of Firms / Institutes Covered by Both Surveys

For primary data collection, this assessment was carried out using semi-structured questionnaires. Hence, two questionnaires were developed, one to capture data from the demand side, and one from the supply side. The questionnaires were pre-tested and revised to ensure the most efficient capture of data. Selected organizations and respondents in the selected organizations were made aware of the survey ahead of actual data collection. Data collection was carried out in two phases, first with the sharing of the questionnaire with the organization to be filled and returned within a given timeframe, and secondly through a validation meeting. All questionnaire data collection and validation were carried out online. A survey support hotline was established to assist all organizations in completing the questionnaire. To complement the findings of the survey, several interviews (Key Informant Interviews) were carried out with a number of key experts in the ICT industry.

1.6 Organization of the Report

The report begins with a global overview of the ICT cybersecurity workforce. It is followed by a review on Sri Lanka's cybersecurity sector and its workforce. A section that presents survey findings about extent, composition and quality of the workforce comes next. The next two sections present projections of demand for and supply of cybersecurity practitioners. The penultimate section analyses the gaps in demand and supply. This section also includes an analysis of the mismatch in demand and supply of skills. An overall conclusion about the findings of the survey is presented in the final section of the report.

Chapter 2: OVERVIEW OF GLOBAL CYBERSECURITY SECTORS

2.1. Global Cybersecurity Landscape

The Global Risks Report 2021 published by the World Economic Forum highlights the impact and domino effect that the COVID-19 pandemic has had globally, while identifying other high-likelihood, high-impact risks. The report states that among the highest likelihood risks of the next ten years are extreme weather, climate action failure and human-led environmental damage; as well as digital power concentration, digital inequality, and cybersecurity failure. The rapid digitalization of human interactions and the workplace over the past two years has forced governments, policy makers and employers to prioritize the safety and security of this alternate universe of virtuality. The global cybersecurity market size is projected to grow from USD 217.9 Billion in 2021 to USD 345.4 Billion by 2026, recording a Compound Annual Growth Rate (CAGR) of 9.7% from 2021 to 2026, according to market research reports.

Global cybercrime costs are expected to grow by 15% per year over the next five years, culminating in $10.5 trillion USD annually by 2025 (Cybersecurity Ventures), with the evolving cybercrime landscape, and despite the large workforce and skills gaps. The (ISC)2 Cybersecurity Workforce Study of 2020 revealed that the gap between desired positions and those employed in cybersecurity has narrowed from 4 million worldwide in 2019 to 3.1 million. The 2021 (ISC)2 Cybersecurity Workforce Study shows that for consecutive year, the Cybersecurity Workforce Gap has decreased, down to 2.72 million. Despite the cybersecurity workforce currently consisting of 4.19 million, the Cybersecurity Workforce needs to grow 65% to effectively defend organizations' critical assets.

Cybersecurity clusters have grown both organically and through intentional initiatives actions taken by local governments, with the largest single population of cybersecurity professionals found in the USA. However, there are substantial cybersecurity talent pools all over the world, with the Asia Pacific market expected to register its highest growth rate in the coming years. The Asia Pacific business process outsourcing market size expected to reach USD 85.80 billion by 2025. Factors such as high digital connectivity, low cybersecurity awareness, growing cross-border data transfers, and weak regulations will create a demand for cybersecurity solution. Currently the cybersecurity workforce gap is more than 2 million in the Asia-Pacific region.

2.2. Local Cybersecurity Landscape

Sri Lanka's cybersecurity market is still small but is projected to become a high-demand niche market to keep up with the IT and BPM industry as well as the rapid digitization of non-IT sectors. Much of the Cybersecurity workforce demand comes from the private sector through 600+ ICT companies and 80+ BPM companies in the country. With generated revenue of US$ 1.5 billion in 2019, the IT-BPM sector is Sri Lanka's 4th largest exporter, with a 29% Contribution to service exports. The attraction for IT-BPM investors in Sri Lanka lies in the Goldilocks situation created by high quality productivity and innovation available at a competitive price point.

Despite these opportunities to grow, there is a significant handicap in the industry in the form of weak cybersecurity and insufficient security regulations. Robust privacy and security laws regarding cybersecurity, and a qualified workforce need to be in place in Sri Lanka to earn the trust of international clients. Over the last two decades, Sri Lanka has enacted several laws and regulations to secure the cyber space and ensure the safety of data, communications and transactions that enter the digital dimension. Sri Lanka CERT was established by the ICT Agency of Sri Lanka (ICTA) in the year 2006, to address the increase of cybersecurity incidents in the country.

However, there is significant vacuum thus a need for improvement, which may be achieved by the Acts and regulatory measures that are in the pipeline to be finalized, including the latest proposals for a 'Cyber Defence Command Act' and the establishment of 'Sri Lanka Cyber Protection Agency'. The National Cybersecurity Index of 2021 has placed Sri Lanka in the 73rd position, having fulfilled 43% of the measures to honor Sri Lanka's commitment to cybersecurity at a global level. In 2020, the Cybersecurity Centre of Excellence (CSCx) was launched by SLASSCOM with hopes to further improve Sri Lanka's position as a hotspot for cybersecurity.

While the regulatory bodies are keeping up with the global shift in identifying the importance of efficient and thorough cybersecurity, there seems to be difficulties in enforcing these necessary frameworks and building blocks in the brick-and-mortar world. Currently only a small section of companies, such as banks, are legally liable for database breaches and hacks. Other sectors and companies are reluctant to allocate the high, but necessary financial expenditure to secure their digital presence as there is no legal obligation to do so. Another contributing factor may be the lack of understanding, or even responsibility, towards the customer and their privacy. Reflecting the global gap in the workforce, Sri Lanka also experiences a significant gap in qualified cybersecurity professionals. Analyzing the local market, predictions have been made that there will be demand for 10,000 cybersecurity professionals, over the next five years.

2.3 Employment in Cybersecurity Sector

Industries such as health care, finance, manufacturing and retail all hire cybersecurity professionals to protect valuable information from cyber breaches. Once a specialty only associated with government agencies and financial institutions, the cybersecurity sector has now entered the mainstream of information protection. The demand for specialists in the field is high and constantly increasing. Generally, it has found that job postings for openings in cybersecurity have grown three times faster than those for IT job overall, and cybersecurity professionals are earning 9% more than their IT counterparts.

Generally, the employments in cybersecurity sector are absolutely depended on the level of education and skills gained through the previous employments. The following table shows the globally accepted skills required to fulfill the cybersecurity employment needs at each educational category.

Table 3: Globally Accepted Skills for Cybersecurity and Educational Requirements

Level of Education	**Employment Needs**	**Skills Required**
Diploma/ Associate Degree in Cybersecurity	Introduction to Computer Forensics and Cyber Crime, Database Security, CompTIA Security+	Introduction to Computer Forensics and Cyber Crime - Processing crime scenes, Digital evidence controls, Recovering image files, E-mail investigations, Network forensics Database Security - Understand database security models, Advantages and disadvantages of access control models, Defending against common attacks, Knowledge of common integrity constraints CompTIA Security+ - Hardening systems, Securing networks, Cryptography
Bachelor's Degree in Cybersecurity	Fundamentals of Networking, Installing and Configuring Windows Server, Ethical Hacking	Fundamentals of Networking - Open system interconnection model, Security protocols, Networking protocols Installing and Configuring Windows Server - Configure server roles and features, Configure Hyper-V, Deploy and configure core network services, Install and administer Active Directory, Create and manage Group Policy Ethical Hacking - Safe techniques on World Wide Web, Hands-on techniques to defend a computer against security attacks, Hands-on techniques to defend a LAN against security attacks
Master's Degree in Cybersecurity	Penetration Testing and Vulnerability Analysis, Applied Cryptography, Digital Forensics	Penetration Testing and Vulnerability Analysis - Introduces methodologies, techniques and tools to analyze and identify vulnerabilities in stand-alone and networked applications. Applied Cryptography - Examines Modern Cryptography from both a theoretical and applied perspective; emphasis is on provable security and application case studies.

		Digital Forensics - Instruction in the application of forensic science principles and practices for collecting, preserving, analyzing and presenting digital evidence; covers topics from legal, forensic, and information-technology domains.
Professional Certification in Cybersecurity	Technology and National Security, Introduction to Penetration Testing, Cyber Risk Management for Decision Makers	Technology and National Security - Terrorism, National security policy, Intelligence gathering, Military platforms, Nuclear and biological weapon technologies Introduction to Penetration Testing - Assessment, Exploitation, Remediation techniques Cyber Risk Management for Decision Makers - Conducting assessments within multiple areas, Mitigation strategies, Standards, ethics, and legal issues

Many institutes offer professional certificates in cybersecurity for those professionals who want to develop further expertise in the field or add credentials to their career. Those professionals examine principles of computer systems security, including attack protection and prevention where accepted certificates explore the cryptographic techniques, legal issues in computer security, digital forensics and designs for network perimeter defenses etc.

Nonetheless, cybersecurity should be made a topic of the boardroom and given extra attention considering the growing threats during the COVID-19 pandemic. While going through the waves of the pandemic, every organization should implement preventive measures for cyber-attacks while strengthening cyber-attack detection, response and recovery capabilities. It is the responsibility of every individual and management to protect themselves and their workplaces from cybercrimes in today's connected world. At the same time, a collective approach is required at organizational, sectoral, national and international levels to fight against cybercrimes and build a safer world for the present and future generations. Based on these requirements, the Government of Sri Lanka (GOSL) proposed to establish cybersecurity units at every possible firm/ institution to minimize the phishing of emails, device sharing and free/cracked software, fake websites/apps and loss of information security focus etc. The Annual Report published by the Central Bank of Sri Lanka (CBSL) has recommended the following proposals to strengthen cybersecurity within the country while significantly expanding its employments immediately.

- Strengthen cyber resilience
- Business Continuity Planning (BCP) for pandemic-related circumstances
- Allocate adequate budget for cybersecurity
- Increase user awareness
- Working closely with National Computer Incident Response Teams (CIRT)

However, Banks and Financial Institutes in Sri Lanka have expected level of employees while other sectors have inadequate number of cybersecurity related staffs. Therefore, the instant strengthening of this sector should be implemented to minimize the cyber-criminal activities amidst during the past.

Totally 233 IT, Non-IT, BPO and Public Sector firms/ institutions were interviewed through the Demand Survey and it was observed that 20% of them (48 out of 233) do not have cybersecurity related staff. There are 926 cybersecurity staff members available in 186 firms/ institutions averaging 4 cybersecurity professionals per firm/ institute. However, cybersecurity firms have more than 20 cybersecurity professionals while other categories show respectively low average numbers. Moreover, 96% of Banks and Financial Institutes have cybersecurity professionals and other categories show relatively low percentage numbers. The following table illustrates the availability of cybersecurity professionals in each category interviewed through Demand Survey.

Table 4: Availability of CSPs as per Demand Survey

Type of the Institutes	Total Number of Firms/ Institutes	Cybersecurity Staff Available Firms/ Institutes	Total Number of Cybersecurity Staff (Part-time and Full-time)	% of Firms/ Institutes which have Cybersecurity Related Staff	Average Cybersecurity Staff per Firm/ Institute
Cybersecurity Firms	13	13	268	100%	21
Other IT Firms	45	36	156	80%	3
Private Sector Non-IT Firms	69	51	149	74%	2
BPO	11	8	45	73%	4
Banks and Financial Firms	26	25	158	96%	6
Government Institutions	69	53	151	77%	2
Total / Average	**233**	**186**	**927**	**80%**	**4**

Considering all 233 firms/ institutes interviewed 98% of cybersecurity practitioners are based locally and only 2% of them are based internationally. Further, half (about 50%) of cybersecurity related operations are handled internally in Sri Lanka and quarter (about 25%) of the employment opportunities are partially outsourced for locally existing firms. About 16% of employment opportunities are fully outsourced for local firms and only 7% have been partially outsourced for international firms. The rest 2% of the operations have been fully outsourced for international firms. The following graph shows the representation of local and international firms on cybersecurity handling operations.

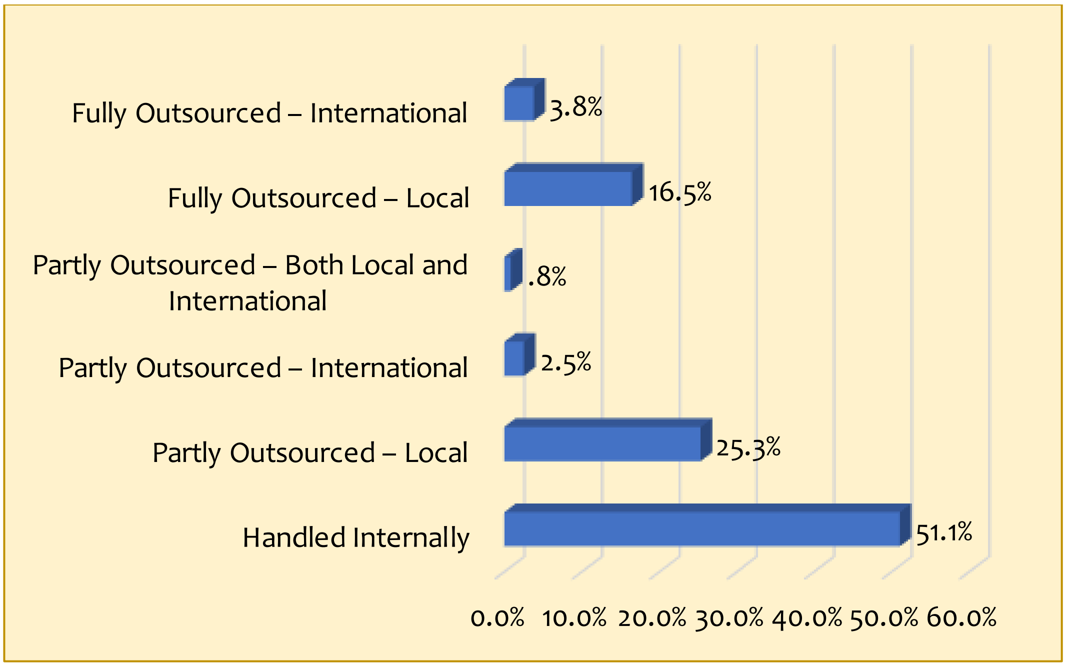


Figure 2: Handling CS Operations in Sri Lanka

As shown in the above graph, almost 50% of the firms have outsourced (partially or fully) their cybersecurity related operations. Some of the reasons stated by respondents for outsourcing the cybersecurity related operations are: they lack any internal full-time cybersecurity professionals/practitioners, they have outsourced for ease in management & consistent monitoring and that it is too expensive to have in-house cybersecurity professionals etc.

2.3.1. Full-time Professionals in Cybersecurity Sector

Out of cybersecurity professionals' available firms, only 58% of firms have full-time cybersecurity practitioners and 91% of them are based in Sri Lanka while the rest 9% are based outside Sri Lanka. The following table shows the availability (bas ed in Sri Lanka or outside Sri Lanka) of full-time cybersecurity practitioners. Furthermore, it has been found that, about 70% of full-time practitioners are based in Sri Lanka and rest 30% are based outside of Sri Lanka.

Table 5: Availability of Full-Time CSPs based in Sri Lanka and Abroad

Type of the Institutes	Number of Institutes have Cybersecurity Staff	Full-time Cybersecurity Practitioners			
		Based in Sri Lanka		Based Outside Sri Lanka	
		No. of Institutions	No. of Staff Members	No. of Institutions	No. of Staff Members
Cybersecurity Firms	13	11	130	4	127
Other IT Firms	36	27	106	2	12
Private Sector Non-IT Firms	51	27	51	1	38
BPO	8	8	33	1	12
Banks and Financial Firms	25	14	83	1	0
Government Institutions	53	10	30	1	0
Total / Average	**186**	**97**	**433**	**10**	**189**

2.3.2. Part-time Professionals in Cybersecurity Sector

Out of cybersecurity professionals' available firms, about 56% of firms engaged cybersecurity practitioners with part-time professionals. The following table shows the availability (based in Sri Lanka or Outside Sri Lanka) of part-time cybersecurity practitioners.

Table 6: Availability of Part-Time CSPs based in Sri Lanka and Abroad

Type of the Institutes	Number of Institutes have Cybersecurity Staff	Part-time Cybersecurity Practitioners			
		Based in Sri Lanka		Based Outside Sri Lanka	
		No. of Institutions	No. of Staff Members	No. of Institutions	No. of Staff Members
Cybersecurity Firms	13	3	7	1	2
Other IT Firms	36	13	29	1	1
Private Sector Non-IT Firms	51	28	57	-	-
BPO	8	-	-	-	-
Banks and Financial Firms	25	15	75	-	-
Government Institutions	53	44	121	-	-
Total/ Average	**186**	**103**	**289**	**2**	**3**

Subsequently, the COVID-19 pandemic has created new challenges for businesses as they adapt to an operating model in which working from home has become the 'new normal'. Companies are accelerating their digital transformation, and cybersecurity is now a major concern. The reputational, operational, legal and compliance implications could be considerable if cybersecurity risks are neglected. Therefore, with the implications immerged during work from home periods due to COVID-19 pandemic, the opportunities for part-time cybersecurity professionals in the country has been increased.

2.4. Cybersecurity Operations in COVID-19 Pandemic

The restrictions imposed by governments in response to the coronavirus pandemic have encouraged employees to work from home, and even 'stay at home'. As a consequence, technology has become even more important in both our working and personal lives. Despite this rise of technology need, it is noticeable that many organizations still do not provide a 'cyber-safe' remote-working environment. Where business meetings have traditionally been held in-person, most now take place virtually. The increase in remote working calls for a greater focus on cybersecurity, because of the greater exposure to cyber risk. The COVID-19 pandemic and increase in working from home were seen as a major cause of this increase, since individuals working at home do not enjoy the same level of inherent protection/deterrent measures from a working environment (e.g., internet security). Prior to the pandemic, about 20% of cyberattacks used previously unseen malware or methods. During the pandemic, the proportion has risen to 35%. Therefore, the widening of local level cybersecurity operations (full-time or part-time) for a better working environment in future is a must.

2.5. Emerging Technologies Influencing Cybersecurity Sector

Three prominent technologies are emerging due to the digital transformation that continues to highly affect required cybersecurity solutions.

2.5.1. Artificial Intelligence (AI) and Machine Learning

Artificial Intelligence (AI) and Machine Learning will increasingly and continuously influence the evolution of cybersecurity.

Security will invariably evolve in an ever-changing cyber environment. Instead of obeying a specific design, security should become more organic and autonomous, much like our immune system. Ongoing training and adaptation will enable systems to recognize and respond to new threats.

Cyberattack detection becomes more widespread, so IoT ecosystems will rely on AI and machine learning's line of defense to assess data reliability. The algorithms for processing data from the network sensors will not implicitly trust a single sensor node. Instead, they will seek consensus from surrounding nodes. Machine learning algorithms can continue to evolve to improve spam and malware detection, making it possible to identify fraudulent transactions quickly.

2.5.2. Predictive Defense

As the attacks are becoming more sophisticated, cybercriminals are also starting to concentrate on large organizations, states, and companies. The defenses must therefore try to evolve on a more advanced level.

Predictive defense and control need to be constant. Because, even if we can't achieve zero-risk security, detecting an attack and intervening in the shortest possible time often makes all the difference. The most crucial weapon lies in "preventive" cybersecurity, which will become "predictive" through its evolution. Defense systems will be able to analyze signals that anticipate an attack. The challenge is indeed complicated and will play out in a fight where artificial intelligence will play a key role. However, we must not forget that the original idea (both the attack and the protection system) will remain human.

2.5.3. Hybrid Cloud

The emergence of new hybrid cloud environments invites a new approach to cyber defense, involving machine learning and autonomous systems in the service of cybersecurity. Organizations tend to move away from traditional security strategies and turn to intelligent SOCs capable of automatically predicting, detecting, avoiding, and responding to threats. For example, many companies are adopting new cloud environments and switching their applications to SaaS solutions to gain agility, scalability, and operational ease. Thus, new hybrid cloud environments are gradually emerging within the informational system. The abundance of these unique environments encourages us to think about a new approach to cyber defense. Forward-looking organizations are moving away from traditional security strategies and turning to innovative SOCs. These security operations centers aim to automatically predict, detect, avoid and respond to threats automatically. SOCs must also correlate vast amounts of data and extract actionable insights.

2.6. Developing a Trustworthy Society

These emerging technologies stemmed from different societal scenarios highlighting the significant factors of cybersecurity evolution. They also show the importance of interactions between multiple data security elements.

Technology in itself will not be the only answer. It must be integrated into more comprehensive defensive approach strategies. Above all, change can only materialize if, at the same time, a society of trust develops in the communities. If consumers feel that a hyper connected community cannot ensure data protection, technological disruptions will be wiped out.

2.7. Takeaway

To protect individual, private, corporate, and government information systems and prevent increasingly sophisticated threats from penetrating, organizations should opt for flexible, intelligent cybersecurity technologies. Artificial intelligence (AI), machine learning algorithms, predictive defense, and hybrid cloud deployments are just a few of the industry's emerging technologies. Furthermore, security operations centers (SOCs) must also increase current proactive security strategies to address pressing protection issues. These security measures should accelerate the future of advanced cybersecurity protocols for all users.

Chapter 3: AN OVERVIEW OF THE CYBERSECURITY WORKFORCE IN SRI LANKA

3.1. Cybersecurity Sector's Contribution to National Economy

The IT-BPM sector is Sri Lanka's fourth largest exporter, generating revenues of over $345 billion USD in 2019 with a 29% contribution to service exports. These numbers are projected to increase rapidly, with the IT-BPM industry envisioning a $1 billion USD revenue by 2025. The potential of the IT-BPM industry has motivated the government to invest 300 million LKR into the "Island of Ingenuity" (IOI) brand, positioning Sri Lanka as a reliable, creative and innovative provider of niche software products and IT-BPM services. The increased presence of large international tech companies speaks to the success of the IT-BPM industry, with the USA, UK, Australia, Norway and Sweden outsourcing ICT services in Sri Lanka.

Due to the lifestyle changes that have occurred from COVID-19, the traditional goods and services related to Information Technology have evolved, with rapidly increasing demands for cybersecurity in the IT-BPM industry. These changing circumstances are creating a wide variety of new markets and economic opportunities in Sri Lanka. With mobility restrictions forcing people to work from home, there was an increase in the need for securing devices to meet the safety criteria of industry needs outside of office networks. This transition made it crucial to strengthen existing cybersecurity infrastructure in order to safeguard important, confidential information. Online learning expanded student's online presence and furthered the need for restrictions and safety in these new educational spaces. E-commerce and online banking were rapidly adopted, developing the need to enhance the systems of online platforms and protect online transactions. As the nature of cybersecurity has changed during this crisis, export revenue from cybersecurity in Sri Lanka alone has the potential to reach a revenue of $500 million USD and create 10,000 new jobs by 2025.

3.2. Key Players Involved in Cybersecurity Workforce

When scoping the cybersecurity landscape in Sri Lanka, there were several different key players identified in different sectors of the country. There is a strong distinction in the Private vs. Public dichotomy of cybersecurity as well as different sectors within the Private domain.

One of the key concerns that had emerged with the Key Informant Interviews (KIIs) that were conducted was that there is a lack of collaborative effort between different stakeholders in Sri Lanka to come together to address cybersecurity concerns. Mr. Sujith Christy, Governance, Risk and Compliance Professional, had stated that "different institutions, different bodies, in Sri Lanka are trying to do the same thing" and that it is crucial that we not only say that we need to build the capacity of cybersecurity - but efficiently and collaboratively working together to ensure that this is the case.

3.3. Suppliers of Cybersecurity Products

Vendors in cybersecurity typically offer different products and security tools / systems for specialized attacks as well as improving general security. Most of the well-known cybersecurity vendors are international brands that provide standardized and innovative solutions to real-life cybersecurity threats and issues. The security systems and tools offered by these vendors includes:

- Identity and Access Management (IAM)
- Anti-malware
- Data Loss Prevention (DLP)
- Endpoint Protection
- Firewalls
- Encryption Tools
- Security Information and Event Management (SIEM)
- Vulnerability Scanners
- Intrusion Prevention / Detection Systems (IPS/IDS)
- Cloud Access Security Broker (CASB)
- Cloud Workload Protection Platform (CWPP)
- Virtual Private Networks (VPNs)

The role of the Private sector in Sri Lanka is to invest money strategically to also ensure that their own staff are trained adequately to the skill-specific tasks assigned to them and the organization.

3.4. Cybersecurity Enabled Services

Cybersecurity entails a wide variety of services of different magnitudes. This includes but is not limited to Network Security, Information or Data Security, Application Security, Cloud Security, Critical Infrastructure Security, End-user Education and Physical Security. As cybersecurity is constantly evolving, the threats and systems in place are also subject to rapid change and therefore continuous monitoring and risk assessment is crucial to defend against unknown and known threats in a swift and efficient manner. As there are also fast transformations in new technologies, the process of keeping up to date with security trends and threat intelligence is challenging as well.

The main types of cyber threats commonly faced are:

- Malware e.g. worms, viruses, Trojans and spyware

- Ransomware
- Social engineering
- Phishing e.g. fraudulent emails or text messages to steal sensitive data
- Spear phishing
- Insider threats
- Distributed denial-of-service (DDoS) attacks
- Advanced persistent threats (APTs)
- Man-in-the-middle (MitM) attacks

3.5.Uses of Cybersecurity in Public and Private Sectors

Much of the Cybersecurity workforce demand comes from the Private Sector through 600+ ICT companies and 80+ BPM companies in the country. Threats to the cybersecurity of the Private Sector include the loss of intellectual property, cybercrime, unauthorized access of confidential business and stock information, recovery from previous cyberattacks, and reputational damage.

As the Public Sector includes many vital services related to the government, society and economy, it is especially important to have a strong cybersecurity infrastructure that protects from attacks. The most common cybersecurity threats faced by the Public Sector have to do with phishing, ransomware, malware, data protection, cryptomining, cyber espionage and software supply chain attacks.

In Sri Lanka, the growing digitization as a result of COVID means that there is a greater need for cybersecurity infrastructure in both the Public and Private Sectors. When lockdown required professionals to work from home and connect to internal networks from outside of the organization, many Public and Private institutions had to quickly create make-shift arrangements to make these systems accessible while ensuring adequate security. Within this climate, many IT professionals in Sri Lanka are calling for greater investments in cybersecurity infrastructure to combat the various threats.

3.6. Suppliers of Cybersecurity Workforce

In Sri Lanka, educational and/or training institutions can be categorized as the following: Government Universities, Professional Chapters / Bodies, Private Degree Awarding Institutions, Registered Vocational Training Institutes (Registered under TVEC), Professional Training Provider and Government Tertiary & Vocational Training Institute (e.g. NAITA, VTA). When scoping the landscape of institutions that offer cybersecurity related courses, the main two categories responsible are Government Universities and Private Institutions. Within the main Government Universities in Sri Lanka, there are also several different faculties that can offer varying levels of cybersecurity or similar related courses. For example, Faculty of Technology, Faculty of Engineering and Faculty of Science of specific Government Universities have indicated that there are cybersecurity related courses available.

Although these cover the overview in Sri Lanka, there is a huge proportion of Sri Lankan nationals that migrate abroad for educational purposes to obtain relevant cybersecurity related qualifications. This includes but is not limited to specialized Undergraduate and Graduate programs as well as professional qualifications such as trade certificates or trade vendor certificates. Moreover, it is also common in Sri Lanka for individuals to begin as IT professionals in an organization and then advance specifically towards cybersecurity through company provided trainings and sponsorships for further studies in the discipline. Certain organizations also provide in-depth and product-specific training opportunities to enhance their cybersecurity expertise.

Chapter 4: QUALITY OF CYBERSECURITY WORKFORCE

4.1. Strength of the Cybersecurity Workforce

When consider the global ICT industry, the telecom services (26%) have been given the biggest contribution while hardware development (23% - devices and infrastructure) has placed at second. The IT business services have contributed almost 20% to the global industry and 46% of new revenue growth in ICT industry has attributed to emerging-tech categories during 2018-2023. The IoT Software, IoT Hardware, Saas + Paas, IoT Connectivity, Robotics/ drones, AR/VR, AI platforms/ applications, big data/analytics, Enterprise Social Software and Next Gen Security etc. are key emerging tech growth drivers where Cybersecurity Operation needs to be applied for all sectors to protect data use in cyber. Therefore, the strengthen of the cybersecurity workforce in future is a must. Globally, the talent recruitment and retention are major challenges for IT leaders where 50% are currently struggling in the area. Only seven percent of IT decision-makers say that hiring has been easy. Also, a lack of budget and resources is another major concern for both IT staff and decision-makers.

Some IT decision-makers do not authorize training even when it's built into their budget and nearly 40% had formal training available but decided to forgo it. Nearly 20% of IT professionals say management does not see a tangible benefit from training. That's a huge disconnect, especially since IT professionals have a strong desire to learn and grow their careers. It's difficult to accomplish that without support from leadership. According to IT decision-makers, skills gaps will cost employers up to 416 hours and over $5,000 per employee, per year. Less than 60% of decision makers say their organizations offer formal training for technical employees, down one percent from the previous year. This tells that organizations aren't serious enough about skill development. However, the COVID– 19 situation globally has positively impacted the Global ICT Industry, even though businesses are grappling with current losses, in the long run, the ICT industry might be one of the few still standing and, in many aspects, stronger than before. Therefore, ICT experts expect that workforce in cyber security will also be demanded and stronger than before.

According to the University Grant Commission (UGC) of Sri Lanka, in 2020 totally 4637 ICT sector skilled students have been completed their academic qualifications from both public (1210 students) and private (3427 students) universities. Gender disaggregated data shows 60% of the qualified students are male and rest are female. The yearly growth of supply from 2018 to 2019 is notable but the projection towards an exponential increase of demand in 2020 data displays a large drop, due to the COVID-19 outbreak. It is expected to stabilize with new policy direction to increase enrolment.

Sri Lanka has advanced in the National Cyber Security Index (NCSI) from 98th place in 2020 to 69th place in 2021. According to the index, education and professional development sub-category got highest rank with 100% achievement compared to the last years.

Furthermore, it clearly shows a significant improvement in 'cybersecurity professional association' at locally. These are the remarkable signs for continuous strengthening of the cybersecurity workforce with in the country. Moreover, Sri Lanka is currently in the process of implementing the Nation's first Information and Cyber Security Strategy (2019-2023) and it is expected to elevate the country's position not only in NCSI but also in all the other global indexes. Therefore, both Public and Private sectors should move towards the development of regulations to secure their information while strengthening the cyber security related competences of their institutes/ organizations.

4.2. Strength of the Workforce by Major Employer Categories

According to the survey findings, there were 39 different designated positions who are engaged with cybersecurity operations and only 12% of them are only specialized for cybersecurity. Others are handling multiple tasks and their primary responsibilities are different areas in ICT sector. According to the NCSI, country's performances in capacity building given for cybersecurity related staff are at mature level. It basically measures the existence of research and development, education and training programs, certified professionals and public sector agencies fostering capacity building. Following are the identified designations of workforce who are handling cyber security incidences in public and private sectors.

Table 7: Designations of Workforce Handling Cyber Security Incidences

Major Employer Category	**Existing Designations**
Consultant	Cyber Security Consultant, Management Consultant, Information System Consultant, Cloud Security Consultant and ICT Consultant etc.
Top Management	Head of Cyber Security, Senior Lead-TechOps Engineer, Senior Lead-DevOps Engineer, Security Operations Lead, Application Security Tech Lead, Technical Lead, Team Lead, Head of IT, Head of Digital Infrastructure, Chief Information Security Officer, Chief Technology Officer and Head of Security of Assurance etc.
Senior Manager Level	Director Cyber Security, Director IT, Senior Manager Network and Security, Senior Database Administrator, Senior IT Administrator, Senior System Engineer, Senior System Analyst, Senior Software Engineer, Senior Information Security Engineer, Assistant Director IT, General Manager of Cyber Security, Senior DevOps Engineer, Senior Manager Information Systems and Assistant General Manager ICT etc.

Major Employer Category	**Existing Designations**
Manager Level	Cybersecurity Manager, Network Security Manager, Technical Manager, Project Manager, Engineering Manager, Manager Information Security, Technical Manager – ICT Infrastructure, Manager – Information Security Governance, Compliance Manager and IT Manager etc.
Specialist/ Assistant Manager Level	Cyber security engineer, DevOps Engineer, Information Security Engineer, Deputy Manager IT, Deputy Manager System Security, IT Specialist, Network Administrator, Cloud Specialist, System Administrator, Assistance manager ICT, Database Security Engineer, Software Engineer, Software Architect, Assistant Manager- Security and Networking, Assistant Manager Telecommunication, Assistant Manager IT Services, Assistant Manager Infrastructure Services.
Officer Level	IT Officer, IT Executive, Information Security Officer, ICT Officer, Management Service Officer, Telecommunication Technical Officer, Analyst and Development Officer-IT etc.
Assistant Level	IT Assistant, ICT Assistant, Network Support Associate, Associate developer, Management Assistant and Assistant IT Executive etc.
Trainee/ Intern	Interns and Trainees

The study found that most of cybersecurity practitioners are at Junior Manager Level and only 30% of the total workforce serve for above manager level positions.

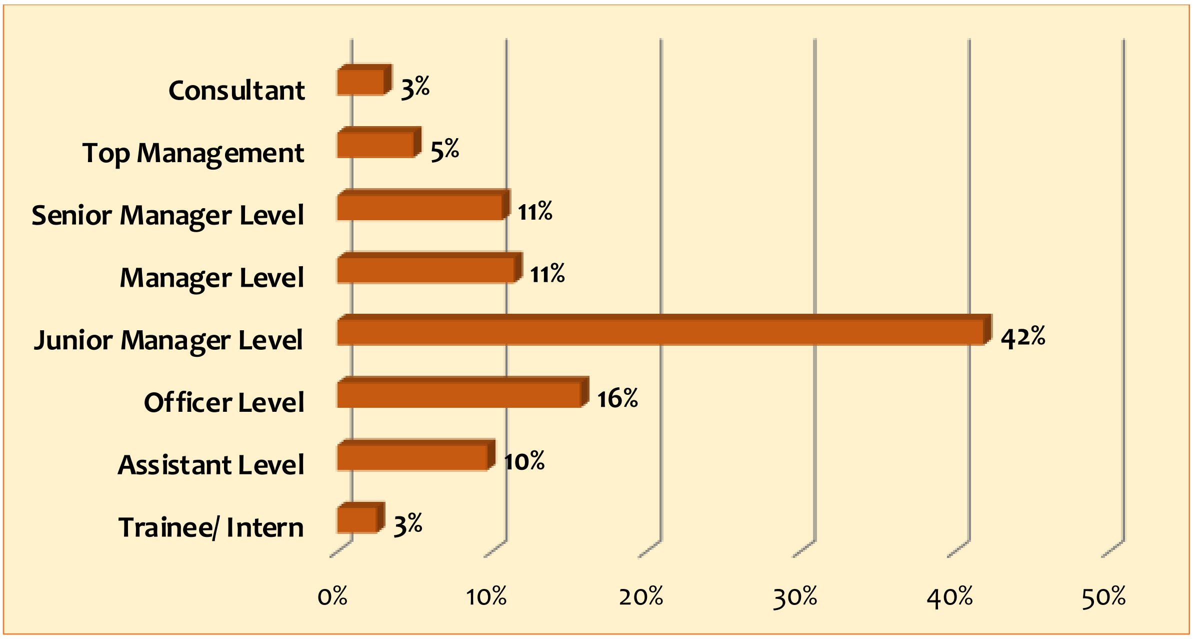


Figure 3: CSPs by Major Employment Category

Gender disaggregate data shows that 10% of the employees are female at 2020 and the demand for female practitioners in 2021 has declined to 9%. Compared to the base employment figures of the sample in 2020, there is a 10% overestimated demand for 2022 (45%) in relation to the 2021 demand (35%). By comparison the number of IT jobs in general has grown about 30% in Sri Lanka. The number of cybersecurity job postings has grown 45% in just two years. That's a 122% increase in demand compared to the overall IT job market.

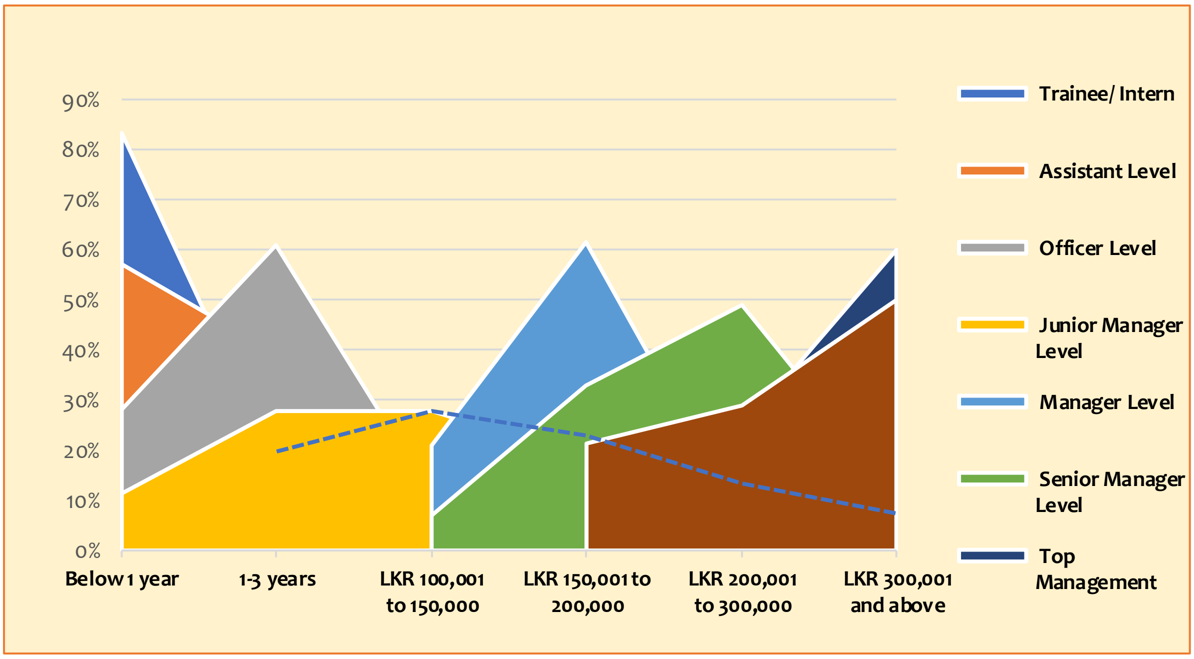


Figure 4: Gross Amount (LKR) Paid as Salaries (LKR) for Major Employment Categories

When it comes to cybersecurity, there is no substitute for a dedicated, immensely talented workforce. Companies need to have infiltration systems set up, as well as recovery systems in the event of a virus or other type of infiltration. Graduates can also parlay their work as cyber defenders in many different manners to build a secured nation.

4.3. Quality of the Cybersecurity Workforce: Educational Qualifications

The young IT professionals in Sri Lanka are generally motivated to study Computer Science and Information Systems with the goal of becoming software engineers. Many students have not expressed clear interest in cybersecurity, although it may be a requirement of their employment at certain organizations, mainly because they are drawn to certain organizations or to specializations with more attractive salary options. The educational system has not created a culture of cybersecurity, but rather, has focused on building opportunities within other areas of technical computer science and information system expertise.

Whilst it's possible to find certain entry-level cyber security positions with an associate's degree, most jobs require a four-year bachelor's degree in cyber security or a related field such as information technology or computer science. Coursework in programming and mathematics/ statistics combined with classes in ethics and computer forensics prepare students with the technical and analytical skills required for successful careers in cyber security. Following chart shows the academic qualifications of each major employer categories. Not only academic qualifications but professional qualifications are vital for success in cybersecurity careers. When conducting KIIs, a key expert in the cybersecurity field added, 'we believe accredited cyber security certification is extremely valuable for practitioners to enhance their expertise and for employers to have confidence in the staff they hire'.

Qualitative data collection of this study found that the benefits of professional certifications are multi-faceted, particularly in the cybersecurity space, where demand for verified skills and capabilities are in such high demand, and where capability needs more than just work experience and able to address the latest technologies, threats and challenges. However, key experts in the sector stated a professional certification requires a number of specific attributes in order to meet the minimum criteria to attain certification. This should include the demonstrating a minimum number of years paid work experience in the field the employees are pursuing a certification in, adhering to a code of ethics, along with having a sponsor to vouch for their character, capability and career experience.

The demand survey was found that junior manager level positions (about 42%) are practiced more on cybersecurity related operations and more than 70% of them have bachelor degree qualifications or above. The following chart illustrates the composition of educational qualifications in the existing career market.

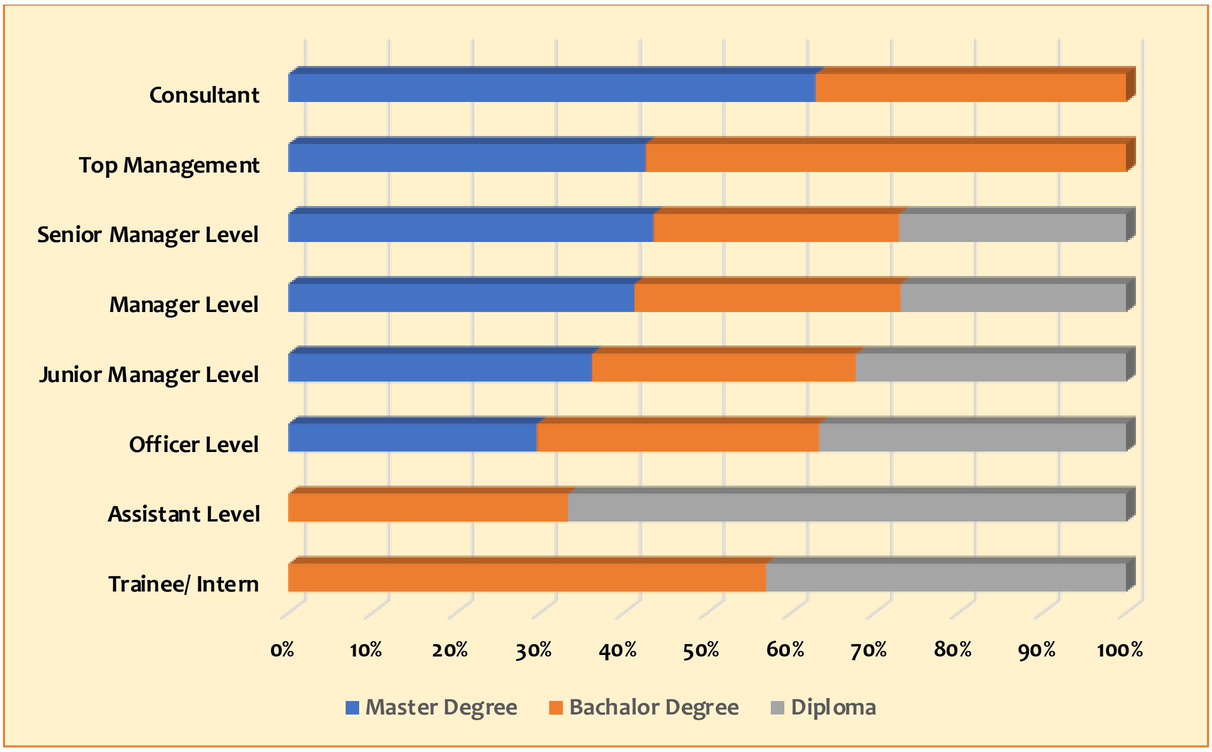


Figure 5: Qualifications of Major Employer Categories

According to the national level initiatives taken by the responsible authorities (SLCERT/ ICTA), they are in a process to develop national information and cybersecurity competency framework which outlines the core competencies that both the government and private sector should possess to effectively work in the cyber environment. In developing the framework, cadre structure of the public service and private sector would be taken in to account. They also work with tertiary and vocational education commission to develop National Vocational Qualification (NVQ) standards for various disciplines in the information and cybersecurity domain. The proposed national information and cybersecurity competency framework shall comply with the NVQ standards and professional qualification standards as defined by international standardization bodies.

SLCERT and ICTA believe the continuous capacity building in cybersecurity industry is greatly important while employers should motivate their employees to complete professional certifications which are align to international standards. As per information and cybersecurity competency framework, they expect to roll out information and cybersecurity training programs for staff at grassroot level in the public service across the country. Similarly, they have planned to offer scholarships for public sector staff to undertake specialized postgraduate degrees and to professional courses in the domain. Furthermore, they recognize continuous participation and contribution to international conferences on Information Security which is essential to state country's position and deepen communication with various actors around the global.

Following chart shows the demand for the completion of professional certificates by major employment categories during 2021/2022.

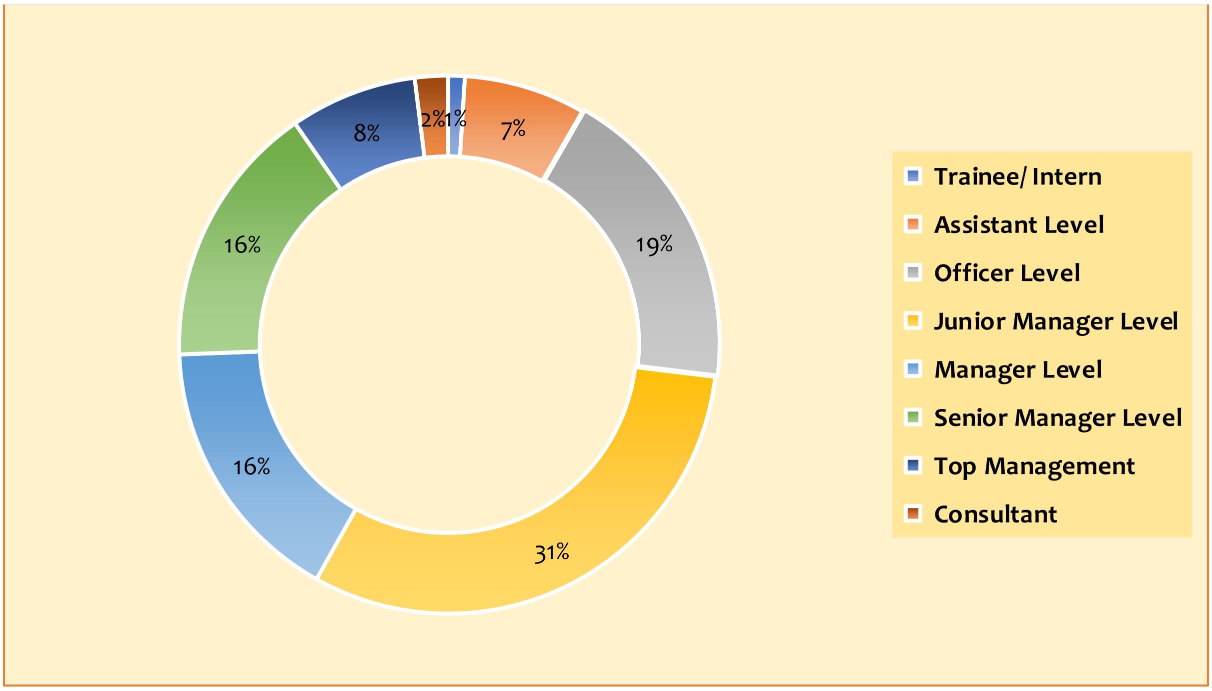


Figure 6: CSPs who are looking for Professional Qualifications (2021/2022)

ICT experts expressed that Vender Certificates and Vender Neutral Certificates related to Cybersecurity will be highly advantageous for practitioners. Further analysis of the qualitative data discovered, there is the requirement to maintain the certification for career advancement. This means completing a minimum number of Continuing Professional Education (CPE) credits to demonstrate that the employees are invested in keeping up-to-date with the latest developments in cybersecurity. Continuous education is critical as cybersecurity is changing by the hour, so there is little value in any certification that doesn’t have a requirement for continuing learning beyond an exam pass. It ensures that practitioners stay sharp, informed and relevant.

4.4. Quality of the Cybersecurity Workforce: Experience by Gender

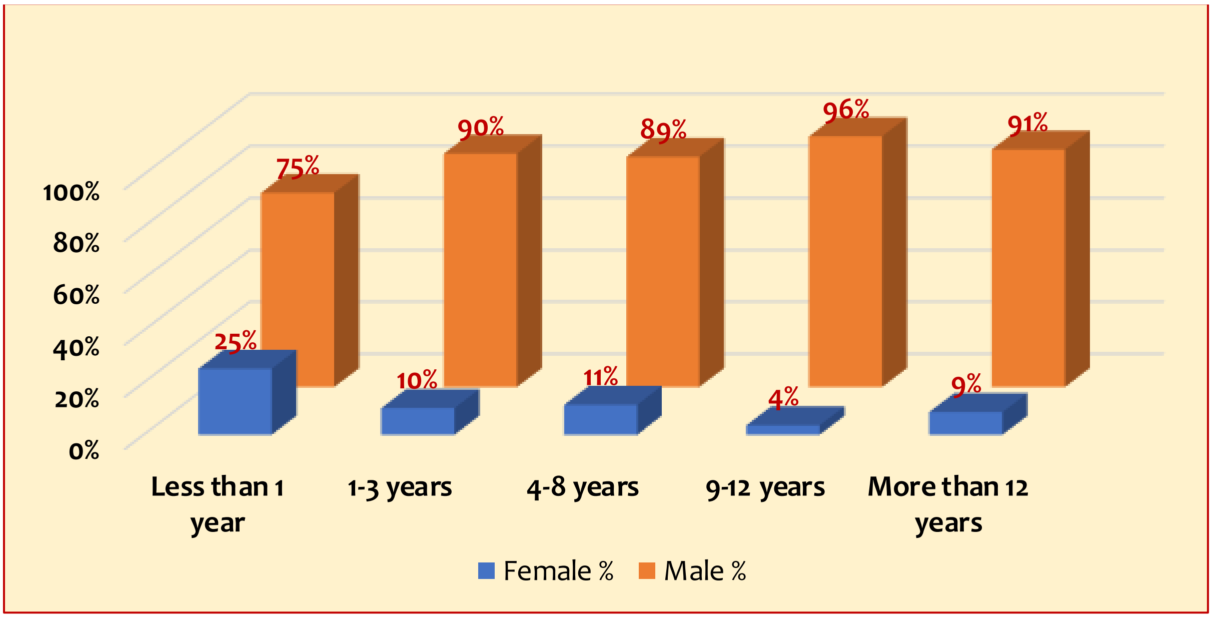


Figure 7: Cybersecurity Practitioners' Years of Experience by Gender

According to the graph above, almost 90% of experienced practitioners in the industry are male in each experience category. The following table illustrates the expected level of experiences (by percentages) for demanded opportunities of each major category by employers in the industry.

Table 8: Level of Experience by Major Employment Category

Major Employment Category	Level of Experience Expected for Demand Jobs by Employers				
	Below 1 year	1-3 years	3-5 years	5-8 years	More than 8 years
Trainee/ Intern	83%	17%	-	-	-
Assistant Level	57%	39%	4%	-	-
Officer Level	28%	61%	11%	-	-
Junior Manager Level	11%	28%	28%	33%	
Manager Level	-	-	21%	73%	6%
Senior Manager Level	-	-	7%	33%	60%
Top Management	-	-	-	16%	84%
Consultant	-	-	-	21%	79%

Despite the high levels of people with paper qualifications, the skills and capacities of these professionals are not up to industry standards. Many experts have suggested that it is better to have fewer institutions with quality education in order to produce better graduates. In addition to developing the educational infrastructure around cybersecurity, it is crucial to recruit students to the field who are motivated by a tangible interest and passion in the subject rather than just by salary considerations.

The development of a skilled and competent workforce to detect, defend and respond to cyber-attacks is a key strategic thrust area under the mission of SLCERT. They believe that the development of public-private, local-international partnerships to create a robust cybersecurity employment pool in the future.

4.5. Quality of the Cybersecurity Workforce: Skills in Emerging Technologies

There is a discrepancy between the current climate of the cybersecurity industry and the skillsets of young professionals in Sri Lanka. Especially with the increasing use of technology due to COVID-19, the entire cybersecurity architecture has to change to effectively address evolving needs.

Higher global demand has motivated many young cybersecurity professionals to migrate to other countries, where the salaries are higher and the employment opportunities are greater. Thus, to adequately utilize the skill sets of this talent pool, Sri Lanka needs to increase investments in local markets and to provide more product-specific skills and financial incentives for young professionals to pursue cybersecurity as a career path.

Chapter 5: DEMAND FOR CYBERSECURITY WORKFORCE

5.1. Total Demand for Cybersecurity Professionals

Worldwide, cybersecurity professionals are in demand. According to a global employment statistic, there are some 3.1 million unfilled positions worldwide. Cybersecurity jobs take an average of 20% longer to fill than other IT jobs and they also pay 16% more on average.

In global context of cybersecurity, "entry-level" can be a bit of a misnomer. For some roles, the global employment indices define entry-level as requiring a bachelor's degree plus up to three years of relevant experience also less with higher-level degrees. There are four entry level occupations have been identified in global context and they are IT auditor, Information Security Analyst, Security Specialist and Digital Forensic Investigator. The specified main duties performed by the entry level professionals are recovering data from erased or damaged hard drives, testing and maintaining firewalls and antivirus software, implementing security training, planning and performing audits, providing guidance on recommended and mandatory security measures, researching new security risks, monitoring networks for security breaches, helping computer users with security products and procedures, and Developing strategies to help their organization remain secure etc. However, with gained experience in cybersecurity, several paths could open up for advancement into more specialized roles for mid-level and advanced cybersecurity professionals which have higher demand and employment benefits.

Cybersecurity professionals in Sri Lanka are providing solutions tailored to assist organizations achieve an increased level of security and resilience for country's leading banking and finance institutes, telecommunication service providers, healthcare service providers, software development companies and multinational conglomerates. However, entry level opportunities in Sri Lanka are Security Architecture Associate, Security Analyst, and Cyber Security Engineer etc. At entry level, a cybersecurity engineer can earn a monthly salary of LKR 120,000 in Sri Lanka and it is a significantly lower amount compared with the IT giants emerging countries. Generally, for any entry level cybersecurity professionals of those countries can earn a monthly salary of LKR 1 million or more.

This study collected the demand data for cybersecurity professionals from sampled organizations such as Cybersecurity Firms, Other IT Firms, Private Sector Non-IT Firms, BPOs, Banks and Financial Firms, and Government Institutions. The following table shows the actual data for 2020 and expected demand for 2021 and 2022.

Table 9: Existing Workforce and Demand for 2021-2022

Year	Male	Female	Total
Base employment at the beginning of 2020	563	67	630
Demand for 2020	341	-	341
Joined During 2020	63	6	69
Left During 2020	29	-	29
Demand for 2021	365	-	365
Demand for 2022	427	-	427

Globally, the workforce shortage and gender disparity in cybersecurity professions pose a greater risk to the digital economies from cyber adversaries. The global efforts and initiatives for women to pursue career in cybersecurity field tend to be lesser than men along with various societal barriers. Under Sustainable Development Goals 17 (Women's equality and empowerment), developed nations have taken initiatives to collaborate and complement efforts to address gender disparity in cybersecurity profession as they have equally shared the cyberspace.

5.2. Skills in Demand

Cybersecurity is an in-demand, fast-growing field with a need for qualified employees, offering high median salaries, job opportunities in a variety of sectors, and a challenging, fast-paced work environment. Hence this emerging field requires having a broad set of technical, professional, and functional skills, as well as the specific cybersecurity skills and key soft skills in demand by employers. Considering the solid foundation in the principles of new cybersecurity opportunities, it is needed to have an overview of security across a variety of platforms, programming and development, digital forensic investigation, specific technical skills and more. The skills like problem solving skills, technical aptitude, knowledge of security across various platforms, attention to detail, communication skills, and fundamental computer forensics skills and, an understanding of hacking are globally demanded common skills in cybersecurity employment flatform. There are some technical skills required at entry level for beginners such as coding, networking, security incident handling & response, applications and systems, analytics & intelligence, data management protection and employer specific soft Skills. This survey measured both technical and soft skills that are requested by employers. According to the findings, the technical skills like incident handling & response, information security audit & compliance, cybersecurity analytics & intelligence and firewall/IDS/IPS skills were top prioritized. Moreover, the soft skills like leadership skills, passion for learning determined, and collaborative and teamwork were highly mentioned by the respondents. The prioritization of both technical and soft skills was measured at three levels and the following descriptions with graphs are illustrated the finding of the survey.

5.2.1. Technical Skills in Demand

The following graph illustrates the locally requested technical skills by the respondents. At level 1, the incident handling & response skill, security information and event management, and cyber–security analytics & intelligence skills were top prioritized. At level 2, information security audit & compliance skill and firewall/IDS/IPS skills were added into the prioritized list. At 3rd level, the skills such as data management protection, network-based threat and vulnerability assessments, and risk analysis and mitigation were added.

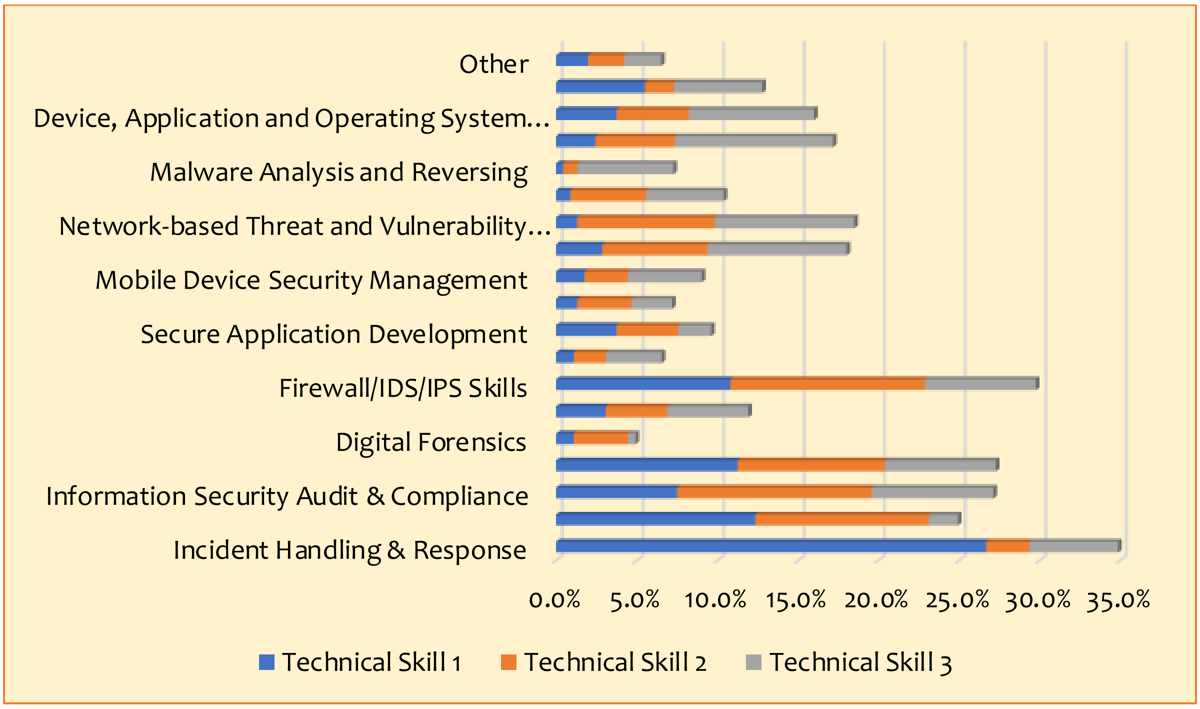


Figure 8: Demand of Technical Skills for CSPs

5.2.2. Soft Skills in Demand

In relation to the soft skills, the leadership, passion for learning, determined, collaborative and teamwork, strong analytical and problem-solving skills, and flexibility and adaptability in the face of changing priorities skills were prioritized.

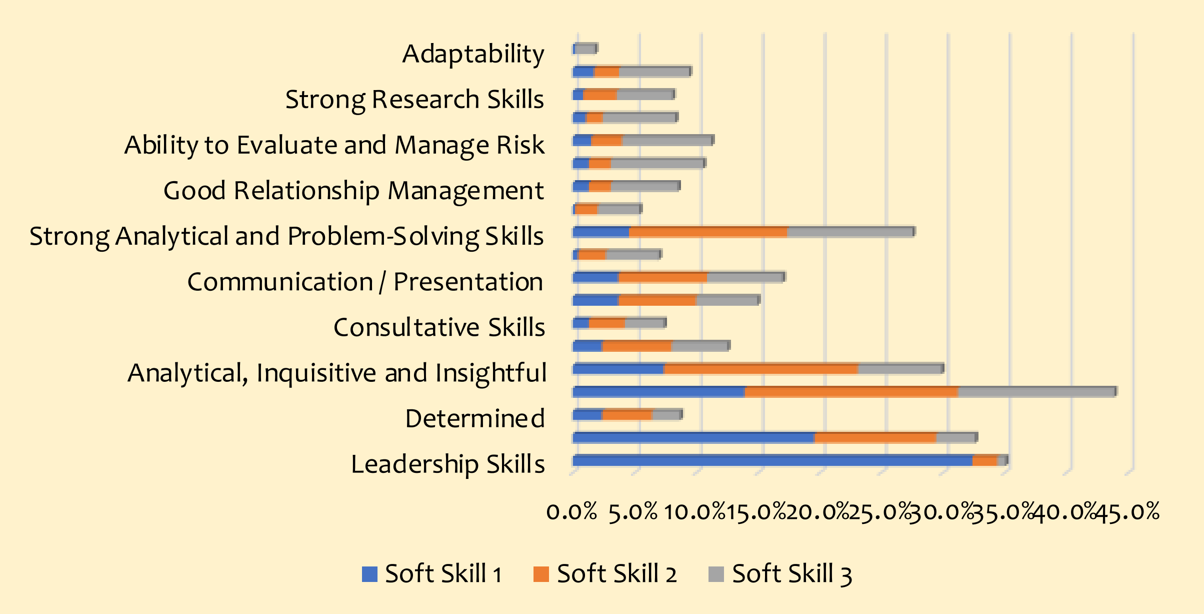


Figure 9: Demand of Soft Skills for Cybersecurity Professionals

5.3. Preferred Means of Skills Development for Career Advancement

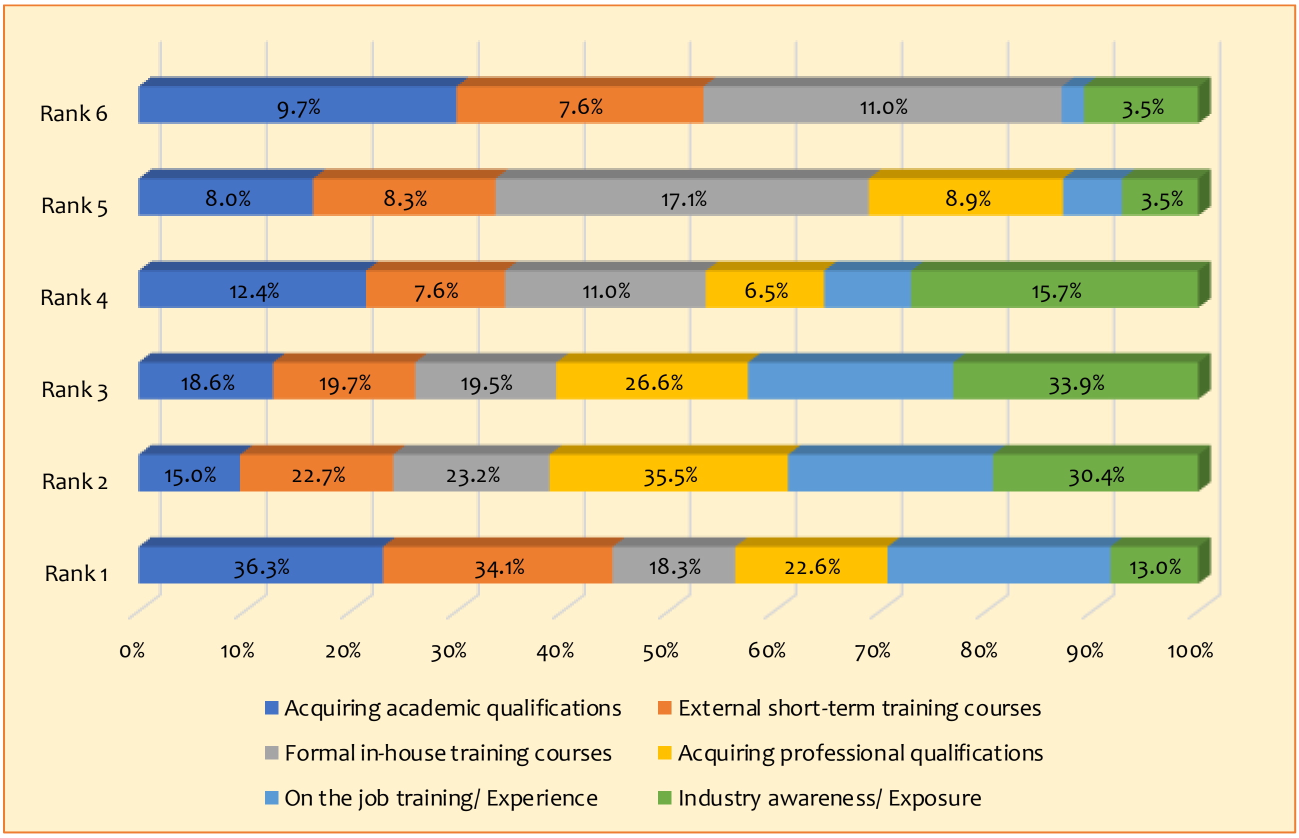


Figure 10: Ranking of Preferred Skills for Career Advancement

The demand survey was asked to rank 06 pre-selected means for skills development from respondents and the above chart shows the percentage values given for preferred means at each rank. 'Acquiring academic qualifications' has taken higher responses at rank 1 followed by 'external short-term training courses. In Sri Lanka, Bachelor Degree offering academic institutions are very low and cybersecurity related subjects are offered only through IT/ICT courses. Therefore, formal in-house training has been selected as 3rd mean at rank number 01. Due to the lack of primary diploma/ degree courses related to cybersecurity, most professionals are motivated to get professional qualifications. Accordingly, there is a high demand for vendor certificates and the forecasted values for vendor certificates are timely increased. The following chart shows the demand for vendor certificates.

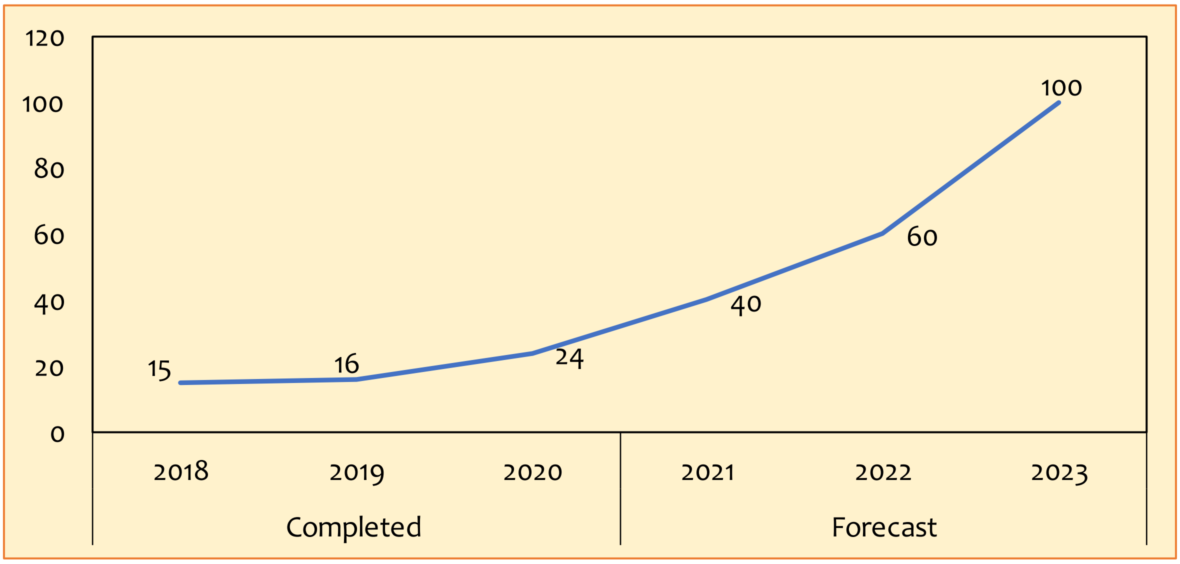


Figure 11: Demand for Vendor Certificates by Professionals

However, the respondents have been selected 'acquiring professional qualifications' as top-rated mean at rank 2. 'Industry awareness/ Exposure' is a pre requisite qualification for career advancement in cybersecurity related industries and it was selected as top-rated mean at rank 3 and 4. Moreover, 'formal in-house training courses' was prioritized at rank 5 as it is also a compulsory requirement for career development in the field. And so on, the 'on the job training' was also rated as third important mean at rank 1, 2 and 3. Cybersecurity beginners in Sri Lanka have followed only subjects at their bachelor degrees, therefore on the jobs trainings is critical factor for career development.

5.4. Practiced Retention Strategies by Employers

Currently, organizations of all sizes and industries are increasingly concerned with cybersecurity risks and how security failures may result in compliance violations, reputational damage, and economic fallout. Therefore, most of organizations have taken initiatives to increase spending in IT security and also, they are planning to make new hires to support the compliance function for their cyber security. However, a global study conducted by ISACA[1] found that 82% of cyber security employees cited better financial incentives, such as salaries and bonuses, as reasons for leaving an employer. Further, this study also found that less than half of cybersecurity organizations have a diversity program for career advancement, and the perception of their effectiveness, when compared to previous years, is declining. The unexpected spread of COVID-19 pandemic has been identified as the prime reason for this decline and also the investment in training is severely affected. However, respondents of the demand survey stated that good compensation plan for employees is the best retention strategy while 'working flexibility', and 'incentives for professional certifications' were rated at second and third respectively.

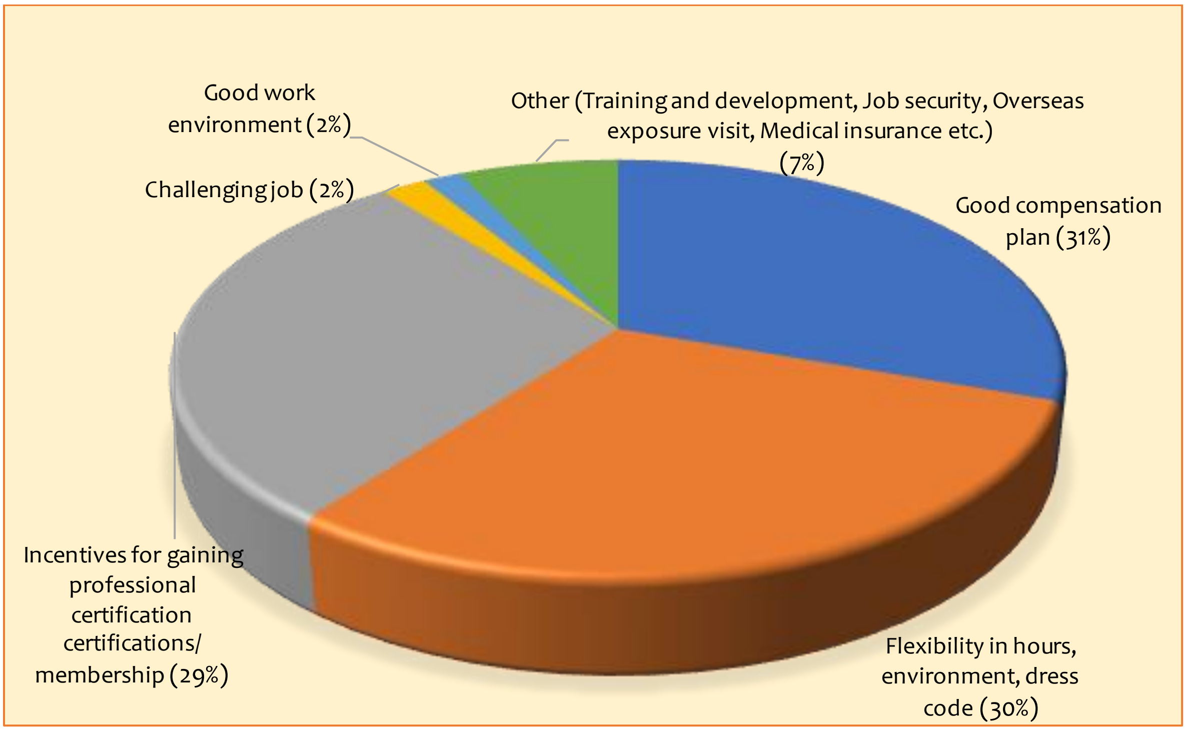


Figure 12: Retention Strategies

Qualitative primary data collection of the demand survey showed that Sri Lanka's cybersecurity market is still small and growing, and one of its main challenges is the lack of laws and regulations around data protection. The lack of regulations and understanding limits the size of the market because only companies that are heavily regulated, like banks, take cybersecurity seriously since they are legally liable. However, the majorities of companies are family-run and lack proper governance structures and they may not always have the technical knowledge and since there is little outsider input in decision-making, security is not prioritized until after an issue occurs. Therefore, the expansion of employment opportunities within such companies happens slowly. However, the entry level opportunities for "freshers" in multi-national, foreign-based companies and medium

[1] ISACA is a global association that provides IT professionals with knowledge, credentials, training and community in audit, governance, risk, and privacy etc.

and large-scale local companies have grown considerably past. Locally, it is expected that there will be 6,000 roles related to cybersecurity in the Sri Lankan job market over the next five years (see chapter 07) that need to be filled, but only a few hundred cybersecurity graduates are entering the profession each year. Working towards making Sri Lanka a cybersecurity hub of sorts, organizations like the Sri Lanka Association for Software Services Companies (SLASSCOM) should heavily push cybersecurity companies to export their services.

5.5. Cybersecurity Related Expenses

From the government to the military, to private and public businesses as well as individuals, all factions of society are becoming increasingly dependent on technology and using digital means to complete tasks, ranging from simple to complex. This inadvertently results in a lot of sensitive data and information being transferred and stored for operations and development. If such sensitive information becomes compromised and falls into the wrong hands, it could not only cause privacy issues for citizens but may also affect the nation's national security and cause severe economic losses for the country. Therefore, all economical sub-sectors are tended to invest more on securing of information has been increased and it was accelerated by COVID-19 pandemic and its effects like growing the working from home culture. However, 2022 is looking to set infamous records in terms of cyber-attack costs, as the damage of cyber-crime is expected to exceed $6 trillion in 2022 which, compared to the $3 trillion globally in 2015.

Sri Lanka's first Information and Cyber Security Strategy to be implemented over a period of five years from 2019 to 2023. The strategy is an institutional framework that aims to create a resilient and trusted cyber security ecosystem that will enable Sri Lankan citizens to have access to safe digital exposure and a facilitate a better future without harm. The implementing of this strategy is continuously increased cybersecurity costs to information owners and it is expected to have 2% more investment on cybersecurity operations, maintenance and salary expenses in 2022 than 2021. The following graph illustrates the cybersecurity related expenses such as salary of staff, costs for operation and maintenance and total cyber security cost against the total annual investments from 2018 (actual) to 2022 (forecast).

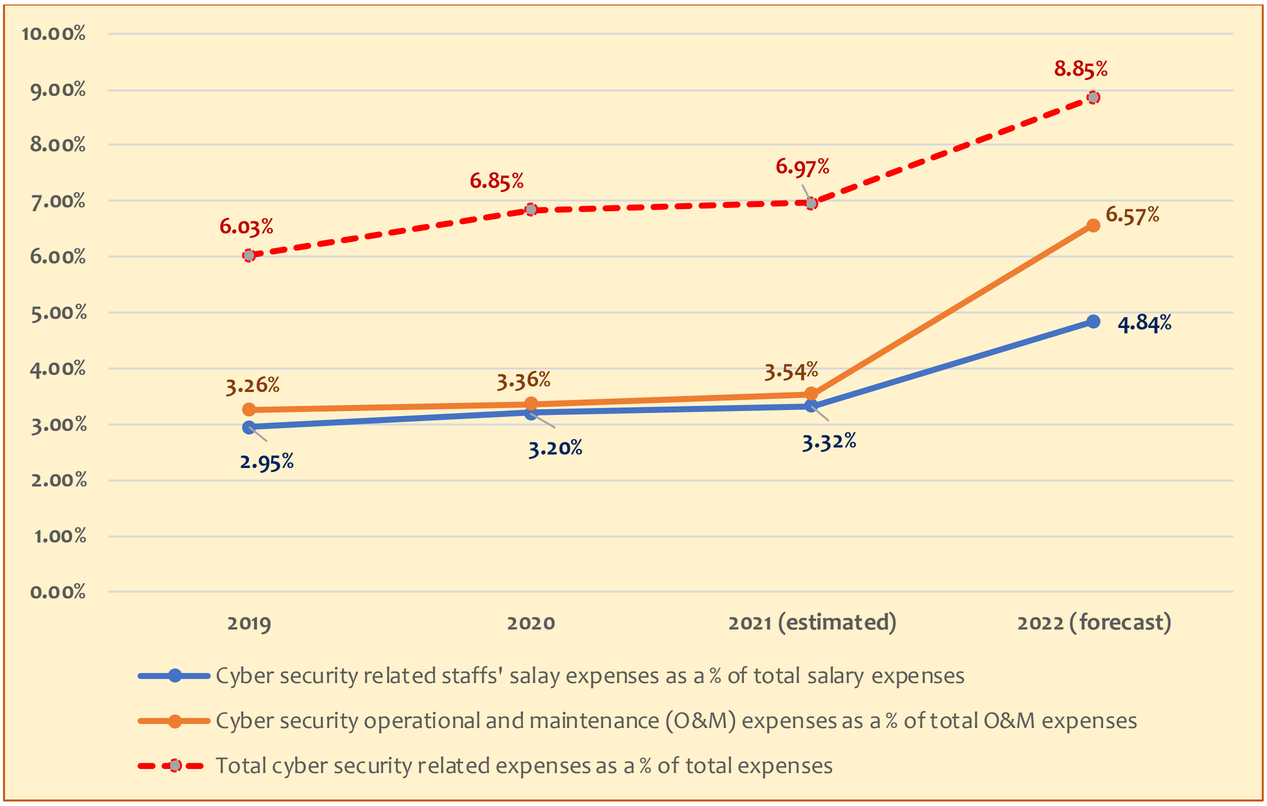


Figure 13: Cybersecurity Related Expenses Distribution

Chapter 6: SUPPLY OF CYBERSECURITY WORKFORCE

6.1 Total Supply of Cybersecurity Professionals

According to the cybersecurity jobs report published in International Cybercrimes the unfilled cybersecurity jobs globally grew by 350%, from 1 million positions in 2013 to 3.5 million in 2021. Looking five years ahead, we predict the same number of openings in 2025 and it is expected that 3.5 million new openings will appear in 2025. For the first time in a decade, the cybersecurity skills gap is leveling off. The global ICT Statistics projects "information security analyst" will be the 10th fastest growing occupation over the next decade, with an employment growth rate of 31% compared to the 4% average growth rate for all occupations. A majority of these (entry to mid-level) positions do not require certifications and allow employers to cast a wider net for candidates. Moreover, governments and companies have continually struggled to hire qualified professionals to assist them in building a better security work-frame. There is a severe shortage of cybersecurity professionals, ringing alarm bells since a digital workforce is instrumental in combating these growing trends of cyberattacks.

One of the primary reasons for the lack of candidates can be pointed towards funding and investments forwarded by IT companies. Training schools at every country are also lacking a cybersecurity curriculum that can train students professionally on emerging technologies. Cost is also another barrier for students to opt for this coursework. Organizations are not keen on investing in cybersecurity or hire "freshers" unless they have prior experience. However, more than 85% of the global IT professionals still believe that there is a shortage of cybersecurity professionals and perhaps it is one of those rare fields that is outgrowing and hiring amid COVID-19. Whilst it's possible to find certain entry-level cybersecurity positions with an associate's degree, most jobs require a four-year Bachelor's Degree in Cybersecurity or a related field such as Information Technology or Computer Science. Global level gender disaggregated data shows that women represent 25% of the global cybersecurity workforce in 2021, up from 20% in 2019, and around 10% in 2011. Cybersecurity Ventures predicts that women will represent 30% of the global cybersecurity workforce by 2025, and that will reach 35% by 2031. However, in Sri Lanka the women representation for cybersecurity careers remains at 10% over the past few years. This can be due to the "glass ceiling" in Sri Lanka in which women struggle to elevate further in their careers to leadership positions due to patriarchal norms in the country – especially in fields commonly dominated by men such as IT.

It was identified the need to consider the supply of talented individuals to the cybersecurity recruitment pool in the required numbers on a wide basis. For example, there are many routes by which an individual can enter the cyber security workforce which need to be identified. Furthermore, there are alternative routes that are likely to play a more significant part in filling the needs of employers, such as apprenticeships, retraining and reskilling, and online learning. Hence the following key areas were identified to explore the supply of new talent.

Undergraduates, postgraduates and PhDs produced each year, in both ICT and Cybersecurity courses

- Degree in Cybersecurity
- Students with relevant A Level/NVQ qualifications moving into further or higher courses
- Existing IT professionals that could potentially move into cyber roles in the near future
- Potential supply gaps that could be addressed through lesser explored talent

Accordingly, data collection conducted through a supply assessment survey with education service providers to assess local level cybersecurity related skills supplies. The supply questionnaire survey collected data from 13 Government Universities, 6 Private Degree Awarding Institutions, 2 Registered Vocational Training Institutes and 1 Professional Training Provider. Altogether there were 22 ICT skill suppliers where only 14 are offered cybersecurity related courses. The following table shows the summary of the courses offered in relation to the ICT and cybersecurity sectors by each type of supplier.

Table 10: Courses Offered for ICT and Cybersecurity

Offered Qualification	Number of ICT and Cybersecurity (CS) Courses Offered by Supply Institutions									
	Government University		Private Degree Awarding Institution		Registered Vocational Training Institute (Registered under TVEC)		Professional Training Provider		Total Courses Offered	
	ICT	CS	ICT	CS	ICT	CS	ICT	CS	ICT	CS
PhD	8	1	2	-	-	-	-	-	10	1
Master's Degree	6	2	4	2	1	-	-	-	11	4
Postgraduate Diploma	4	-	3	-	-	-	-	-	7	-
Bachelor's Degree	12	3	6	4	2	1	1	-	21	8

Offered Qualification	Number of ICT and Cybersecurity (CS) Courses Offered by Supply Institutions									
	Government University		Private Degree Awarding Institution		Registered Vocational Training Institute (Registered under TVEC)		Professional Training Provider		Total Courses Offered	
	ICT	CS	ICT	CS	ICT	CS	ICT	CS	ICT	CS
Higher Diploma	-	-	5	1	1	1	-	-	6	2
Diploma	-	-	4	-	1	1	-	-	5	1
Trade Certificates (Vendor Certificates)	-	-	2	1	2	2	-	1	2	3
Trade Certificates (Vendor Neutral Certificates)	-	-	-	-	-	-	-	1	-	2
Total Number of Suppliers	13	6	6	5	2	2	1	1	22	14

Some of the suppliers stated that the 2008/21 circular for the state universities pressed by UGC, there are 5 categories under the Computer Science stream. In which cybersecurity part has not been introduced as a one of the 5 categories. The standard committee of Computer Science in UGC is expected to expand the number of subject categories of Computer Science from currently conducting 5 categories to 6/7 by introducing cybersecurity as a new one. Furthermore, they explained that they are covering some network security courses but not much in cybersecurity. They don't have diversified lecturers for that kind of programs. Number of carder positions limited and less. Diversified experts of cybersecurity are also limited on the lecturer panel. But if students want to do a research project in cybersecurity, they have been allowed to do that. Apart from within the Jaffna peninsula, the demand for cybersecurity positions are also less compared to the Western Province. They are some Computer Security courses as follows in the Physical Science stream and Computer Science stream, and the degree programs that they offer are Bachelor of Science Honors in Computer Science and Bachelor of Science Honors in Applied Science. One government university expressed, they offer only module in Information Security with 2 credits and it is only a 30hrs course in Bachelor's Degree.

However, according to industry experts all ICT courses offered in public and private sector institutions need to take immediate and accelerated actions to design cybersecurity courses as the demand side has 300% rapid increase in annually during last 5 years.

6.2 Qualifications Completed in 2018, 2019 and 2020

The following table shows the number of students who completed their academic qualifications in relation to cybersecurity in 2018, 2019 and 2020.

Table 11: No. of Students who completed their Academic Qualifications in Cybersecurity

Year	Completed Qualifications	Government University		Private Degree Awarding Institution		Registered Vocational Training Institute		Professional Training Provider		Total	
		Male	Female	Male	Female	Male	Female	Male	Female	Male	Female
2018	PhD										
	Master's Degree	50	12	66	9					116	21
	Postgraduate Diploma	8	3							8	3
	Bachelor's Degree			26	6					26	6
	Higher Diploma			21	4	2	2			23	6
	Diploma					7	1			7	1
	Trade Certificates (Vendor Certificates)							15		15	
	Other Qualifications					18				18	
	Total in 2018	**58**	**15**	**113**	**19**	**27**	**3**	**15**		**213**	**37**
2019	PhD										
	Master's Degree	56	13	67	8					123	21
	Postgraduate Diploma	12	3							12	3
	Bachelor's Degree			79	20					79	20
	Higher Diploma			23	3					23	3
	Diploma										
	Trade Certificates (Vendor Certificates)										
	Other Qualifications			13						13	
	Total in 2019	**68**	**16**	**182**	**31**					**250**	**47**
2020	PhD										

Year	Completed Qualifications	Government University		Private Degree Awarding Institution		Registered Vocational Training Institute		Professional Training Provider		Total	
		Male	Female	Male	Female	Male	Female	Male	Female	Male	Female
	Master's Degree	60	10	87	13					147	23
	Postgraduate Diploma	14	4							14	4
	Bachelor's Degree			100	34	7	2			107	36
	Higher Diploma			12	3	13	2			25	5
	Diploma					9				9	
	Trade Certificates (Vendor Certificates)			22	2					22	2
	Trade Certificates (Vendor Neutral Certificates)										
	Other Qualifications										
	Total in 2019	**74**	**14**	**221**	**52**	**29**	**4**			**324**	**70**

According to the suppliers' data, female candidates have showed a slight improvement in enrolment for cybersecurity courses from 2018 to 2020. However, the demand for female practitioners is still remained around 10%. Data shows only 15% to 20% of female employees are moving towards to follow the higher education qualifications in cybersecurity.

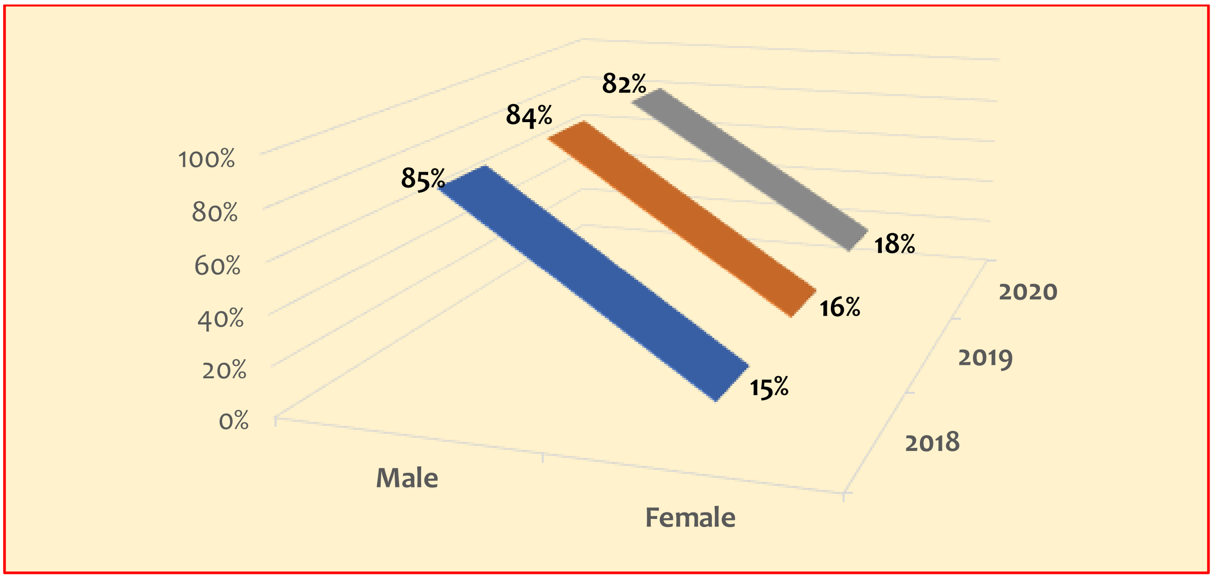


Figure 14: Total Supply by Gender in 2018, 2019 and 2020

6.3 Cybersecurity Courses Designed to Offer in 2021, 2022 and 2023

Sri Lanka's cybersecurity market is anticipated to witness significant growth in the coming 4-5 years. This is backed by an increase in the growth of the modern industrial landscape which is leading to a rise in the automated technology underpinned by massive software and internet technology use. Moreover, this is expected to be of great importance for shaping the industrial landscape of the cyber industry. Additionally, a rise in the growth of digital platforms supported by the rapid growth of digital and technical aid. There is a need for technical aid over the digital platform to safeguard the data and software-indulged industrial work and is expected to benefit the Sri Lanka cybersecurity market to seek growth in the coming time period. Furthermore, the market anticipates registering significant revenue growth in the coming time period underpinned by deeper penetration of digitalization in the developing and developed economies across the region. The era of digitalization has posed great opportunities on the face of the technological up gradation and advancement adoption across various industrial applications and as a result is leading to the exposure of the digital platforms towards digital threats which poses a great need for security to be followed for the long-term success of digital business platforms and is expected to be a catalyst in the overall market growth of the Sri Lanka cybersecurity market in the forthcoming years. Hence, the market suppliers expect to increase the number of graduates/ post graduates during next 03 years and the following table shows the forecast data by major suppliers for 2021, 2022 and 2023.

The following table shows the forecast data by major suppliers for 2021, 2022 and 2023.

Table 12: Forecast Data by Major Suppliers for 2021, 2022 and 2023

Forecast Year	Qualification	Government University	Private Degree Awarding Institution	Registered Vocational Training Institute	Total
2021	PhD	16	14	2	32
	Master's Degree	135	50		185
	Postgraduate Diploma				
	Bachelor's Degree		153	9	162
	Higher Diploma			14	14
	Diploma			16	16
	Trade Certificates (Vendor Certificates)		40		40
	Other Qualifications			18	18
	Total Forecast for 2021	**151**	**257**	**59**	**467**

2022	PhD	19	17	2	38
	Master’s Degree	155	60		215
	Postgraduate Diploma				0
	Bachelor’s Degree		160	5	165
	Higher Diploma			8	8
	Diploma			12	12
	Trade Certificates (Vendor Certificates)		60		60
	Other Qualifications			22	22
	Total Forecast for 2022	**174**	**297**	**49**	**520**
2023	PhD	20	20	3	43
	Master’s Degree	185	75		260
	Postgraduate Diploma				0
	Bachelor’s Degree		195	12	207
	Higher Diploma			9	9
	Diploma			8	8
	Trade Certificates (Vendor Certificates)		100		100
	Other Qualifications			25	25
	Total Forecast for 2022	**205**	**390**	**57**	**652**

On the basis of end-user industry segmentation, the retail industry is expected to contribute towards the growth of the cybersecurity in the coming time frame. This is backed by the massive deployment of e-commerce platforms leading to immense and vital product-related information loaded over the web, which requires timely updates and security as such data is exposed to customer malware activities and false claims by famous brands to catch the interest of the public for fraudulent means. As a result, this may hamper the industrial outlook and goodwill of top retail brands. Henceforth, leading to an increased need for cybersecurity to safeguard the interest of the consumers and sustain the goodwill of the organization/brand and is expected to be a much vital source of growth for the Sri Lanka cybersecurity market in the coming years.

According to the forecast data collected for 2021, 2022 and 2023 the following table illustrates the percentage of credits assigned for cybersecurity related subjects in relation to the academic courses. Common cybersecurity credits offer courses available at both public and private sector institutions are Certificate of Cyber Security, Advanced Certificate in Network and Systems Administration, Diploma in Cyber Security, Advanced diploma in Cyber Security, Higher National Diploma in Network Engineering, Bachelor of Information and Communication Technology, Bachelor of Science (Cyber Security), BSc. (Hons) Ethical Hacking and Network Security, BSc. in ICT (Specialized in Network and Security Technologies), BSc. in ICT (Specialized in Network and Security Technologies), Master of

Cybersecurity, MSc Cyber Security and Forensics, MSc Networking and Information Security (NIS).

Table 13: Percentage of Credits Assigned for Cybersecurity Subjects

Academic Course	Average Total Credits of the Course	Assigned Credits to Cover Cybersecurity Subjects	Cybersecurity Credit as % of Total Credit
Certificate Courses	32	21	66%
Bachelor's Degree	190	80	42%
Master's Degree	113	83	73%
PhD	120	110	92%

The workforce shortage and gender disparity in cybersecurity profession pose a greater risk to the digital economies from cyber adversaries. The global efforts and initiatives for women to pursue career in cybersecurity field tend to be lesser than men along with various societal barriers, which consequently result in their underrepresentation and underutilization in cyber industry. The data collect collected by the survey is given evidences that the suppliers in both public and private sectors are expected to enroll male to female students for next 03 years by 80%: 20% ratio.

6.4 Skills Plan to be Developed through Future Courses

Employees who are pursuing a career in this field will need to have a broad set of technical, professional, and functional skills, as well as the specific cybersecurity skills and key soft skills in demand by employers that will set their employees apart from the competition. Key experts in the supply side expressed, some of the skills should naturally have, for example, an inclination for analytical thinking and technology that need to develop through formal training or education. According to them, depending on students' background, a certificate or diploma courses in cybersecurity is a good place to start. It will provide a solid foundation in the principles of cybersecurity, in addition to an overview of security across a variety of platforms, programming and development, digital forensic investigation, specific technical skills such as those relating to computer and operating systems and networking and more. Suppliers have designed to develop following technical skills of cybersecurity students during next three years. Cybersecurity analytics and intelligence skill was rated as prioritized technical skill that needs to be developed during forthcoming courses.

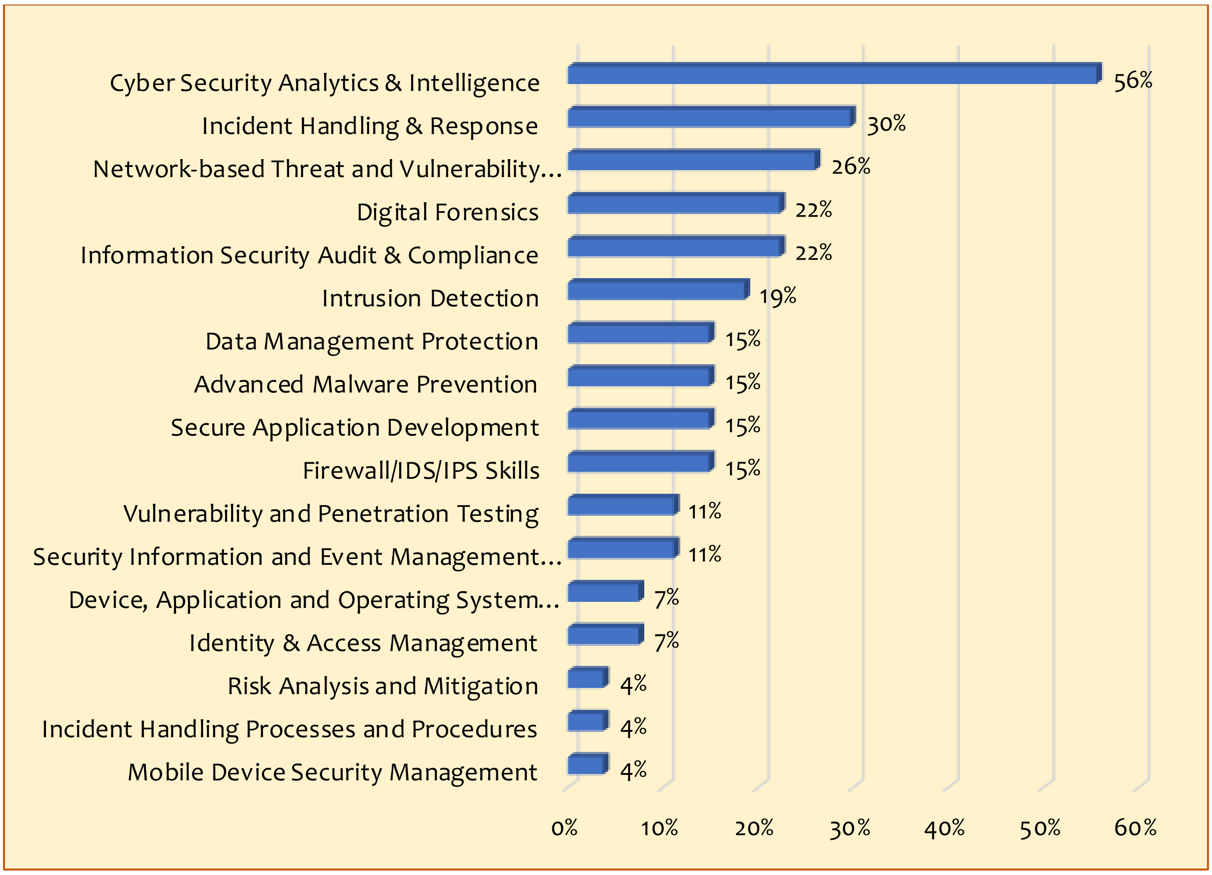


Figure 15: Cybersecurity Related Technical Skills to be Developed within Next 3 Years

Employees seeking cybersecurity roles should have a profound thirst for knowledge and a strong sense of curiosity for their career development. The cyber threat landscape is continuously evolving, so if employees are transitioning into this field, they need to be prepared to continually learn, and perform the task earnestly. Therefore, the course contents were developed by the suppliers to catch up not only on the technical skills, but the soft skills as well. Furthermore, they expected to develop the following soft skills through the cybersecurity related learnings. According to the data provided, each supplier who has designed to offer cybersecurity related courses during next 3 years, all of them are expected to develop communication skill as a prioritized soft skill. Strong problem-solving skills and teamwork abilities are the next prioritized soft skills followed by skills in communication. Lastly but certainly not the least, soft skills are extremely crucial in this field to understand the requirements of the companies and understand the motives of attackers. Furthermore, they expected to develop the following soft skills through cybersecurity related teachings.

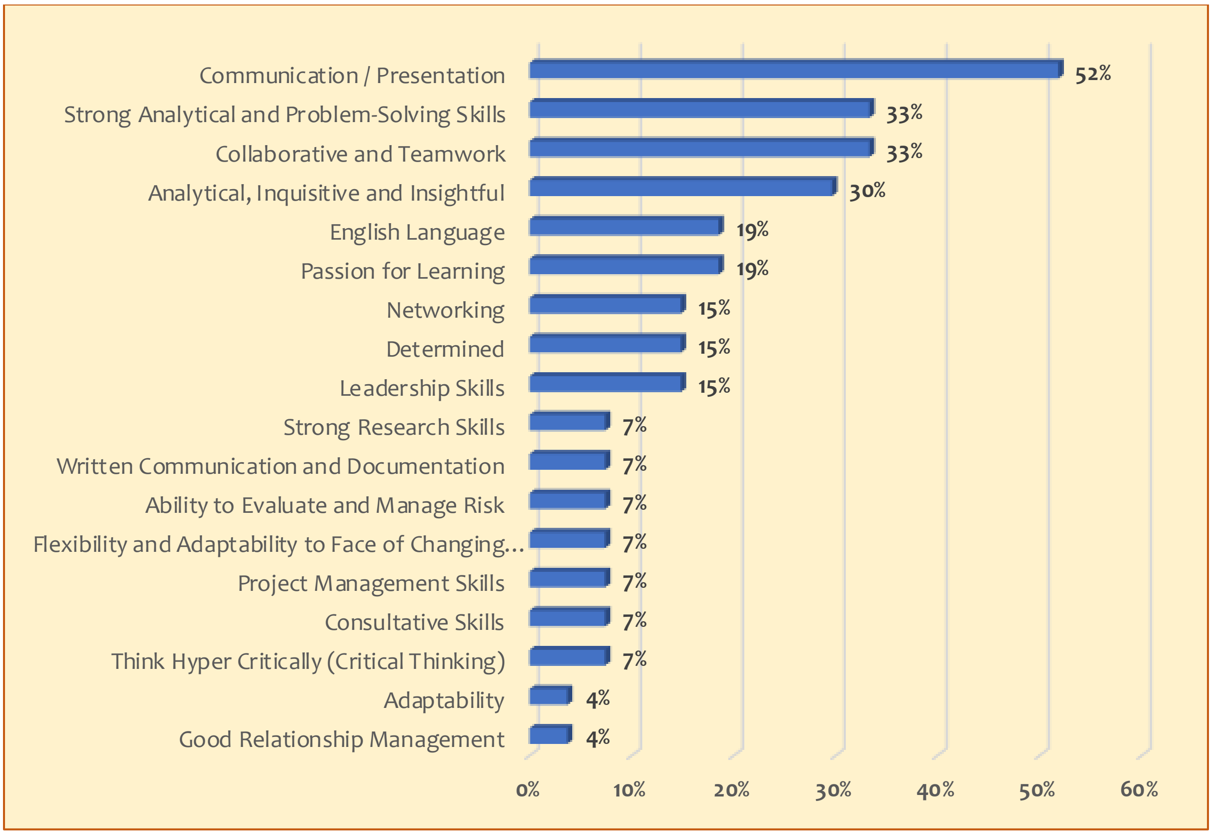


Figure 16: Soft Skills Categories for Development in Next 3 Years

More than one fifth of full-time cyber security teachers in Sri Lanka are female.

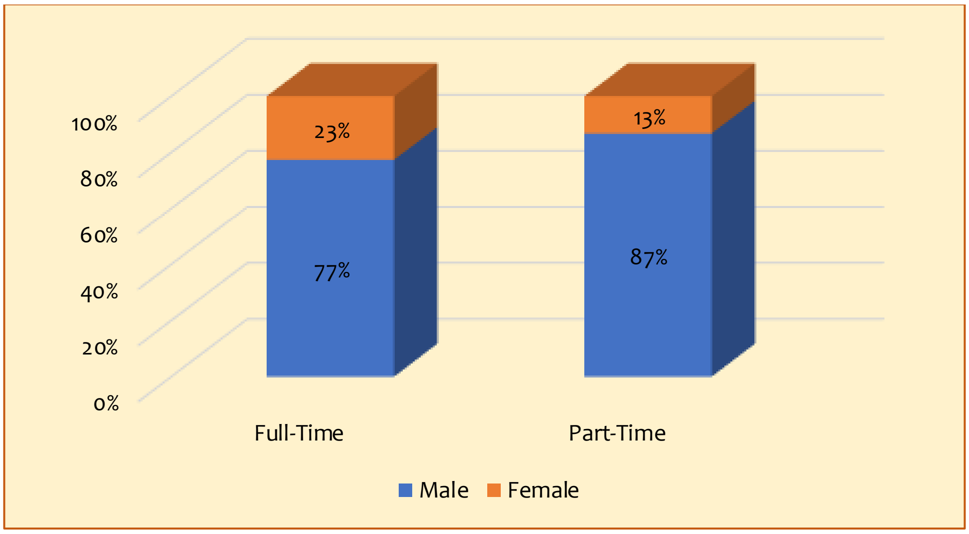


Figure 17: Type of Employment (Full-time / Part-time) for Cybersecurity Teachers

70% of lecturers' have 3-8 years' experience in cybersecurity related teaching experience and about 24% of them having more than 8 years of experience.

Table 14: Years of Teaching Experience in Cybersecurity for Cybersecurity Lecturers

Type of Employment	Type of Institute	Gender of Lecturer	0-1 years	1-3 years	3-8 years	8-12 years	Above 12 years	Total
Full-Time	Government University	Male			6	2	3	11
		Female			1			1
	Private Degree Awarding Institution	Male	2	2	13	6	6	29
		Female		5	4	2		11
	Registered Vocational Training Institute	Male			1			1
		Female						
	Professional Training Provider	Male						
		Female						
Total Full-Time Lecturers			**2**	**7**	**25**	**10**	**9**	**53**
Part-Time	Government University	Male			4			4
		Female						
	Private Degree Awarding Institution	Male			20	14	9	43
		Female			2	1	1	4
	Registered Vocational Training Institute	Male		4	55	3	2	64
		Female			1			1
	Professional Training Provider	Male			20			20
		Female			15			15
Total Part-Time Lecturers			**-**	**4**	**117**	**18**	**12**	**151**
Total Lecturers			**2**	**11**	**142**	**28**	**21**	**204**

The following graph illustrates the teaching experience of cybersecurity lecturers by their qualifications.

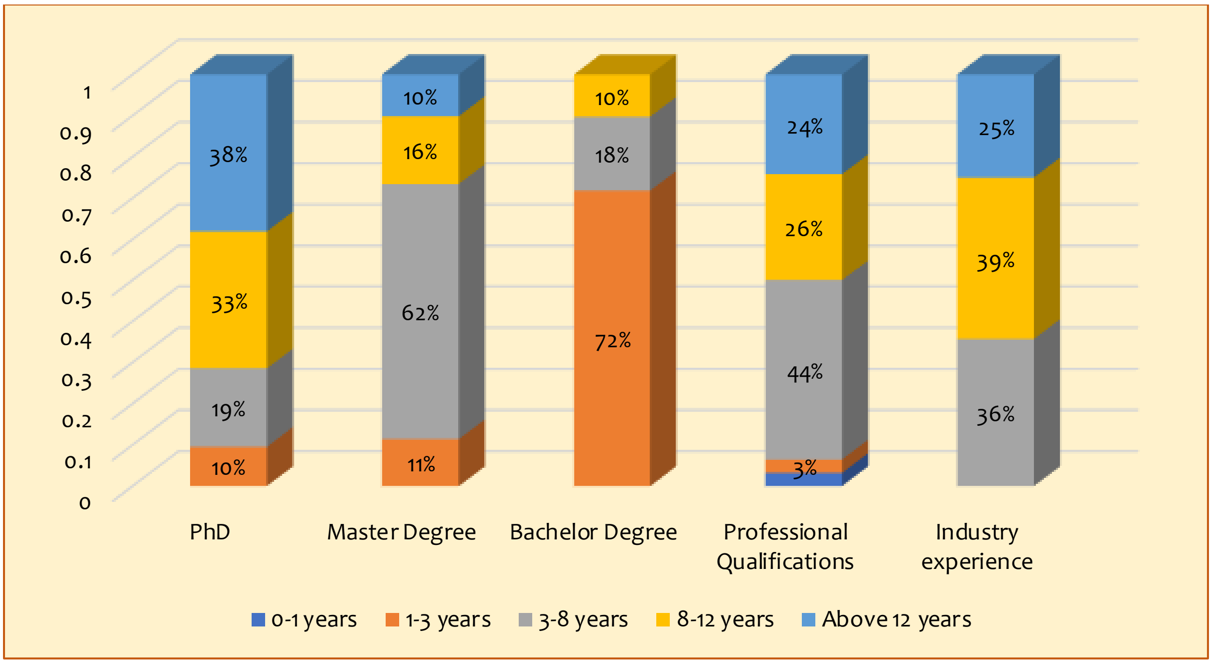


Figure 18: Experience of Lecturers by their Qualifications

Most PhD holders have more than 12 years experiences and all of them are represented in universities that offer Master level degrees in Cybersecurity. More than 70% of Bachelor Degree holding trainers have 1-3 years' experience. However, trainers who have industry experience, stated that their level of experience is matured than academically qualified trainers. It was emphasized that the importance of gaining general hands-on experience in IT into cybersecurity highlighted how important it is to continuously approach this field as a student to keep learning new things and to always stay abreast of the latest developments. According to the top-level teachers in the public sector universities, there's a difference between difficult and challenging in learning the cybersecurity subjects. Furthermore they stated, the learning cybersecurity can be challenging, but it doesn't have to be difficult, especially if students are passionate about technology. Nurture a curiosity for the technologies students are working with, and they might find that challenging skills become easier. Many cybersecurity courses include virtual labs where students can practice applying their skills using real security tools in simulated environments. It's convenient to have these labs ready to go as part of a structured course, but they can get as much practice as them want by setting up their own virtual lab. It was also highlighted during the KIIs that Sri Lanka should work towards having better lecturers who can act as mentors for cybersecurity students to learn from as this is the best method to proactively learn about cybersecurity.

Chapter 7: DEMAND – SUPPLY GAP IN THE CYBERSECURITY WORKFORCE

7.1 Demand for Cybersecurity Practitioners

The demand survey collected actual data from responded companies for 2020 and 2021. In 2020 the calculated total workforce of cybersecurity practitioners was 1011. However, after one year that number has increased approximately by 400 new entries. According to the KIIs, several key informants responded that the number needs to be doubled as the COVID-19 pandemic has transformed all aspects of lives and has taken into the digital arena. Due to that, the protection of cyber space for 'information security' should be locally emphasized for nation's defense. According to the experts in the supply market, they need to plan a major development of cybersecurity content crosswise the course as all undergraduates to signify the admission into the sketchily defined cybersecurity labor forces. Furthermore they stated that, there are more choices that exist for present professionals to enhance their skill-set, with diplomas from technical training firms, additional graduations through college education, or separate hands-on courses to advance specific skills. However, the higher-level cybersecurity practitioners have understood that, there is a great boom in these occupations and the specific skill sets, where the growth in local level cybersecurity jobs has just begun. Due to the effect of the COVID-19 pandemic, paving the way for higher acceptance of digital technologies at the individual, corporate, industry, and national levels and it creates a big market for cybersecurity practitioners.

7.1.1 Estimated Demand for Total Cybersecurity Workforce

Table 15: Actual and Estimated Demand of CSPs from 2020 to 2025

Year	Actual	Estimated
2020	1011	-
2021	1415	-
2022	-	1819
2023	-	2223
2024	-	2627
2025	-	3031

Based on the surveyed data, the total cybersecurity workforce has estimated and approximately, it is expected to have 3,000 practitioners by 2025. However, the smaller number of non-IT firms has been taken into account when conducting the survey and that number needs to be projected to 20% of total non-IT companies existed locally (approximately 6,000). Also 20% of the IT companies were used as sampling points and the estimated figures were calculated considering that factor too. Moreover, considering the macro-economic characteristics in the country, the demand analysis was performed exponentially and it ended at the range of 5000-6000 workforce. Therefore, the survey findings provided evidence that the expectation about the blooming of local cybersecurity market by 4000-5000 practitioners within next few years.

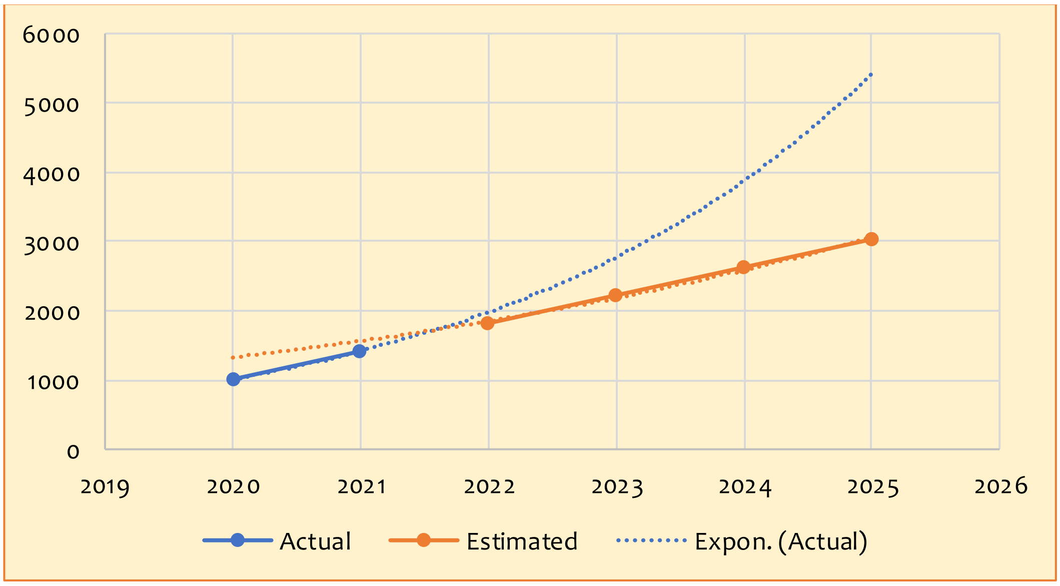


Figure 19: Demand for Total Cybersecurity Workforce

7.1.2 Estimated Annual Demand for Cybersecurity Workforce

The sample data shows approximately 500 estimated opportunities for new entries will create annually in the market. This number needs to be projected for whole population in the market and it has estimated nearly 800-1000 new cybersecurity practitioners are required annually to fill the gaps in the whole market. It is expected, in 2025, it requires 1000-1200 new graduates annually to fill the gaps in the market. The ICT industry is Sri Lanka's fourth largest export earner and existing government has taken key initiatives for data/ information protection interventions. Also, Sri Lanka's competitive advantage in the IT and business process outsourcing (BPO) industry is built high value to cost and a niche talent base for doing business for new investors. The Port-City project implemented by the government will also be a better market for new ICT investors within next decade. Therefore, the annual demand for the local market need around 1000 of new cyber security professionals.

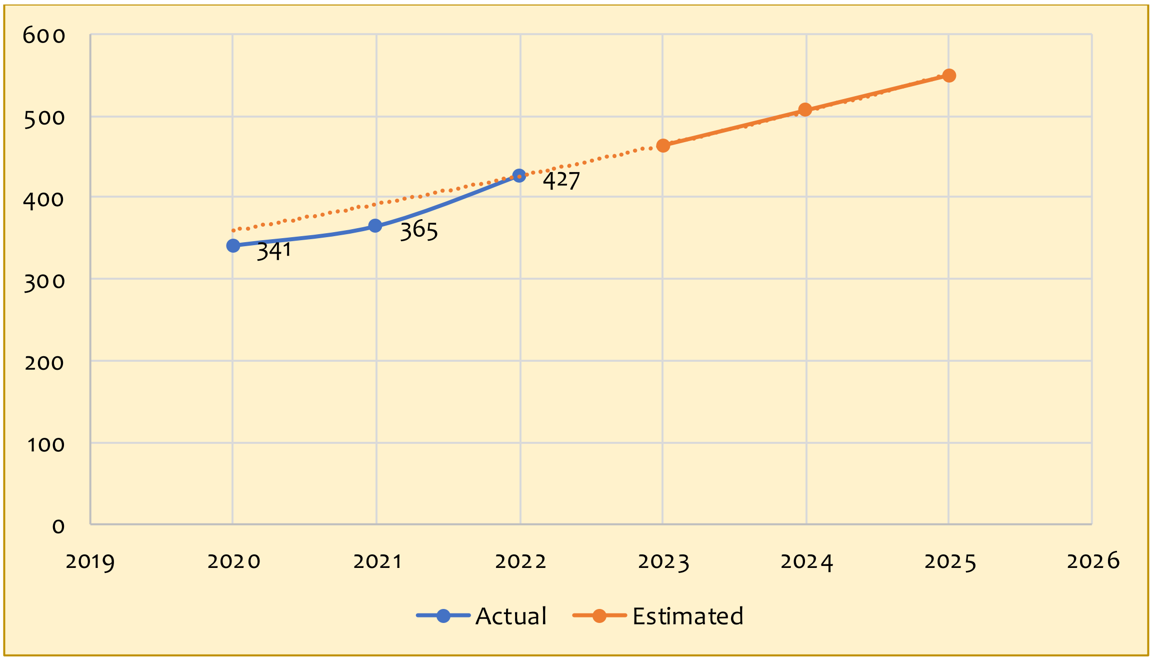


Figure 20: Annual Demand for Cybersecurity Practitioners

7.2 Supply of Cybersecurity Practitioners

7.2.1 Supply of Cybersecurity Practitioners (Qualifications Completed and Estimated Figures)

The table below displays the type of qualification for cybersecurity and the number of both completed graduates as well as estimated graduates. There is an increasing trend in the number of cybersecurity qualifications in Sri Lanka which shows a clear expansion in the supply of cybersecurity professionals in the country.

Table 16: Type of Qualification and Estimated Figures for Cybersecurity

Qualification	**Completed Qualifications**			**Estimated Figures**		
	2018	**2019**	**2020**	**2021**	**2022**	**2023**
PhD	0	0	0	35	42	48
Master Degrees	137	144	170	185	215	260
Pg Dip	11	15	18			
Bachelor Degrees	32	99	165	187	190	232
Higher Diploma	29	36	30	14	8	9
Diploma	8	11	9	16	12	8
Vendor Certificates	15		24	40	60	100
Other Qualifications	22	13	16	18	22	25
Total	**254**	**318**	**432**	**495**	**549**	**682**

When examining which qualification has the highest number of completed qualifications and estimated figures, Master's Degrees in Cybersecurity have emerged as the most sought after qualification. Secondly, Bachelor's Degrees in Cybersecurity have also rapidly increased over the past three years and continue to show an exponential increase in the years to come. One of the reasons for the high number of students for conducting Master's Degrees related to Cybersecurity is that even students who conduct their Bachelor's or undergraduate programs in IT choose to specialize their further studies specifically in cybersecurity. There is also a notable increase in the estimated figures for Vendor Certificates which showcases the importance of these certificates when it comes to cybersecurity as it allows for more product-specific / problem-specific knowledge to be obtained.

7.2.2. Forecast of the Supply of Cybersecurity Practitioners

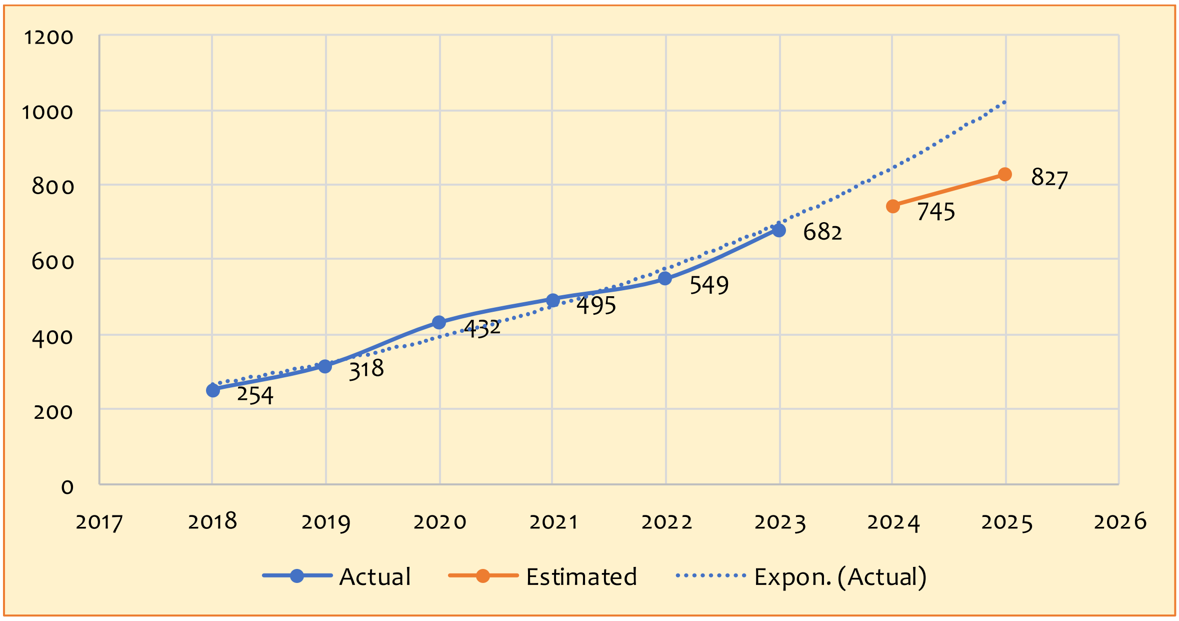


Figure 21: Forecast of the Supply of Cybersecurity Professionals

As shown in the figure above, there has always been a steady increase in the number of cybersecurity graduates in Sri Lanka and it is also projected that an even rapid increase in the supply of cybersecurity professionals will take place from 2022 onwards.

7.3 Gap between the Demand and Supply of Cybersecurity Practitioners

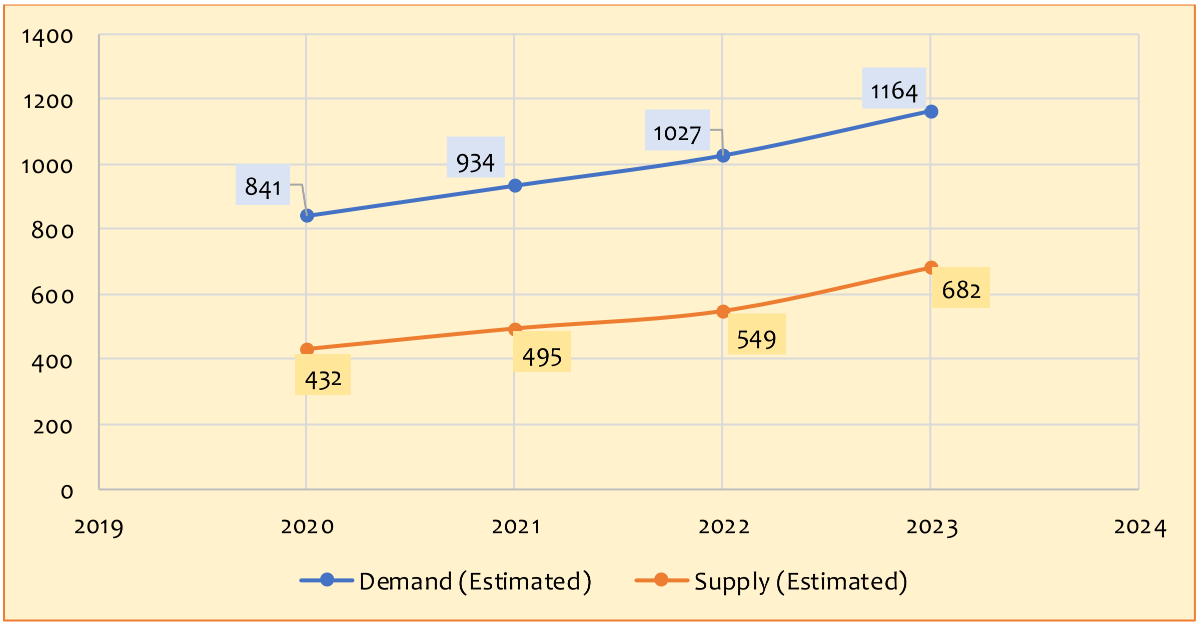


Figure 22: Gap between Demand and Supply of CSPs

Although there is a definite estimated increase in the supply of cybersecurity graduates in Sri Lanka, the figures for the estimated demand has drastically doubled. This demonstrates that there is a substantial gap between the demand and supply of cybersecurity professionals in the country. With rapidly evolving infrastructure of the Internet due to COVID-19 and the rise of remote working and online school, cybersecurity has dominated as one of the most sought after job openings and degrees to study.

Chapter 8: CONCLUSIONS AND RECOMMENDATIONS

The main conclusion of the survey is that there is a significant demand for the Cybersecurity practitioners in Sri Lanka. Although there is an estimated increase in the supply of cybersecurity graduates and other academic qualifications, it is insufficient to fulfil the market requirement. The demand for cybersecurity practitioners is mainly from the private sector of Sri Lanka.

Globally, the ICT sector experiences a transition with the impact of COVID-19 over the last two year which has created a significant demand for cybersecurity practitioners globally as well as Sri Lanka. Some of the academic institutes have planned to increase the intake to supply of cybersecurity practitioners to the market.

Cybersecurity are related professions are mostly considering as mid-career challenging professions for IT Graduates.

The employers should encourage their IT employees to enhance qualification by conducting relevant professional and academic programs. The training institute should be connected with the ICT industry to develop more industry oriented academic and professional programs for cyber security. The IT employees of the organizations should be encouraged to acquire cybersecurity related qualifications enabling them to get involved in cybersecurity related operation in organizations. This will help the industry to bridge the gap of supply and demand of cyber security practitioners in Sri Lanka.

With the current demand for Cybersecurity practitioners in Sri Lanka a lot of training service provided, including Government universities have planned to offer academic programs at graduate level and above. However, some of the training service providers do not have the human resources, industry accepted accredited training programs and the supporting infrastructure to conduct the academic and professional training programs in Cybersecurity. On the other hand, most of the academic program and professional programs are not affordable for many individuals starting careers in IT field.

The industry is not fully satisfied with the competencies of the entry level cyber security staff and the skill provided the training service provided.

It is suggested to develop education program in cybersecurity for students with relevant A Level/NVQ qualifications moving into further or higher courses at affordable rates.

The selected training providers should be encouraged and supported to establish the required infrastructure to offer hand-on experience on cybersecurity. It is a felt need to build the capacity of cybersecurity practitioners training service providers which can be promoted by collaboratively working arrangements between policy makers; including

Ministry of education, University Grant Commission, TVEC, private and government training service providers, ICT industry representatives and professional bodies interested in the subject matter.

It is essentials to have a collaborative mechanism monitor and evaluate the academic and profession programs with a committee from by the stakeholders concede of by empowering an existing committee.

This study is the first study of this nature in Sri Lanka. Most of the information are generated from the information gathered from sample of organization with stakeholder consultation. The study started in a pre-Covid-19 environment and conducted in a post in a post Covid-19 scenario. Therefore, the information collected and the estimations based on the responses could have impacted by the prevailed situation and the global and local transformation on ICT industry associate with the COIVD-19.

The information collected should be supported with further studies and follow-up studies and industry verifications at different intervals to fine-tune the projections and make recommendation for strategic mid-term and long-term intervention in the future.

References

Cybercrime Magazine. 2021. Cybersecurity Jobs Report: 3.5 million openings In 2025. [online] Available at: <https://cybersecurityventures.com/jobs/> [Accessed 2 December 2021].

Department of Census and Statistics, 2016. Information Technology and Information Technology Enabled Services.

LearnHowToBecome.org. 2021. Cybersecurity Degrees & Careers | How to Work in Cybersecurity. [online] Available at: <https://www.learnhowtobecome.org/computer-careers/cyber-security/> [Accessed 28 December 2021].

NetQuest. 2021. What is The Future of Cybersecurity? | Trends & Emerging Technologies –

NetQuest. [online] Available at: <https://netquestcorp.com/what-is-the-future-of-cybersecurity-trends-emerging-technologies/> [Accessed 2 December 2021].

PurpleSec. 2021. 2021 Cybersecurity Statistics Trends & Data. [online] Available at: <https://purplesec.us/resources/cyber-security-statistics/> [Accessed 2 December 2021].

SLASSCOM, 2021. Cyber Security Centre of Excellence CSCx. https://slasscom.lk/cyber-security-centre-of-excellence-cscx/

Annex 1: Terms of Reference

Brief Terms of Reference: Cybersecurity Professional’s Supply and Demand Assessment

1. Background

With the rapid development of the Information and communication technology during the last decades, online services delivery and online social engagements have grown exponentially. Along with the numerous rewards that digitalization provides, there are threats and risks emerging where it is almost impossible to terminate the negative impacts. The fiscal institutions, defence agencies and the government institutes have become the primary targets of the attackers nowadays. Hence the cyber hazards should be identified beforehand and should be taken precautions in advance. Most of the attacks turn out to be successful due to the lack of awareness and lack of skills of the people who are handling these ICT systems.

In this context, it is necessary to ensure the availability of a cadre of knowledgeable and highly skilled professionals in the field of information and cybersecurity domain to protect, detect, defend and respond to these cyberattacks. It has been proved from the researchers conducted by universities, research institutes and other academic organizations all over the world that there is a vacuum in information security experts in the field. In 2016, a skills gap analysis from Information Systems Audit and Control Association (ISACA) estimated a global shortage of 2 million cybersecurity professionals by 2019. As per the Global Cybersecurity Index (GCSI), Sri Lanka requires to expend much effort on building overall human resource capacity to combat emerging cyber threats.

In Sri Lanka, to date, there are lack of initiatives to address the domestic shortage of cybersecurity experts. Therefore, Sri Lanka CERT aims to conduct a national level survey to analyse the gap between the supply and demand of information and cybersecurity professionals in the industry. Results of this analysis will be utilized by Sri Lanka CERT to formulate appropriate strategies and policies to fill the supply and demand gap of cybersecurity professionals of the country.

2. Aim and Objectives of the Study

The aim of this study is to obtain services of a consultancy firm to assess the supply and demand of the information and cybersecurity professionals of the country and to formulate a strategy to fill the gap.

The specific objectives of the study include,

(a) Data gathering and Analysis of the supply of professionals for the Information and Cybersecurity related job roles.

(b) Data gathering and Analysis of the demand for the Information and Cybersecurity professionals in the job market.

(c) To analyze the gap between supply and demand of information and Cybersecurity professionals.

(d) Formulate an operational strategy to fill the gap between supply and demand of Information and Cybersecurity professionals in Sri Lanka.

3. Scope of Activities

3.1. The consultant shall identify and closely work with the key stakeholders in this domain relevant to the assignment. Key stakeholders should include but not limited to, Industry representatives (E.g.: FITIS, SLASCOM, Industry Skills Sector Council etc.), Tertiary and Vocational Education Commission, Department of Man Power and Employment, universities, private sector institutes, government organizations, private firms, and recruitment agencies.

3.2. The consultant shall closely work with the Project Steering Committee (PSC) appointed by Sri Lanka CERT.

3.3. The consultant shall develop a suitable study approach to analyze the supply and demand of information and cybersecurity professionals. The consultant shall use a wide range of data collection methods including, review of secondary documents (E.g.: labor market reports, Vocational Education and Training Plans/reports), case study analysis, surveying and interviewing the relevant officers, focus group discussions with key stakeholders and so forth.

3.4. The consultant shall review the previous studies with similar scope that has been done by government and private institutions and adopt the best practices from those studies.

3.5. The consultant shall provide a detailed study implementation plan outlining all the steps involved in the design and implementation of the study, including a project time schedule and resource plan, and outlines of the instruction manuals for enumerators to be developed.

3.6. The consultant shall propose a suitable sampling strategy for the study. The consultant shall justify the appropriateness of the sample to the PSC. The sample should adequately represent various industry sectors and the total population. (The consultant shall refer an internationally accepted classification schemes such as International Standard Classification of Occupations (ISCO))

3.7. The consultant shall propose a suitable methodology to collect data for the study. The consultant shall collect data from primary, and secondary sources.

3.8. Consultant shall develop a suitable research instrument, and approval shall be sought from the PSC before the implementation.

3.9. The consultant shall pre-test the survey/interview questionnaire and re estimate the sample size. After the pre-test, if necessary, revise the questionnaire and documentation. If necessary, adapt the sample size to ensure that final results will be of statistical validity and representative. A test of data entry (data entry program and procedures) must also be included in the testing procedures.

3.10. The consultant shall find out through a study on how many information security professionals are qualified/certified/graduated during the last five years from both the government and private universities/institutes. The consultant is supposed to consider the total population.

3.11. The consultant shall find out through a study that how many individuals get the industry certifications on information and cybersecurity domain.

3.12. The consultant shall provide a total calculation on how many occupations are available for information security professionals in private and government sectors per year during last five years. These job positions should be taken from different sectors such as finance, defence, health, ICT, power and energy etc.

3.13. The consultant shall consider the diversities among the professionals such as gender, age and demographic profiles when producing the results.

3.14. Based on the analyzed data the consultant should be able to provide the industry sector vise demand of the information and cybersecurity professionals on deferent domains (E.g.: Application security, Network security, Mobile security)

3.15. Based on the analyzed data the consultant should forecast the supply and demand of the information security related job role at least for next five years.

3.16. The consultant should develop a five-year operational strategy to fill the gap between the supply and demand of information and cybersecurity professionals in the country.

3.17. The consultant shall enter collected data via database software. The software must be able to verify ranges and consistency of the data and generate reports indicating missing data, data outside of the accepted ranges, and inconsistent answers. Clean data records and verify that the sample is still sufficient for reliable statistics. The ownership of the database shall be remained with Sri Lanka CERT.

3.18. The consultant shall be responsible to implement all possible quality control measures in the study to ensure the quality, reliability and validity of data collected and analyzed.

3

3.19. Final study findings shall be in English. The report must contain descriptive statistics of all variables of the survey, cross tables, and graphs, as well as qualitative presentations. Selected variables should be presented by graphs and/or correlation measures, on thematic maps. A critical review of the methodology, realization, and results should be given, together with recommendations for improvement. The report must be submitted in electronic form and as a hardcopy.

3.20. The consultant shall deliver a presentation at Sri Lanka CERT|CC to present and discuss Final Report findings, when specified by Sri Lanka CERT|CC. These presentations should be delivered as validation presentations for the industry experts when necessary.

4. Qualification of Key Staff

4.1. Consultant is free to propose the number and structure of experts appropriate to his implementation approach, provided that the team properly covers the above mentioned functions. The suggested minimum number of staff, qualification and experience required for this assignment is presented in the table below. Additional marks will be allocated for the strength of the team proposed by the consultant.

4.2. Positions to cover other project functions must also be presented in the bid, including the number of staff, their input in terms of staff days, and their work schedule. Particular persons must be nominated according to their roles and responsibilities and their CVs must be included in the proposal. A description of an appropriate organization structure, team collaboration arrangements and project management functions must be included in the proposal.

Key Staff	Minimum Academic Qualification	Minimum Experience	Minimum Number of Assignments Conducted
Project Coordinator	Bachelor's Degree from a recognized university	Minimum 3 years demonstrated experience in managing research projects	At least 3 studies with similar scope
Chief Consultant	Master's Degree from a recognized university	Minimum 10 years of demonstrated experience in baseline study/ impact/outcome evaluation study. Demonstrated experience in conducting supply and demand assessments Demonstrated experience in designing research, developing surveys and qualitative questionnaires, collecting data through surveys and interviews/focus groups, analyzing data, interpreting data. Demonstrate experience in developing strategies and policies. Ability to interpret quantitative, qualitative and mixed methods data. Excellent oral and written language skills (Sinhala /Tamil and English) – Ability to write similar evaluation reports	5 national level studies specially in the areas of ICT. Experience in conducting 3 similar studies
Statistician cum Qualitative data analyzer	Master's degree in statistics/qualitative data from a recognized university	Minimum 5 years demonstrated experience in statistical analysis/qualitative data analysis and national level research/project evaluations	5 national level studies

Enumerators	Diploma or higher qualification from a recognized institute	Demonstrated experience in conducting face-to-face interviews and surveys − Excellent language skills in Sinhala, Tamil and English.	Participated in at least 5 studies

5. Key Deliverables and Payment Schedule

Duration of the assignment is 12 weeks.

5

Phase/ Reports	Task	Deliverable	Deadline	Payment
Inception Report	− Develop the Inception report	Inception Report including the work plan and the overall approach to the study	Contract date + Week 1	5%
Interim Report I	Develop the Conceptual Framework to assess the supply and demand gap	− Report including the detailed study approach, conceptual framework, research method, interview/survey questions, sampling strategy	Contract date + Week 3	5%
Interim Report II	Assess the Supply side	− Supply of information and cyber security professionals − Present findings	Contract date + Week 6	15%
Interim Report III	Assess the Demand side	Demand for information and cyber security professionals − Present findings	Contract date + Week 8	25%

Interim Report IV	Analyse the gap between the supply and the demand	Analyze the gap between the supply and the demand − Present findings	Contract date + Week 10	20%
Final Report	− Operational Strategy	− Final report proposing the strategy to fill the gap between the supply and demand of information and cyber security professionals in the country. − Present the report	Contract date + Week 12	30%

Annex 2: Demand Questionnaire

Assessment of the Demand for Cybersecurity Professional in Sri Lanka

In line with implementation of the National Information and Cybersecurity Strategy of Sri Lanka, Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT), the implementation agency of the strategy, has initiated a program to identify the supply and demand of cybersecurity professionals in Sri Lanka, and to develop a strategy to fill the demand and supply gap of cybersecurity professionals in the country.

The survey will be carried out in two phases. In the first phase, the demand of the Cybersecurity Professionals will be assessed by covering wide range of organizations including government organizations and organizations in the fields of IT, Manufacturing, Financial and Telecommunication. In the second phase, the supply of the Cybersecurity Professionals will be assessed by taking into account the number of professionals produced by the academic institutes.

The purpose of this questionnaire is to assess the demand of the cybersecurity professionals in Sri Lanka which will be assessed by taking into account the present and future demand for cybersecurity professionals of your organization. Sri Lanka CERT has awarded a contract to the Institute for Participatory Interaction in Development (IPID) to undertake this survey.

We kindly invite you to fill in the attached soft copy of the questionnaire and email to surveys@ipid.lk and pubudu@cert.gov.lk within two weeks. Alternatively, you may request for a hard copy of the questionnaire which will be delivered to you. Should you have any queries on this, please do not hesitate to contact, Mr. Amil Epa, the Survey Team Leader of the IPID through 0117219886 (Survey Hotline) / Email: surveys@ipid.lk or Mr. Pubudu Withanage, the Project Manager of Sri Lanka CERT through +94 769 812 716 / Email: pubudu@cert.gov.lk.

Sri Lanka CERT appreciates your kind cooperation and assistance provided in support of this important survey, which will be vital in formulating strategies to fill the demand and supply gap in the Country.

Thank you.

Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT)

Room 4-112, BMICH, Bauddhaloka Mawatha, Colombo 07

Section A: About the Institute

Optional Responses	
Name of the organization	
Name of the respondent	
Position of the respondent	
Contact Details (Mobile)	
Contact Details (E-mail)	

1. Year of establishment in Sri Lanka: ___________

2. Total number of employees: ___________ (Head Office and branches in Sri Lanka, including minor staff)

3. Location of the Head Office/ Country Office in Sri Lanka: ___________

4. Type of Organization (Major component)

Type of Organization	**Please Mark**	**Instructions**
ICT Company		*After question 05 move to **section B***
BPO/ BPM Company		
Government / Semi Government		*After question 05 move to **section C***
Private Sector (Non-ICT and BPO/ BPM)		
INGO/NGO/Not for Profit		
Academic (Educational Institute)		
Other (Specify) ………………………………………………..		

5. How are Cybersecurity operations handled by the Organization?

	Please Mark	**Name of the Company**
I. Handled Internally		*Not applicable*
II. Partly Outsourced – Local		

III.	Partly Outsourced – International		
IV.	Fully Outsourced – Local		
V.	Fully Outsourced – International		

5.1 If 'Fully' or 'Partly' outsourced, why?

Section B: The specific nature of ICT production/ Service:

1. Ownership/ Operations (Please select the most appropriate answer)

I.	Sri Lankan owned Company, conducting operations only in Sri Lanka	
II.	Sri Lankan owned Company, having branches / operations in Sri Lanka and other Countries	
III.	Owned by a Foreign Company, conducting operations only in Sri Lanka	
IV.	Owned by a Foreign Company, having branches / operations in Sri Lanka and other Countries	
V.	Joint venture, conducting all operations in Sri Lanka	
VI.	Joint venture, having branches / operations in Sri Lanka and other Countries	

2. Please Rank your Core Businesses by revenue. (Rank 1 - Highest to 5 - Lowest) This is for **ICT Companies only.** *(Multiple responses are accepted)*

I.	IT Services	
II.	Software Services	
III.	Software Products	
IV.	Technology, Hardware & Equipment: Communications Equipment	
V.	Technology, Hardware & Equipment: Technology, Hardware, Storage & Peripherals	
VI.	Technology, Hardware & Equipment: Electronic Equipment, Instruments & Components	
VII.	Telecom & Networking: Telecommunication	
VIII.	Telecom & Networking: Networking & Server Solutions	
IX.	Semiconductors & Semiconductor Equipment	
X.	Security Product/ Services Companies*	
XI.	Cybersecurity Management Services	
XII.	Cybersecurity Consulting	
XIII.	Other (Pls. specify)	

*OEM, system integrators, product distributors and resellers

Section C: Cybersecurity Practitioners / Professional

Please refer to all the **sections** and **questions** carefully, as the questions collect information on the current situation as well as future demands.

Cybersecurity Professional/ Practitioner: (Definition for the Assignment)
Staff who are responsible for securing the information systems /IT infrastructure (Software and Hardware) of an organization against/from web threats, malware, viruses, DoS attacks, phishing, etc.

6. What is the Cybersecurity staff (Professionals and Practitioners) workforce distribution in your organization?…………………(Total)

Note: *Enter number of staff, consider any employee assigned with a Cybersecurity role in the tables below. The staff with or without Academic and Professional Qualifications in Cybersecurity must be considered.*

A) *Full-time Cybersecurity Practitioners (Sole responsibility)*

	Nationality	Total	Female
Based in Sri Lanka	Sri Lankan		
	Foreign		
Based outside Sri Lanka	Sri Lankan		
	Foreign		

B) *Part-time Cybersecurity Practitioners (In-house staff, perform Cybersecurity requirements as part of their job description)*

	Nationality	Total	Female
Based in Sri Lanka	Sri Lankan		
	Foreign		
Based outside Sri Lanka	Sri Lankan		
	Foreign		

7. The number of **Cybersecurity Professionals/ Practitioners** by their qualifications

A. Academic Qualifications in Cybersecurity – Only for Sri Lankans (based in Sri Lanka and overseas)

Note: Please consider the qualifications which include cyber/ information and communication technology security related subjects as the main component of the 'highest qualification'.

When considering a person who has multiple qualifications, take <u>the highest academic qualification</u>. Please make sure that there is <u>no duplication</u> of the same person across multiple qualifications.

Academic Qualification (Cybersecurity or relevant discipline)	**Total**	**Female**
PhD in Cybersecurity		
Master's Degree in Cybersecurity		
Postgraduate Diploma in Cybersecurity		
Bachelor's Degree in Cybersecurity		
Bachelor's Degree in IT/Science; specialized in Cybersecurity		
Higher Diploma in Cybersecurity		
Diploma in Cybersecurity		
Certificate in Cybersecurity		
Other (Specify)………………………………		

B. Professional Qualifications in Cybersecurity (Count persons with both academic and professional qualifications / professional qualification only) – Only for Sri Lankans (based in Sri Lanka and overseas)

Professional Qualifications	**Total**	**Female**
Trade Certificates (Vendor Certificates) *		
Trade Certificates (Vendor Neutral Certificates) **		

Examples for Vender Certificates and Vender Neutral Certificates

- **Trade Certificates (Vender Certificates) - CISCO, AWS, Oracle, Microsoft*
- ***Trade Certificates (Vender Neutral Certificates) – CISA, CISM, CISSP, etc.*

C. Industry Experience in Cybersecurity Only for Sri Lankans (based in Sri Lanka and overseas)

Note: Count Staff in Cybersecurity related jobs only with experience in cybersecurity, but without academic and professional qualifications in cybersecurity. The staff may hold academic and professional qualifications in other fields.

	Total	**Female**
Only Industry Experience		

8. Age distribution of **Cybersecurity Professionals/ Practitioners** – Only for Sri Lankans (based in Sri Lanka and overseas)

Age Range		Number of Cybersecurity related staff	
		Total	Female
I.	18 – 24		
II.	25 – 34		
III.	35 – 44		
IV.	45 – 54		
V.	55 and above		
	Total		

Note: Total must tally with Question No. 06

9. Total experience of **Cybersecurity Professionals/ Practitioners** in related jobs only for Sri Lankans (based in Sri Lanka and overseas)

Experience		Number of Cybersecurity related staff	
		Total	Female
I.	Less than one year		
II.	1 - 3 Years		
III.	4 – 8 Years		
IV.	9 - 12 Years		
V.	More than 12 years		
	Total		

Note: Total must tally with Question No. 06.

Section D: Demand for Cybersecurity Professionals/ Practitioners

10. How many Cybersecurity Professionals/ Practitioners in each Job Category remained at the end of year 2020 and what is your demand for the years 2021 and 2022? *(In the case of one-person handling multiple jobs, please categorize it based on their primary responsibilities. Please make sure there is no duplication of the same person across multiple categories.)*

Job Category/ Designation		Base employment at the beginning of 2020		Demand for 2020	Joined During 2020		Left During 2020		Joined During 2021		Demand for 2021	Demand for 2022
		Total	Female	Total	Total	Female	Total	Female	Total	Female	Total	Total

Demanding Qualifications, Technical and Soft Skills

11. For the demanding job categories/designations for 2020 -2022, what are the minimum qualifications (Professional and academic) experience looked for? *(Please collect data for the same positions as mentioned in Q 10)*

Job Category/ Designation		Academic (Related to Cybersecurity)			Specific Professional Qualifications *(Related to Cybersecurity)*	Other Qualifications *(Please Specify)*	Average Experience in Cybersecurity *(Years)*	Salary in LKR* *(Please Refer Codes)*
		MSc/ Post-graduate	Bachelor's Degree	Diploma				

* Code 1 - Less than LKR 50,000. Code 2 – LKR 50,001 to 100,000 Code 3 - LKR 100,001 to 150,000
Code 4 – LKR 150,001 to 200,000 Code 5 - LKR 200,001 to 300,000 Code 6 – LKR 300,001 and above

12. For the demanding job categories/designations for 2020 -2022, what are the minimum Technical and Soft Skills looked for? (Use the numbers from the list below)

Job Category/ Designation		Technical Skills			Soft Skills		
		Skill 1	Skill 2	Skill 3	Skill 1	Skill 2	Skill 3

Skills List

	Technical Skills		**Soft Skills**
1	Incident Handling & Response	1	Leadership Skills
2	Security Information and Event Management (SIEM)	2	Passion for Learning
3	Information Security Audit & Compliance	3	Determined
4	Cybersecurity Analytics & Intelligence	4	Collaborative and Teamwork
5	Digital Forensics	5	Analytical, Inquisitive and Insightful
6	Identity & Access Management	6	Think Hyper Critically (Critical Thinking)
7	Firewall/IDS/IPS Skills	7	Consultative Skills
8	Intrusion Detection	8	Project Management Skills
9	Secure Application Development	9	Communication / Presentation
10	Advanced Malware Prevention	10	English Language
11	Mobile Device Security Management	11	Strong Analytical and Problem-Solving Skills
12	Data Management Protection	12	Excellent Communication
13	Network-based Threat and Vulnerability Assessments	13	Good Relationship Management
14	Incident Handling Processes and Procedures	14	Flexibility and Adaptability in the Face of Changing Priorities
15	Malware Analysis and Reversing	15	Ability to Evaluate and Manage Risk
16	Risk Analysis and Mitigation	16	Written Communication and Documentation
17	Device, Application and Operating System Hardening	17	Strong Research Skills
18	Vulnerability and Penetration Testing	18	Networking
19	Other 1 (Specify)	19	Adaptability
20	Other 2 (Specify)	20	Other (Specify)

Section E: Career Development and Employee Retention

13. What are the preferred means of skills development for career advancement within your organization for Cybersecurity staff?

	Means of Skills Development	**Rank**
1	Acquiring academic qualifications	
2	External short-term training courses	
3	Formal in-house training courses	
4	Acquiring professional qualifications	
5	On the job training/ Experience	
6	Industry awareness/ Exposure	
7	Other *(Specify other)*	

14. What are the practiced means of employee retention within your organization for Cybersecurity Practitioners / Professionals? *(Indicate the top three methods)*

	Practiced Means of the Retention Strategy	**Rank**
1	Good compensation plan	
2	Flexibility in hours, environment, dress code	
3	Incentives for gaining professional certification	
4	Challenging job	
5	Good work environment	
6	Training and development	
7	Job security	
8	Overseas exposure visit	
9	Medical insurance	
10	Clear career path	
11	Stability of the company	
12	Stock options/ Ownership of company	
13	Good employer – employee relationship	
14	Work from home facility, mobility	
15	Other (specify)	

Section F: Cybersecurity Budget

1. Cybersecurity as a percentage (%) of the Total Annual Budget allocated in 2019 to 2022?

Description	**2019**	**2020**	**2021**	**2022**
Cybersecurity and related expenses as a %				
a) Salary Cybersecurity Staff as a %				
b) Operations maintenance on cybersecurity as a %				

Annex 3: Supply Questionnaire

Assessment of the Supply for Cybersecurity Professional in Sri Lanka

In line with implementation of the National Information and Cybersecurity Strategy of Sri Lanka, Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT), the implementation agency of the strategy, has initiated a program to identify the demand and supply of cybersecurity professionals in Sri Lanka, and to develop a strategy to fill the demand and supply gap of cybersecurity professionals in the country.

The survey will be carried out in two phases. In the first phase, the demand of the Cybersecurity Professionals will be assessed by covering wide range of organizations including government organizations and organizations in the fields of IT, Manufacturing, Financial and Telecommunication. In the second phase, the supply of the Cybersecurity Professionals will be assessed by taking into account the number of professionals produced by the academic institutes.

The purpose of this questionnaire is to assess the supply of the cybersecurity professionals in Sri Lanka which will be assessed by taking into account the present and future of any Cybersecurity related programs of your organization. Sri Lanka CERT has awarded a contract to the Institute for Participatory Interaction in Development (IPID) to undertake this survey.

We kindly invite you to fill in the attached soft copy of the questionnaire and email to surveys@ipid.lk and pubudu@cert.gov.lk within two weeks. Alternatively, you may request for a hard copy of the questionnaire which will be delivered to you. Should you have any queries on this, please do not hesitate to contact, Mr. Amil Epa, the Survey Team Leader of the IPID through 0117219886 (Survey Hotline) / Email: surveys@ipid.lk or Mr. Pubudu Withanage, the Project Manager of Sri Lanka CERT through +94 769 812 716 / Email: pubudu@cert.gov.lk.

Sri Lanka CERT appreciates your kind cooperation and assistance provided in support of this important survey, which will be vital in formulating strategies to fill the supply and demand gap in the Country.

Thank you.
Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT)
Room 4-112, BMICH, Bauddhaloka Mawatha, Colombo 07.

A. About the Institute

Optional Responses	
Name of the organization	
Name of the respondent	
Position of the respondent	
Contact details (Mobile)	
Contact details (E-mail)	

15. Year of establishment in Sri Lanka: __________

16. Which category does your institution fall into? (Select the answer based on your registration/ ownership)

Institution	"x"
Government University	
Government Tertiary & Vocational Training Institute (e.g., NAITA, VTA)	
Private Degree Awarding Institution	
Registered Vocational Training Institute (Registered under TVEC)	
Professional Chapters / Bodies	
Professional Training Provider	
Other (Specify) ………………….	

17. Do you offer any ICT or related programs? (Multiple Answers) - If 'NO', do not continue.

Program	"x"
PhD	
Master's Degree	
Postgraduate Diploma	
Bachelor's Degree	
Higher Diploma	
Diploma	
Trade Certificates* (Vendor Certificates)	
Trade Certificates** (Vendor Neutral Certificates)	
Other (Specify)………………………………………………..	

**Trade Certificates (Vender Certificates) - CISCO, AWS, Oracle, Microsoft*

*****Trade Certificates (Vender Neutral Certificates) – CISA, CISM, CISSP, etc.*

a. Does your organization offer any Cybersecurity related programs? If **'NO',** do not continue after Question 3.2.

Cybersecurity related Courses: (Definition for the Assignment)

Courses/ Programmes that offer a combination of computer expertise and Cybersecurity education. The study courses that contain a minimum of one third of the subject matter (Course Units/ Modules) on cybersecurity will be considered as a cybersecurity related course.

Program	
PhD	
Master's Degree	
Postgraduate Diploma	
Bachelor's Degree	
Higher Diploma	
Diploma	
Trade Certificates (Vendor Certificates)	
Trade Certificates (Vendor Neutral Certificates)	
Other (Specify) ………………………………………………..	

**Trade Certificates (Vender Certificates) - CISCO, AWS, Oracle, Microsoft*

*****Trade Certificates (Vender Neutral Certificates) – CISA, CISM, CISSP, etc.*

b. If your organization offers any ICT programs but not Cybersecurity related programs, what are the main reasons?

B. Output of Cybersecurity Professionals/ Practitioners (Consider Sri Lankan citizens only)

18. How many students have ***completed*** and are ***expected for completion*** according to the education qualification levels in Information Security related programs as given below?

Note: Forecast for 2021 - Please consider those who have completed and are expected to complete on or before December 2021.

Academic and Professional Qualification	**Completed**						**Forecast**		
	2018		2019		2020		2021	2022	2023
	Male	Female	Male	Female	Male	Female	Total	Total	Total
PhD									
Master’s Degree									
Postgraduate Diploma									
Bachelor’s Degree									
Higher Diploma									
Diploma									
Trade Certificates (Vendor Certificates)									
Trade Certificates (Vendor Neutral Certificates)									
Other (Specify)									

1. *Only courses that have at least* ***500 contact hours*** *can be counted as an* ***Advanced Diploma***
2. *Only courses that have at least* ***400 contact hours*** *can be counted as a* ***Diploma***

Examples for Vender Certificates and Vender Neutral Certificates

- *Trade Certificates (Vender Certificates) - CISCO, AWS, Oracle, Microsoft*

- *Trade Certificates (Vender Neutral Certificates) – CISA, CISM, CISSP, etc.*

C. Courses Offered, Cybersecurity related Course Units and Enrolments (after dropouts)

19. Please list the courses offered, the number of students who completed the courses and the expected completion for 2021 to 2023

Note: Forecast for 2021 - Please consider those who have completed and are expected to complete on or before December 2021.

Name of the Program	**Units (For Degrees and above)**				**Completed**						**Forecast**		
	Total Units (Modules)	Total Credits	Cybersecurity Units (Modules)	Total Cybersecurity Credits	2018		2019		2020		2021	2022	2023
					Male	Female	Male	Female	Male	Female	Total	Total	Total

Example for name of the Program

- BSc. (Hons) in Information Technology - Cybersecurity
- MSc. in Information Security
- Master of Philosophy (MPhil) (Cybersecurity)

D. Technical and Soft Skills

20. Please list the courses offered and the **Technical and Soft Skills** taught / trained during the programs. (Use the number given in the list below)

Name of the Program	**Skill Provided**					
	Technical Skills			Soft Skills		
	1	2	3	1	2	3

Skills List

	Technical Skills		Soft Skills
1	Incident Handling & Response	1	Leadership Skills
2	Security Information and Event Management (SIEM)	2	Passion for Learning
3	Information Security Audit & Compliance	3	Determined
4	Cybersecurity Analytics & Intelligence	4	Collaborative and Teamwork
5	Digital Forensics	5	Analytical, Inquisitive and Insightful
6	Identity & Access Management	6	Think Hyper Critically (Critical Thinking)
7	Firewall/IDS/IPS Skills	7	Consultative Skills
8	Intrusion Detection	8	Project Management Skills
9	Secure Application Development	9	Communication / Presentation
10	Advanced Malware Prevention	10	English Language
11	Mobile Device Security Management	11	Strong Analytical and Problem-Solving Skills
12	Data Management Protection	12	Excellent Communication
13	Network-based Threat and Vulnerability assessments	13	Good Relationship Management
14	Incident Handling Processes and Procedures	14	Flexibility and Adaptability in the Face of Changing Priorities
15	Malware analysis and reversing	15	Ability to Evaluate and Manage Risk
16	Risk Analysis and Mitigation	16	Written Communication and Documentation
17	Device, Application and Operating System Hardening	17	Strong Research Skills
18	Vulnerability and Penetration Testing	18	Networking
19	Other 1 (Specify)	19	Adaptability
		20	Other (Specify)

E. Resource Panel

21. What is the lecturing experience of your institute's lecturers? (**Cybersecurity related courses delivery only**)

a) By Level of engagement

Level of Engagement		0 – 1 Year experience		1 – 3 Year experience		3 – 8 Year experience		8 - 12 Year experience		Above 12 Year experience	
		Total	Female	Total	Female	Total	Female	Total	Female	Total	Female
1.	Full-time										
2.	Part-time										

b) **By Academic qualification in Cybersecurity** (Count persons / lecturer once by his/ her highest Academic qualifications in Cybersecurity)

Academic Qualification	0 – 1 Year experience		1 – 3 Year experience		3 – 8 Year experience		8 - 12 Year experience		Above 12 Year experience	
	Total	Female	Total	Female	Total	Female	Total	Female	Total	Female
1. PhD										
2. Masters/ Postgraduate										
3. Bachelor's Degree										
4. Other										

c) By **Professional qualifications in Cybersecurity** (Count persons / lecturers with both academic and professional qualifications and professional qualification only)

Qualifications	0 – 1 Year experience		1 – 3 Year experience		3 – 8 Year experience		8 - 12 Year experience		Above 12 Year experience	
	Total	Female	Total	Female	Total	Female	Total	Female	Total	Female
Academic and professional qualifications										
Professional qualifications only										

d) By **Industry Experience in Cybersecurity** (Count persons / lecturers only with Industry Experience; the lectures may hold other academic and professional qualifications)

Experience	0 – 1 Year experience		1 – 3 Year experience		3 – 8 Year experience		8 - 12 Year experience		Above 12 Year experience	
	Total	Female	Total	Female	Total	Female	Total	Female	Total	Female
Industry Experience only										

Annex 4: Key Informant Interview Guidelines and Interview List

Assessment of the Supply for Cybersecurity Professionals in Sri Lanka: Key Informant Interview (KII) Guidelines

Introduction to the Survey:
In line with implementation of the National Information and Cybersecurity Strategy of Sri Lanka, Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT), the implementation agency of the strategy, has initiated a program to identify the demand and supply of cybersecurity professionals in Sri Lanka, and to develop a strategy to fill the demand and supply gap of cybersecurity professionals in the country.

The survey will be carried out in two phases. In the first phase, the demand of the Cybersecurity Professionals will be assessed by covering wide range of organizations including government organizations and organizations in the fields of IT, Manufacturing, Financial and Telecommunication. In the second phase, the supply of the Cybersecurity Professionals will be assessed by taking into account the number of professionals produced by the academic institutes.

The purpose of Key Informant Interviews:
The purpose of Key Informant Interviews is to conduct interviews with key professionals in this field and obtain their points of view in the demand and supply of cybersecurity professionals in Sri Lanka. This will be assessed by taking into account the present and future environment of Cybersecurity in Sri Lanka. Sri Lanka CERT has awarded a contract to the Institute for Participatory Interaction in Development (IPID) to undertake this survey.

KEY INFORMANT INTERVIEW QUESTIONS

The General Environment of Cybersecurity:

1. Cybersecurity situation in SL in relation to the global context
2. What are the barriers that prevent the growth of Cybersecurity in SL?
3. Outsourcing Cybersecurity and threats
   a. Why do they outsource internationally /locally? *(Specially government sector)*
   b. What are the opportunities and threats?
   c. What can be done to minimize threats?

The Roles of Various Stakeholders in Cybersecurity in Sri Lanka:

4. What role can the Government play in CS in SL?

5. What role can the IT industry play in SL?
6. What role can the private sector play?
7. What role can the training service providers (Universities) play?

The Supply of Cybersecurity Professionals in Sri Lanka:

8. Is the current supply of CS professionals and quality sufficient?
9. Why are the numbers of students for CS courses low?
10. What can be done to increase the quality?

Cybersecurity Policies and Legal Framework in Sri Lanka:

11. What is your opinion about the policy framework and legal framework on CS in SL?
12. What can be done to strengthen this further?

Comments and Suggestions:

LIST OF KEY INFORMANTS:

1. Mr. Sujith Christy - Director - Layers-7, CISO John Keells Holdings
2. Mr. Waruna Sri Dhanapala - Additional Secretary (Regional Administration
3. Reforms) at State Ministry of National Security, Home Affairs & Disaster Management
4. Dr. Rasika Dayarathna - Senior Lecturer, University of Colombo
5. Mr. Sathish Bowatta - Lead Engineer, LSEG Technology
6. Air Cdre. (Rted.) T.G.J. Amarasena - CEO, Sri Lanka CERT
7. Mr. Jeewapadma Sandagomi - Senior General Manager ERM, Mobitel (Pvt) Ltd
8. Mr. Mohan Chathuranga - Deputy General Manager – IT Governance of MAS
9. Holdings, Sri Lanka and Director - Cyber Labs Pvt & Membership Director, Co-Chair - Cybersecurity Centre of Excellence at SLASSCOM
10. Mr. Rahal Jayawardene - President - Corporate Development & Cybersecurity at
11. MillenniumIT ESP, President Cybersecurity Centre of Excellence CSCx - SLASSCOM
12. Mr. Janaka Jayalath - Deputy Director General - Tertiary & Vocational Education
13. Commission
14. Mr. Kavinga Abewardana - Lecturer - Sri Lanka Institute of Information Technology
15. Mr. Jayantha Fernando - Director & Legal Advisor at ICT Agency of Sri Lanka