

Addressing Cybersecurity Skill Shortages in the GCC Region

March 2021



Table of Contents

- Acknowledgments..... 4
- Introduction 5
 - Importance of Cybersecurity Skills for GCC Countries..... 5
 - Problems Facing GCC countries in Skills Acquisition..... 5
- Research Approach 7
- Executive Summary..... 8
 - Main Challenges Facing Cybersecurity Professionals 8
 - Assessment of Skills Gaps in the Market 8
 - Bridging the Skills/Experience Gap 9
 - The Struggle to Retain Talent 9
- Detailed Findings..... 10
 - 1. Challenges Facing Cybersecurity Professionals in the GCC..... 10
 - 2. Assessment of Skills Gaps in the Market 11
 - 3. Optimizing Training Initiatives & Bridging the Experience Gap 17
 - 4. Retaining Cybersecurity Talent 18
 - 5. Learning from Other Markets 19
- Conclusion..... 22
 - Asserting Cybersecurity functions’ Influence within Organizations 22
 - Nurturing Cybersecurity Talent Requires Focus on Soft Skills 22
 - Bridging the Experience Gap by Offering Hands on Training Initiatives 22
 - Retention Through a Holistic and Personalized Approach 23
- Way Forward..... 24
- Appendix I: List of Cyber Skills 25
- Appendix II: References 28
- Appendix III: Draft Questionnaire 30



Acknowledgments

This survey was conceived and executed by the UK Gulf WIC Fellowship Skills Syndicate Group who identified the benefits that the insights obtained through this survey would bring to the region, designed an approach that was comprehensive, valid, and achievable, and personally conducted all the interviews and data collection.

We would like to thank all the members of the Syndicate Group who gave so freely of their expertise and worked so tirelessly to create and deliver this valuable resource for the region. Special thanks go to:

- Dr. Haya Almagwashi, King Abdulaziz University, KSA
- Eng. Haifa Nasser Al-Shabib, Gulf Cooperation Council.
- Nahla Al-Balushi, Information Security Manager Central Bank of Oman.
- Ruaa Al-Jassar, Cybersecurity Training & Awareness, Kuwait
- Eng. Sara Al-Khelaifi, Qatar Central Bank, Qatar
- Eng. Maram Ali AlMahameed, Artifact Analyst, National Cybersecurity Center, Bahrain

Introduction

Importance of Cybersecurity Skills for GCC Countries

In recent times, the cyber threat landscape has expanded significantly, with organizations now up against a wider range of threats, from attacks on critical infrastructure, denial of services and digital sabotage to online influence operations which highlights the vulnerable nature of information systems. The Gulf Cooperation Council (GCC)—comprising of Bahrain, Kuwait, Oman, Qatar, United Arab Emirates and Saudi Arabia—has been particularly vigilant especially after events of 2011 which demonstrated the new dangers emanating from digital communication (Shires & Hakmeh, 2020). For this reason, cybersecurity resilience has been identified as essential within the GCC region, particularly with regard to countries being prepared to detect, respond to, and prevent future cyberattacks.

Over the last few years, there has been a further increase in cyber-attacks within the GCC region. Both the government and the private sector have been targets of malicious attacks, including crypto-jacking, ransomware, and virus attacks. Some of the major attacks include the Kuwait Ministry of Interior, the Qatari news agency, and the Saudi Aramco attacks in 2017 (Chandra, Sharma, & Linqet, 2019). The UAE stated that there were at least 86 cyber-attacks within the country in 2018 with the main one being the data breach of ride-sharing service, Careem, which resulted in the exposure of data of over 14 million people. Additionally, the development of smart cities increases the likelihood cyber-attacks. Such cities have resulted in the creation of a highly innovative economy that would be placed under threat without proper cybersecurity (Chandra, Sharma, & Linqet, 2019). The GCC has also been wary of attacks that may lead to disruption of the flow of oil and gas considering that the energy sector represents a significant source of income for the countries.

Problems Facing GCC countries in Skills Acquisition

With the field of cybersecurity growing in importance globally, cybersecurity personnel are in great demand. The *ISC² Global Information Security Workforce Study 2015* predicted that there would be a shortfall of 1.5 million cybersecurity personnel by 2020¹. By 2020, however, ISC² was reporting the shortfall to have more than doubled to 3.1 million². The takeaway message from this research is that despite efforts to increase

¹ ISC². (2015). *Global Information Security Workforce Study*.

² ISC². (2020). *Global Information Security Workforce Study*.

numbers of professionals, the increase in cyber-attacks means the gap is still widening. According to Shires (2018), the GCC countries have been hosts to numerous cybersecurity conferences in the Middle East. Cybersecurity concerns of these countries are in the same range with those of other wealthy nations that have high internet connectivity and differ from those of their neighbors that still have underdeveloped internet connectivity (Shires, 2018). Despite this, the countries have policies hampered by unclear content on cybersecurity expertise. The cybersecurity professionals need a wide range of skills such as communication, data analytics, compliance and organizational psychology (Shires, 2018). They also require expertise in information technology.

Dawson and Thomson (2018) state that the social traits of the cybersecurity workforce have been ignored despite the increasing role of social networking in instigating political unrest. Most human resource managers rarely place emphasis on understanding a person's social traits when considering hires in cybersecurity (Dawson & Thomson, 2018). They view social information as part of the data points in cyber operations and fail to recognize it as an indicator of a person's likely success when working as part of cybersecurity team.

This paper will shed light on the main challenges as perceived by professionals working in the field within the GCC region. The research will go on to focus on understanding current training priorities as well as identifying the key skills needed to propel the influence of cybersecurity within organizations. The paper will also examine professionals' current perceptions on existing training plans on a national and regional level and how those can be enhanced to retain employees and yield positive returns on the professionals themselves as well as the wider business and national digital ecosystems.

Research Approach

In order to understand the state of cybersecurity in the region—specifically when it comes to skills gaps and shortages—16 qualitative in-depth interviews with professionals within the field were conducted. These interviews were one-on-one to allow the moderator to probe and understand in-depth insights and to ensure the respondents felt comfortable to share their opinions and experiences in a private setting. This was particularly important in this context given the sensitivity of the topic.

Interviews included a wide range of professionals in different roles across various sectors. Interviews spanned the entirety of the GCC covering KSA, UAE, Qatar, Oman, Bahrain and Kuwait. The paper focusses on overall cybersecurity skills gaps within the region rather than independently studying each GCC state. Ultimately, the purpose of this effort is to draw conclusions based on the collective experiences and encounters to form an overall view of the main challenges facing cybersecurity specifically when it comes to training and competency building.

Executive Summary

Main Challenges Facing Cybersecurity Professionals

There are a multitude of different challenges currently facing those working in cybersecurity and they are mostly linked with the relative immaturity of the field. First and foremost, the newness of the field coupled with the rapid advancements and digitization currently underway are contributing to the evident skills gap in the market, which, in turn, is putting a huge strain on existing talent. Furthermore, cybersecurity professionals are taking on very demanding roles and are often expected to work around the clock, which contributes to the high levels of burn out witnessed amongst professionals working in the field.

Another main challenge brought on by limited familiarity is the internal disconnect often felt by people assuming these roles as they struggle to integrate into the wider company structure. This also translates into them feeling overlooked when it comes to organizations' attempts to put in place appropriate development and training plans.

Assessment of Skills Gaps in the Market

While professionals stressed the importance of having a well-rounded cybersecurity team that is proficient across a wide range of cybersecurity skills, they highlighted incident response and threat management as two of most crucial skills needed within this field. Both skillsets are paramount in mitigating cybersecurity threats faced by an organization and minimizing the financial, reputational and data losses that accompany a security breach. Furthermore, professionals stressed the importance of cybersecurity governance specifically in relation to risk assessment which allows the organization to efficiently allocate efforts to mitigate appropriate threats.

Nonetheless, technical skills in isolation are not enough to equip someone to deal with the demands of the role. The more successful candidates often possess other competencies that facilitate their roles and fortify their impact within their organizations. This includes soft skills like critical and analytical thinking which allow professionals to mobilize their technical knowledge and apply it to real cybersecurity threats as they occur. Other key competencies include communication and emotional intelligence which are important skills to have—especially as someone climbs up the career ladder—because this allows them to bridge the communication gap they often face with other stakeholders within the organization.

Bridging the Skills/Experience Gap

The majority of interviewed professionals emphasized the importance of knowledge sharing as a tool to bridge the experience and skills gaps currently prevailing in the field. Knowledge sharing is not only seen as crucial to equip new entrants to the field, with the knowledge needed to kick off their careers, but it is also important when it comes to improving an organization's overall resilience and mitigating cyber threats.

Furthermore, practical hands-on experience, that is either acquired on the job or through simulated incidents at virtual and physical labs, was deemed essential. Most agreed that despite the importance of acquiring solid theoretical knowledge the only way to master a skill is to experience it first-hand. That said, some noted that as it currently stands emphasis on practical training lags behind and that more effort and investment is needed in order to expose professionals to simulated real-life scenarios even prior to them joining the field.

The Struggle to Retain Talent

Given the skills shortage, it's crucial for organizations to keep employee turnover as low as possible. However, as it currently stands, due to limited understanding of the field, companies struggle to retain and to keep those working within their organizations satisfied and motivated. While financial incentives were cited by many to be important when it comes to motivating and retaining professionals in the field, they also highlighted that these incentives are not enough in isolation. Motivating cybersecurity professionals requires a multidimensional approach that combines monetary rewards with clear professional development prospects as well as a built-in recognition system. Also, many noted that a one size fits all strategy is not sufficient and that in order to retain cybersecurity talent, it is crucial for organizations to invest the time and energy to understand what drives each individual working within their cybersecurity team.

Detailed Findings

1. Challenges Facing Cybersecurity Professionals in the GCC

Overworking as Major Contributor to Burn Out

Given the nature of the role, cybersecurity employees are expected to be on call 24/7 and be ready to tackle any occurring incident or breach at a moment's notice. Working in such a demanding and high-pressure environment often contributes to excessive burn out amongst an already limited pool of available skills. As reported by one interviewee, the issue is further exacerbated by the fact that university graduates embark on this career path, not fully understanding the level of commitment needed when accepting a cybersecurity role within an organization. This is, in part, due to their limited exposure to on-the-job training prior to starting their careers within the field. Nonetheless, if these roles become notorious for their incessant workload, then there is the potential risk of deterring future talents as well as the inability to retain existing ones.



“Cybersecurity staff are like medical doctors. They should be ready to receive a call at any time” – Cybersecurity Professional

It is also worth noting that the demanding nature of the role makes it particularly challenging for women working in this sector. With more responsibilities outside the workplace, women often feel unable to meet the demands of the job, which is one of the contributing factors to lower female participation in this field. According to a 2020 study by ISC², just over half of cybersecurity professionals surveyed (51% worldwide, both men and women) perceive the percentage of women in the field to have risen over the last five years. While there are regional variations in the perceived increase of women participation in the cybersecurity workforce, the data in the study suggests that the actual percentage of women in the cybersecurity workforce has remained close to constant over the last three years, with women making up approximately 25% of study participants globally³.

The Alienation of Cybersecurity Functions

More on the business side—and perhaps the most important challenge facing cybersecurity functions—is the limited integration of cybersecurity on a company-wide level. While many cybersecurity departments currently operate in silos, increased digitization dictates an expansion of the role that cybersecurity personnel assume within an organization.

³ ISC² (2020). *Global Information Security Workforce Study: Cybersecurity Workforce Study, 2020*

Achieving this requires alignment on an organizational level with management acknowledging the importance of embracing cybersecurity by design and for employees to recognize that they all play a role when it comes to safeguarding their organization's information assets.

Nonetheless, this is not always the case; many of the interviewed professionals reported that people working in the field often face challenges when it comes to garnering support from different functions across the organization. Barriers to collaboration are often linked to lack of awareness on the importance of cybersecurity and impending threats or, in some cases, resistance to submit to a perceived additional layer of supervision on their work. Some experts reported that a lot of the breaches they deal with on a regular basis are in fact due to the negligence of company employees when it comes to following standard cybersecurity protocols. On a larger scale, the challenge also lies in winning management support when it comes to embedding cybersecurity in company culture by design rather than being perceived as an independent business function. Ultimately, the difficulty in acquiring support from internal stakeholders is as a primary hindrance for people working in this field.



People don't believe in the importance of cybersecurity until an incident happens" – Cybersecurity Professional

Training Shortcomings

Given the technical nature of the role, some cybersecurity personnel in the region report feeling overlooked when it comes to their company's training and development plans. The lack of understanding of the technical nature of the role makes it very difficult for management and HR personnel to put in place solid training plans that contribute to the professional development of their cybersecurity employees. Furthermore, some interviewed professionals working in the field also highlighted the lack of funding as a major obstacle to addressing the skills gap.

It is also important to note, that most professionals highlighted that training should not only be focused on technical aspects of the job; professionals in the field are also calling for increased emphasis on developing important soft and workplace skills that are just as crucial when it comes to fortifying the caliber of professionals working within this field. Only by investing in cybersecurity employees' technical and professional development will they be empowered to play an integral role in driving digital transformation.

2. Assessment of Skills Gaps in the Market

Closing the Skills Gap

Carr (2016) explains that countries need to take a holistic view of the existing cybersecurity skills gap. The holistic view is important in ensuring that they target both technical and non-technical skills (Nobles, 2018). While the myth is that cybersecurity involves only those in the computer science and information technology fields, the reality is that it is a multidisciplinary field where people need both technical and non-technical skillsets. Higher education institutions in the GCC countries should be aligned with the skills requirements within the countries (Griffith, 2017). That way, it will be easy to produce more highly qualified cybersecurity professionals.

Further, the GCC countries should promote industry-school partnerships. There is a need to ensure that the skills taught within the schools are readily applied within the industry. Carr (2016) states that a greater collaboration with universities is likely to reduce the mismatch that currently exists between the graduates and industry needs. Considering the scarcity of cybersecurity professionals, it is important to ensure that the few who are trained have skills matching the needs of the industry.

To this end, recently a recognizable effort was made by Saudi Arabia with the launch of two key frameworks that work as guidelines for raising the quality of education and training in cybersecurity for the supply and demand. The first framework is (SCyWF)⁴, which identified 40 job roles in cybersecurity and for each job role defined the relevant tasks and needed knowledge and skills and abilities for that role. The second framework (SCyber_Edu)⁵ provides a description of the minimum requirements and knowledge units that should be covered by higher educational programs in cybersecurity in Saudi Arabia, spanning from Diploma to Doctoral degrees.

With that in mind, the following sections outline the technical and non-technical skills that are considered to be the most important by professionals working in the field.

Highlighting the Need for Cybersecurity Related Technical Skills

Cybersecurity roles often require a wide range of skills that are intricate and specific to the field, including skills like penetration testing and cybersecurity architecture. These roles also sometimes demand more general IT and business skills, such as project management, risk assessment, network engineering, SQL, system administration, and technical support. Considering this, interviewed professionals were asked to prioritize

⁴ The Saudi Cybersecurity Workforce Framework (SCyWF),2020.

⁵ The Saudi Cybersecurity Higher Education Framework (SCyber_Edu),2020.

five key training areas from a list of fifteen core cyber skills based on their perceived need within their organizations.

1. Vulnerability Assessment
2. Penetration Testing
3. Cybersecurity Architecture
4. Incident Response
5. Digital Forensics
6. Cybersecurity Operations
7. Cybersecurity Network Operations
8. Threat Intelligence Management
9. Cybersecurity Governance
10. Cybersecurity of Industrial Control Systems and Operational Technologies (ICS/OT)
11. Cybersecurity Systems and Applications Development
12. Cybersecurity Research
13. Cybersecurity Training and Awareness
14. Communication and Knowledge Transfer
15. Leadership

Table 1. Skills Categories Shown to Interviewees⁶

For the vast majority of interviewed professionals, Threat Intelligence Management came up as one of the most important technical skills. Threat Intelligence Management focuses on the analysis and collection of information on both possible and present cyber-attacks that jeopardize the security of an organization. It is a proactive and preemptive security measure that prevents security breaches, and safeguards an organization from potential financial or data losses.

Incident Response was also amongst the perceived most needed skills for people working within this field. This particular skill involves the effective implementation of the methodology through which organizations choose to respond to a cyber-attack. Effective Incident Response aims to reduce the damage inflicted as a result of any given breach, and facilitates swift recovery. With that in mind, most professionals stressed the importance of being able to instinctively detect and respond to security incidents to mitigate business risks including loss of data, reputational risks, and potential losses in revenue.

Another key area of focus that emerged was cybersecurity governance. This particular skill encompasses multiple competencies, including the ability to perform cybersecurity related impact and risk assessments, developing and applying appropriate cybersecurity policies as well as skills in conducting cybersecurity audits or compliance reviews of

⁶ Refer to appendix for detailed descriptions of skills

technical systems. One interviewed expert noted that governance specifically needs to be a topic that is addressed on a national level rather than only an organizational level.

While all sub-skills were deemed necessary, special emphasis was placed on governance in relation to risk assessment. One interviewee noted that risk assessment is crucial when it comes to prioritizing the multiple threats faced by an entity at any given time. This is done by mapping out the risks based on vulnerability and probability as well as impact, in order to be able to allocate efforts efficiently to mitigate appropriate threats.

Most of those interviewed also placed at least one skill pertaining to leadership or cybersecurity training and awareness at the top of their priority lists. What these skills have in common is their importance for disseminating cybersecurity related information, processes, or guidelines across an organization. They require collaboration with multiple stakeholders either to ensure business continuity or further reinforce the role of cybersecurity on a strategic company level. Investing in this sort of skill building will ultimately empower cybersecurity professionals within their organizations.



Through raising awareness, we simplify the concept of “cybersecurity” and make it less intimidating for non-technical people.”

It is also worth noting that interviewed professionals working within the ICT sector all agreed that penetration testing should be a priority area of focus. Penetration testing, which is sometimes referred to as “ethical hacking”, involves running simulated cyber-attacks against a company’s computer system to check for inherent vulnerabilities that can be exploited in case of a real cyber-attack. More importantly, it uncovers the degree of damage that could be done if these vulnerabilities were exploited. This, of course, comes as no surprise considering the degree of damage that can be inflicted on a national, business, and personal level in the case of any breaches committed on communication networks in a given country. This highlights the importance of being preemptive in identifying imminent threats.

Ultimately, most interviewed professionals stressed the importance of all listed skills and highlighted that for the most part they are all interlinked. So, having special expertise pertaining to each competency within a team is essential to ensure the cybersecurity function within an organization is running seamlessly and effectively and playing its role of protecting the organization from cyber threats.

Highlighting the Need for Well Rounded Individuals Working in the Field

Being hired as a cybersecurity expert requires more than just possessing a high level of technical skill. The more successful candidates often possess other competencies that facilitate their roles and fortify their impact within their organizations. This in no way diminishes the significance of technical skills, but rather emphasizes the importance of not seeking them in isolation. With that in mind, interviewed cybersecurity professionals all expressed the need for proper training for the below mentioned skills at a university level and called for the integration of core competency building in university curricula.

As perceived by professionals within the field, the most important soft skills needed to succeed in cybersecurity roles are analytical and critical thinking skills. Only by being able to quickly draw conclusions and design appropriate responses, will cybersecurity professionals be successful in safeguarding their organizations from potential threats. These skills correlate very closely with multiple technical skills cited in the earlier section of the paper, including incident response, threat intelligence management and cybersecurity architecture. It is those skills that allow people to mobilize their technical knowledge in a constructive manner and to effectively tackle incidents and mitigate threats as they occur.

Furthermore, with cybersecurity playing a bigger role across the organization and due to increased collaboration between internal stakeholders, it is paramount that cybersecurity professionals possess solid communication skills which enable them to articulate technical jargon in a way that resonates with non-technical internal stakeholders. This becomes particularly important as someone climbs the career ladder and starts assuming strategic leadership roles. As mentioned earlier in the paper, limited efforts in fostering better communication skills are currently contributing to professionals' inability to exert their influence within their organizations.



Security is no longer a function of its own. It is a function that should be integrated at stage zero and across all the aspects of business operations. We are no longer an IT function; we are a business function and that's why we really need to work on our communication" – Cybersecurity Professional

Emotional intelligence was also cited as a key competency that should be harnessed and nurtured amongst cybersecurity professionals. On the one hand, this particular skill allows cybersecurity personnel to have a better grasp of how to influence people around them as well as understand what messages to focus on when it comes to igniting interest in the topic and affecting organizational behavior change. On the other hand, this skill also helps when it comes to safeguarding the organization against possible internal breaches. By possessing higher awareness of people's behaviors and attitudes,

professionals will be better equipped to detect possible internal breaches or risks prior to their occurrence.

Finally, further building on the importance of the evolving role of cybersecurity functions to propel e-business transformations, business acumen among cybersecurity professionals is indispensable. To reference *ISACA's State of Cybersecurity 2019 report*⁷: "Currently, the most-prized hire in a cyber security team is a technically proficient individual who also understands business operations and how [cybersecurity] fits into the greater needs of the enterprise".

Assessment of Current Training Efforts

Organizational Training Efforts

Most interviewed professionals reported three main components incorporated within their organization's cybersecurity training plans. Certifications were referenced by many as essential training tools, and this is often the formal measure through which organizations base their evaluation of any given cybersecurity employee. This is particularly important when an employee wants to hone their skills in a specific area of cybersecurity or develop a specific specialization.

But what was especially striking was the degree by which professionals emphasized the importance of practical hands-on experience that is either acquired on the job or through simulated incidents at virtual and physical labs. Most agreed that despite the importance of acquiring solid theoretical knowledge the only way to master a skill is to experience it first-hand.

For fresh graduates and new hires specifically, professionals also underscored the importance of knowledge transfer, shadowing, and job rotations when it comes to training new people. Some professionals even cited having proper knowledge management systems that focus on the proper dissemination and sharing of knowledge and expertise across different roles and seniority levels within the cybersecurity function.

Regional/National Training Efforts

A lot of the recollected regional and national training efforts pertained to initiatives focused on university students and fresh graduates as well as school students. Cited initiatives mostly included hackathons and competitions targeting young talent and the main aim is to raise awareness about possible careers within cybersecurity and attract

⁷ ISACA. 2019. *State of Cybersecurity 2019 - Part 1: Current Trends in Workforce Development*.

young talent to pursue this path. That is not to say that more advanced training or academies are not available but rather to highlight that entry level training and initiatives were the most salient.

3. Optimizing Training Initiatives & Bridging the Experience Gap

As it currently stands, professionals working in the field have the option of pursuing a wide range of different certification options to hone their technical skills. All interviewed professionals agreed that companies should play an important role in facilitating these opportunities. Some noted that it is also important that people working in the field are also afforded the time to invest in themselves and pursue those training opportunities, which is not always possible given the demanding nature of the job.

Nonetheless, the lack of technical and soft skills and shortcomings in training efforts are not perceived to be the only issues when it comes to cybersecurity professionals. In fact, given the immaturity and fast-paced nature of the field, there is also an evident gap when it comes to professionals' experience in dealing with all sorts of security threats and breaches.

The overwhelming majority of interviewed professionals stressed the importance of knowledge sharing as a tool to bridge gaps in cyber security experience. Knowledge sharing was perceived through two distinct lenses, the first pertaining to equipping new entrants with the knowledge needed to kick off their careers within the field while the latter focuses on knowledge sharing to improve overall organization's resilience when it comes to mitigating cyber threats.

Zooming in on the first angle, the main challenge faced by companies when hiring new talent is often their lack of practical experience. This in turn requires companies to invest a substantial amount of time preparing and getting new talent acquainted with job requirements and protocols. To combat this issue, organizations often have mentoring and shadowing programs for their new joiners. Furthermore, some also resort to exposing new entrants to case studies of previous incidents in order to give fresh graduates a chance to put their knowledge to use without jeopardizing the organization's operations. Nonetheless, many expressed that this phase is often time consuming and can be more streamlined if more focus is placed on exposing new talent to real-life scenarios even prior to them joining the professional world.



In university curricula students are taught the theoretical aspect to security but what is missing is the link when it comes to how to implement what they

*have learned in real life scenarios and when facing real cyber threats.” –
Cybersecurity Professional*

Moving on to the other side of the equation, knowledge management is also crucial when it comes to equipping the organization with the knowhow to deal with the ever-evolving cyber-threats. This is often done through knowledge sharing sessions between employees in order to give them a chance to learn from each other’s experiences and add to their library of expertise on incident response without having witnessed each incident firsthand. Some even highlighted the importance of this type of knowledge sharing on a cross-organization and even cross-country level. Nonetheless, some professionals highlighted that knowledge sharing is not always easy. Organizations are often dealing with confidential information and it is not always possible to set-up these knowledge sharing initiatives without compromising an organization’s privacy.

Finally, it was highlighted that for cybersecurity professionals wanting to advance, it is crucial that they remain passionate. Ultimately, the field is constantly evolving and that requires unparalleled commitment from those working in it and the desire to continually learn and stay up to date.


4. Retaining Cybersecurity Talent

Most interviewed professionals acknowledged that retaining cybersecurity employees is no easy task and that is not specific to the GCC region, but rather a global issue. On the one hand, given the lack of understanding of the field and the technical nature of the roles, enterprises struggle to understand what they need to do to motivate and retain talent. On the other hand, given the limited pool of talent available in the market, cybersecurity professionals have their pick of the different institutions they can potentially explore. Nonetheless, despite being valuable commodities in the market, most professionals noted that for the most part, people working in the field struggle to find company cultures that embrace their roles and offer an environment that allows them to thrive. Furthermore, some emphasized that retention is particularly challenging within governmental organizations given that professionals favor private enterprises mainly due to better financial incentives.

The Need for Recognition


The thirst for recognition within this field is quite evident, with most interviewed professionals underscoring the importance of appreciation when it comes to retaining cybersecurity talent. Ultimately, by celebrating and rewarding achievements, companies prove to their cybersecurity professionals that they acknowledge their contributions and understand the crucial role they play in ensuring business continuity. This often starts

with leadership stepping up and acting as sponsors for their cybersecurity talent which in turn will restore faith in leadership and drive motivation and loyalty.

 *The impact of moral recognition lasts far longer than any financial incentive, and is more likely to contribute to increased loyalty” – Cybersecurity Professional*

The Importance of Professional Development

Another area of consensus among interviewed professionals was the need for clear and long-term development plans for people working in this field. They highlighted the importance of growth prospects and professional development opportunities in making employees feel valued and inspired to continue working within their organizations. This, of course, entails a continuous investment not only in general training as mentioned before but also an intricate understanding of each employee’s skillset and talents in order to be able to devise personalized goals that align with each individual’s long term professional goals.

 *Having clarity is very important as well as showing staff that the company is investing in them and in their learning and career development. All these factors will strengthen loyalty of cybersecurity professionals towards their organizations.” – Cybersecurity professional*

5. Learning from Other Markets

The United Kingdom Efforts

Researchers have identified the UK’s approach to cybersecurity as one of the benchmarks to be considered. By virtue of being a multidisciplinary profession, there was little consensus about the cybersecurity skillset. The UK government therefore created the cybersecurity body of knowledge (CYBOK) program (Rashid, Danezis, Chivers, Lupu, & Martin, 2018). The purpose of the body was to create a repository of data for cybersecurity. It also aimed to codify the foundational and currently recognised cybersecurity knowledge so it could then act as a guide to academic research, technical reports, textbooks and standards creation (Rashid, Danezis, Chivers, Lupu, & Martin, 2018). The reason for this advanced creation is that cybersecurity is still in its infancy and has not settled on an area of exclusive competence. However, the UK government still recognises that the immaturity of cybersecurity should not be a barrier to handling the emerging issues, especially considering the continuing changes in technology. One

of the main roles of CYBOK is the improvement of skills on cybersecurity to counter the effects of cybercrime.

For the UK to get on a par with growing cyber skills needs there have been efforts to enhance training of more security experts. The government recognized that the existing disciplines have developed in isolation and are fragmented, hence requiring a more central approach. Research by Curry and Bird (2018) showed that there are various areas of concentration that may be useful in improving the cybersecurity skillset. The first is staff training where the UK government has been trying to use best practices in implementing appropriate information security (Curry & Bird, 2018). For the purpose of public awareness, the government implemented a Massive Open Online Course to ensure that the general public is aware of cybersecurity related issues and how to prevent them. The UK also started supporting both traditional and competency-based certifications. Tittle and Lindros (2018) explain that some of the certifications, such as certified ethical hacker and certified information security manager, are an important starting point for creation of professionals with the required skillset.

Singapore Efforts

The GCC may also consider benchmarking against Singapore. The Singapore education system is an important link to the country's prosperity. It has always been vital in ensuring the small population supports itself by ensuring that there is a competent workforce to support industrial development (Woo, 2017). The Singapore school system focuses on creating a workforce that is capable of meeting future challenges.

In 2013, Singapore launched the National Cyber Security Masterplan 2018 (NCSM2018). After its launch, the country developed the National Cybersecurity R&D Program to promote research and development and increase cyber security expertise (Sarker, et al., 2019). Through the program, there is more collaboration among agencies, research institutes, academia, and the private sector. A 5-year budget of 130 million SGD was dedicated to funding research in the technical and human related aspects of cybersecurity (Vu, 2016). Further, the Infocomm Development Agency (IDA) initiated a company-led training (CLT) program where young professionals would collaborate with CLT partners. Through CLT, professionals were mentored and trained in the areas of technology to meet the needs of the local cybersecurity industry (Vu, 2016). The partnership with businesses meant that they got the opportunity to work on real-world problems, therefore bridging the gap between industry requirements and what is taught within the universities.

Further, Singapore NCSM2018 launched the Cyber Security Awareness and Outreach Program which aimed to explore novel methods of covering more users through a Cyber Security Awareness Campaign; it enhanced awareness of cyber risks to the public and promoted secure online behavior (Sarker, et al., 2019). The younger generations have also been engaged through National Infocomm Security Competition (NISEC). The efforts made by Singapore have ensured that, apart from professionals being more competent in their work, there is greater awareness of the general public about the cybersecurity threats they are likely to face.

Conclusion

In order to tackle the challenges that cybersecurity talent currently face in the region, it is crucial that governments, organizations, and educational institutions all work together to provide an ecosystem that strengthens the standing of people working in the field. Based on the feedback and experiences of interviewed professionals, in order to reach that goal, the following actions need to be prioritized:

Asserting Cybersecurity functions' Influence within Organizations

In order for cybersecurity functions to thrive there needs to be a collective effort to elevate the role of cybersecurity professionals within organizations. First and foremost, fortifying the influence of cybersecurity functions falls under the responsibility of organizations' leadership, who are required to act as champions and nurture a culture that values cybersecurity roles and understands the importance of integrating them across the wider company structure.

With that in mind, it is the role of management to ensure the training of non-cybersecurity personnel and raising awareness in order to instill a better understanding of the significance of cybersecurity roles within the organization. Ultimately, it is crucial to ensure that every stakeholder across the organization, irrespective of their seniority level, is doing their part to defend their enterprises against cybersecurity risks.

Only by bridging the gap will cybersecurity functions no longer solely play the role of security defenders but rather business enablers that propel organizations forward amidst the increasing demands brought about by the unprecedented rapid digitization.

Nurturing Cybersecurity Talent Requires Focus on Soft Skills

On the other side of the spectrum, fortifying the influence of cybersecurity functions also requires an effort to develop professionals' soft skills in order to provide them with the tools that allow them to secure their demands as well as disseminate their message across the organization and garner the support of multiple stakeholders. With that in mind, it becomes important that organizations focus their training efforts on honing their talents' communication and leadership skills in order to empower them to exert their influence and effect positive change within their organizations.

Bridging the Experience Gap by Offering Hands on Training Initiatives

Given the technical nature of the field, cybersecurity professionals have access to a wide range of different certifications that allow them to hone their skills across different specializations. Nonetheless, most professionals underscored that this is not enough in

isolation. According to professionals in the field, there is an insufficiency in the number of initiatives that provide hands on training before professionals embark on this career path. This requires a heavy investment in internship and scholarship programs that focus on bridging the gap between knowledge and actual implementation at an early stage, which is currently perceived to be lacking.

Retention Through a Holistic and Personalized Approach

In order to retain talent in this field, it is crucial that companies invest the time and effort to understand what drives cybersecurity employees and focus on initiating development and incentive schemes that are relevant to the needs of those working in the field. This requires a special emphasis on professional development and highlighting growth prospects available for cybersecurity professionals, which, in turn, gives employees clarity and drive to pursue these prospects within their organizations. Additionally, it is essential that companies do not undermine the importance of recognition when it comes to boosting moral and retaining talent. While this can be generalized across most professions, within this field particularly it stands out due to the disconnect professionals often feel within their organizations.

Way Forward

In order to substantiate the results and provide a numerical overview of the state of market based on the findings gathered during this phase, the second phase should entail carrying out a quantitative survey with a representative sample of establishments across the following sectors: Telecommunication, Banking, Cybersecurity Services and Oil & Gas⁸. Additionally, it is recommended that the quantitative phase is followed by qualitative interviews that focus on key themes emerging from both phases in order to provide more in-depth understanding of the main uncovered findings.

- A. **Quantitative Approach:** the quantitative approach would include telephone surveys with senior cybersecurity personnel working in one of the specified sectors. Some objectives covered in the quantitative phase would include:
- Sizing of the different challenges identified in the qualitative phase across the entirety of the GCC and identifying key differences by sector.
 - Substantiating the perceived skills gaps in the region and understanding differences that arise between the different segments.
 - Measure the prevalence of training plans and identify key approaches adopted when it comes cybersecurity personnel professional development.
 - Measure the degree to which organizations outsource cybersecurity services and the reasons behind that.

Important note: refer to appendix to view the suggested draft questionnaire.

- B. **Qualitative Approach:** The qualitative approach will entail in-depth interviews with a preselected professional to delve deeper into some of the key findings extracted in the quantitative phase. The sample will be chosen directly from the quantitative phase based on the results that need further exploration.

⁸These are the same sectors explored in this phase

Appendix I: List of Cyber Skills

Vulnerability Assessment	Skill of using commercial tools to identify vulnerabilities with the potential for exploitation.
Penetration Testing	Skill of conducting penetration testing against networks, infrastructure, web applications, mobile devices and control systems and participating in simulated attack exercises based on scenarios derived from threat intelligence.
Cybersecurity architecture	Skills in applying security architectural principles to networks, IT systems, Control Systems (e.g., SCADA, ICS), infrastructure and products to meet the business needs and the technical requirements.
	Skills in incorporating relevant security policies and risk mitigations into a secure architectural design while assessing the vulnerabilities of existing products and technologies.
Incident Response	Skills in detecting and responding effectively to cybersecurity incidents and applying Incident Response plans.
Digital Forensic	Skills in conducting forensic analyses using forensic tools in multiple Operating System environments and in electronic evidence acquisition effectively, with minimum disruption to the business.
Cybersecurity Operations	Skills in securely configuring and maintaining information, control, and communications equipment in accordance with relevant security policies, standards, and guidelines.
Cybersecurity Network Operations	Skills in using intrusion detections tools and technologies to monitor network and system activity and to analyze the information and identify recognized indicators of compromise and warnings.
Threat Intelligence Management	Skills in assessing and validating information from various sources to predict and prioritize threats to an organization and reporting cybersecurity threat trends relevant to the organization.
Cybersecurity Governance	Skills in performing cybersecurity related impact and risk assessments.
	Skills in developing and applying appropriate cybersecurity policies that comply with relevant standards at the level of an organization, programme, project or operation.

	Skills in conducting cybersecurity audits or compliance reviews of technical systems.
Cybersecurity of Industrial Control Systems & Operational Technologies (ICS/OT)	Skills in translating operational requirements into protection needs and applying appropriate measures for protecting ICS/OT environments against relevant cyber threats.
Cybersecurity Systems and Applications Development	Skills in developing new techniques and /or tools as security countermeasures to identified risks and in incorporating the principles of security by design in the development of systems and applications.
	Skills in assessing the impact of the application of new system updates and products on the organization cybersecurity.
Cybersecurity Research	Skills in conducting cybersecurity research and using existing knowledge from available resources in experimental development to produce new or substantially improved devices, products, and processes to tackle cybersecurity issues.
Cybersecurity Training and Awareness	Skills in identifying cybersecurity awareness, training and culture management needs and in developing and delivering training, behavioural analysis programmes and/or security culture management programmes in alignment with an organization’s cybersecurity strategies and policies and the relevant local and global standards and regulations.
Communication and Knowledge Transfer	Skills in communicating information clearly and in a manner relevant to the target audience and in presenting complicated concepts in a simpler way to influence senior management as well in sharing knowledge and expertise in cybersecurity with others.
Leadership	Skills in encouraging and supporting others to meet objectives and in developing cybersecurity professionals.

	<p>Skills in collaborating with stakeholders to ensure business continuity and disaster recovery programs meet organizational requirements and in using expertise to maximize the cost effectiveness of cybersecurity strategy and relevant decisions and in negotiating effectively on cybersecurity issues and vendors agreements.</p>
--	--

Appendix II: References

- Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43-62.
- Chandra, G. R., Sharma, B. K., & Linqet, I. (2019). UAE's strategy towards most cyber resilient nation. *International Journal of Innovative Technology and Exploring Engineering*, 3(12), 2803-2809.
- Curry, J., & Bird, D. A. (2018). A case for using blended learning and development techniques to aid the delivery of a UK cybersecurity core body of knowledge. *International Journal of Systems and Software Security and Protection*, 9(2), 28-45.
- Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, 9, 1-12.
- Griffith, B. (2017). Growing the next generation of cyber professionals. *European Cybersecurity Journal*, 3(3), 15-19.
- Intel Security. (2016). *Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills*. Washington, DC: Center for Strategic and International Studies.
- ISACA. (2019). Part 1: Current Trends in Workforce Development. *State of Cybersecurity*.
- ISC². (2015). The Cybersecurity Workforce Estimate and the Workforce Gap. *Global Information Security Workforce Study*.
- ISC². (2020). The Cybersecurity Workforce Estimate and the Workforce Gap. *Global Information Security Workforce Study*.
- Nobles, C. (2018). The cyber talent gap and cybersecurity professionalizing. *International Journal of Hyperconnectivity and the Internet of Things*, 2(1), 42-51.
- Rashid, A., Danezis, G., Chivers, H., Lupu, E., & Martin, A. (2018). Scoping the Cyber Security Body of Knowledge. *IEEE Security and Privacy Magazine*, 16(3), 96-102.
- Sarker, K., Rahman, H., Rahman, K., Arman, S., Biswas, S., & Bhuiyan, T. (2019). A comparative analysis of the cyber security strategy of Bangladesh. *International Journal of Cybernetics & Informatics*, 8(2), 1-21.

- Shires, J. (2018). Enacting expertise and risk in Cybersecurity. *Politics and Governance*, 6(2), 31-40.
- Shires, J., & Hakmeh, J. (2020). Is the GCC Cyber Resilient? *International Security Programme*, 1-20.
- Vu, C. (2016). Cyber Security in Singapore. *Rajaratnam School of International Studies*, 1-28.
- Woo, J. J. (2017). Educating the developmental state: Policy integration and mechanism redesign in Singapore's skills future scheme. *Journal of Asian Public Policy*, 3, 1-18.

Appendix III: Draft Questionnaire

Demographics

Disclaimer: Please note that all information will be used for research purposes only and will not be shared with anyone except members directly involved in the GCC-UK Fellowship study. The purpose of this survey is to gather and synthesize data to help support and develop cybersecurity capacity building within the Gulf, and meet GCC demand and present current challenges in disseminating cyber security skills, with the aim to overcome any challenges through the study's recommendations. The identified cybersecurity skills were based on the UK's IISP Skills framework and the NIST's NICE Framework and SCyWF framework.

ADD DEFINITION OF CYBER SECURITY IF NECESSARY:

By cyber security, I mean any strategy, processes, practices or technologies that organizations have in place to protect their networks, computers, programs, the data they hold, or the services they provide, from unauthorized access, harm or misuse.

S4. Are you a decision maker regarding the cyber security within your business? **List, Single Response**

1	Yes
2	No TERMINATE

Background Information of Organization

O1. Which sector does your organization belong to? **List, Single Response**

1	Oil and Gas
2	Telecommunications
3	Banking
4	Cybersecurity Training
5	Other (Specify)

O2. Is your organization ... ? **List, Single Response**

1	Government
2	Private
3	Semi Government
4	Non-Profit

O3. Currently, what is the size of your organization (by full time employees)? **Single Response**

	O3	O3A (RECODE)
1	Less than 50	Small
2	51-100	Medium
3	101-150	Medium
4	149-200	Medium
5	201 – 250	Medium
6	251-300	Large
7	301-350	Large
8	351-400	Large
9	Over 400	Large

Cyber Security

O4. Is the cybersecurity department currently, a separate department in your organization? **List, Single Response**

1	Yes
2	No

O5. Where do most of the employees currently engaging in cyber tasks work (within a designated cyber security department or under any other departments), list all that applies? **list, multiple response**

1	Finance Department
2	IT Department
3	Information Department
4	Cybersecurity Department
5	Other Departments (Specify)

O5A. How many of your employees are working in cyber security roles? **Numeric (ALLOW DON'T KNOW)**

O5B. Can you please distribute the total number of employees working in cyber security roles in your organisation into Males and females? **Numeric (ALLOW DON'T KNOW)**

A	Males	_____	Persons
B	Females	_____	Persons

O6. Please Identify which of the following Cybersecurity roles exist within your organization, if you are unaware please select don't know? **List, single response per row**

Only ask for codes 2 or 3 mentioned in O6

O7. Please Identify which of the following Cybersecurity roles are needed and which ones are not needed within your organization? **List, single response per row**

		O6			O7	
		Yes	No	Don't Know	Needed	Not Needed
A	Chief Information Security Officer	1	2	3	1	2
B	Cyber Security Managers	1	2	3	1	2
C	Cyber Security Architect	1	2	3	1	2
D	Network Security Engineer	1	2	3	1	2
E	Cyber Security Operations Specialist	1	2	3	1	2
F	Cyber Security Analyst	1	2	3	1	2
G	Penetration Tester	1	2	3	1	2
H	Threat Intelligence Analyst	1	2	3	1	2
I	Systems and Application Cybersecurity Engineer	1	2	3	1	2
J	Cybersecurity GRC Roles	1	2	3	1	2
K	Cybersecurity Incident Responder	1	2	3	1	2
L	Cybersecurity Researcher	1	2	3	1	2
M	Other (Specify) _____	1	2	3	1	2

Outsourcing

Q1. Are any aspects of your cyber security handled by individuals or organizations outside your own organization? This does not include software firms providing technical support or security updates for their own applications, such as Microsoft updates to Office 365. This may include a service provider that manages your IT or network, or helps you recover from cyber incidents. **List, single response**

1	Yes
2	No

Q2. Which of the following aspects of cyber security are covered by your outsourced provider or providers? **List, single response per row**

(ROTATE STATEMENTS)

		Yes	No	Don't Know
A	Designing secure networks, systems and application architectures	1	2	3
B	Penetration testing	1	2	3
C	Using cyber threat intelligence tools or platforms	1	2	3
D	Carrying out forensic analysis of cyber security breaches	1	2	3
E	Interpreting malicious code, or the results shown after running anti-virus software	1	2	3
F	Using tools to monitor user activity	1	2	3
G	Setting up firewalls	1	2	3
H	Detecting and removing malware on the organization's devices	1	2	3
I	Creating back-ups of your files and data	1	2	3
J	Keeping software up to date	1	2	3

Technical Skillsets

T0. Which of the following cybersecurity skills are relevant to your organization? By relevant we mean the ones that are important and needed within your organization? **List, single response per row (YES/NO)**

	Skillset
A	Vulnerability Assessment: Skill of using commercial tools to conduct vulnerability assessments tests for public domain and assessment of the potential for exploitation.
B	Penetration Testing: Skill of conducting penetration testing against networks, infrastructures, web applications, mobile devices and control systems and participating in simulated attack exercises based on scenarios derived from threat intelligence.
C	Cybersecurity Architecture: Skills in applying security architectural principles to networks, IT systems, Control Systems (e.g. SCADA, ICS), infrastructures and products to meet the business needs and the technical requirements.
D	Cybersecurity Architecture: Skills in incorporating relevant security policies and risk mitigations into a secure architectural design while assessing the vulnerabilities of existing products and technologies.
E	Incident Response: Skills in detecting and responding effectively to cybersecurity incidents and applying incidents response plans.
F	Digital Forensic: Skills in conducting forensic analyses using forensic tools in multiple operating system environments and in electronic evidence acquisition effectively with minimum disruption to the business.
G	Cybersecurity Operations: Skills in securely configuring and maintaining information, control and communications equipment in accordance with relevant security policies, standards and guidelines.
H	Cybersecurity Network Operations: Skills in using intrusion detections tools and technologies to monitor networks and systems activity and to analyse the information and identify recognised indicators of compromise and warnings.
I	Threat Intelligence Management: Skills in assessing and validating information from various sources to predicts and prioritises threats to an organisation and reporting cybersecurity threat trends relevant to the organisation.
J	Cybersecurity Governance: Skills in performing cybersecurity related impact and risk assessments.
K	Cybersecurity Governance: Skills in developing and applying appropriate cybersecurity policies that complies with relevant standards at the level of an organisation, programme, project or operation.
L	Cybersecurity Governance: Skill in conducting cybersecurity audits or compliance reviews of technical systems.
M	Cybersecurity of Industrial Control systems and Operational Technologies (ICS/OT) (e.g. SCADA, ...): Skills in translating operational requirements into protection needs and

	applying appropriate measures for protecting ICS/OT environments against relevant cyber threats.
N	Cybersecurity Systems and Applications Development: Skills in developing new techniques and /or tools as security countermeasures to identified risks and in incorporating the principles of security by design in the development of systems and applications.
O	Cybersecurity Systems and Applications Development: Skills in assessing the impact of the application of new system updates and products on the organisation cybersecurity.
P	Cybersecurity Research: Skills in conducting cybersecurity research and utilizing existing knowledge from available resources in experimental development to produce new or substantially improved devices, products and processes to tackle cybersecurity issues.
Q	Cybersecurity Training and Awareness: Skills in identifying Cybersecurity awareness, training and culture management needs and in developing and delivering training, behavioural analysis programmes and/or security culture management programmes in alignment with the organisation’s cybersecurity strategies and polices and the relevant local and global standards and regulations.
R	Communication and Knowledge Transfer: Skills in Communicating information clearly and in a manner relevant to the target audience and in presenting complicated concepts in a simpler way to influence senior management as well in sharing knowledge and expertise in cybersecurity with others.
S	Leadership: Skills in encouraging and supporting others to meet objectives and in developing cybersecurity professionals.
T	Leadership: Skills in collaborating with stakeholders to ensure business continuity and disaster recovery programs meet organizational requirements and in using expertise to maximise the cost effectiveness of cybersecurity strategy and relevant decisions and in negotiating effectively on cybersecurity issues and vendors agreements.

FOR T1 ONLY SHOW SKILLS = “YES” IN T0

T1. Please rank each technical skill from the below cybersecurity skillsets by importance in your organization (From: 1= Not important At All to 10= Extremely Important). **List, Single Response Per Line**
Rotate Statements

	Skillset
A	Vulnerability Assessment: Skill of using commercial tools to conduct vulnerability assessments tests for public domain and assessment of the potential for exploitation.
B	Penetration Testing: Skill of conducting penetration testing against networks, infrastructures, web applications, mobile devices and control systems and participating in simulated attack exercises based on scenarios derived from threat intelligence.

C	Cybersecurity architecture: Skills in applying security architectural principles to networks, IT systems, Control Systems (e.g. SCADA, ICS), infrastructures and products to meet the business needs and the technical requirements.
D	Cybersecurity architecture: Skills in incorporating relevant security policies and risk mitigations into a secure architectural design while assessing the vulnerabilities of existing products and technologies.
E	Incident Response: Skills in detecting and responding effectively to cybersecurity incidents and applying incidents response plans.
F	Digital Forensic: Skills in conducting forensic analyses using forensic tools in multiple operating system environments and in electronic evidence acquisition effectively with minimum disruption to the business.
G	Cybersecurity Operations: Skills in securely configuring and maintaining information, control and communications equipment in accordance with relevant security policies, standards and guidelines.
H	Cybersecurity Network Operations: Skills in using intrusion detections tools and technologies to monitor networks and systems activity and to analyse the information and identify recognised indicators of compromise and warnings.
I	Threat Intelligence Management: Skills in assessing and validating information from various sources to predicts and prioritises threats to an organisation and reporting cybersecurity threat trends relevant to the organisation.
J	Cybersecurity Governance: Skills in performing cybersecurity related impact and risk assessments.
K	Cybersecurity Governance: Skills in developing and applying appropriate cybersecurity policies that complies with relevant standards at the level of an organisation, programme, project or operation.
L	Cybersecurity Governance: Skill in conducting cybersecurity audits or compliance reviews of technical systems.
M	Cybersecurity of Industrial Control systems and Operational Technologies (ICS/OT) (e.g. SCADA, ...): Skills in translating operational requirements into protection needs and applying appropriate measures for protecting ICS/OT environments against relevant cyber threats.
N	Cybersecurity Systems and Applications Development: Skills in developing new techniques and /or tools as security countermeasures to identified risks and in incorporating the principles of security by design in the development of systems and applications.
O	Cybersecurity Systems and Applications Development: Skills in assessing the impact of the application of new system updates and products on the organisation cybersecurity.
P	Cybersecurity research: Skills in conducting cybersecurity research and utilizing existing knowledge from available resources in experimental development to produce new or substantially improved devices, products and processes to tackle cybersecurity issues.
Q	Cybersecurity training and awareness: Skills in identifying Cybersecurity awareness, training and culture management needs and in developing and delivering training, behavioural analysis programmes and/or security culture management programmes in

	alignment with the organisation's cybersecurity strategies and polices and the relevant local and global standards and regulations.
R	Communication and Knowledge transfer: Skills in Communicating information clearly and in a manner relevant to the target audience and in presenting complicated concepts in a simpler way to influence senior management as well in sharing knowledge and expertise in cybersecurity with others.
S	Leadership: Skills in encouraging and supporting others to meet objectives and in developing cybersecurity professionals.
T	Leadership: Skills in collaborating with stakeholders to ensure business continuity and disaster recovery programs meet organizational requirements and in using expertise to maximise the cost effectiveness of cybersecurity strategy and relevant decisions and in negotiating effectively on cybersecurity issues and vendors agreements.

Only Show codes rated 4 & 5

T3. In your opinion, which of the following cybersecurity skills has the highest priority in your training plans? **(RANK the top 10 skills)** List, Multiple Response.

Rotate Statements

	Skillset
A	Vulnerability Assessment: Skill of using commercial tools to conduct vulnerability assessments tests for public domain and assessment of the potential for exploitation.
B	Penetration Testing: Skill of conducting penetration testing against networks, infrastructures, web applications, mobile devices and control systems and participating in simulated attack exercises based on scenarios derived from threat intelligence.
C	Cybersecurity architecture: Skills in applying security architectural principles to networks, IT systems, Control Systems (e.g. SCADA, ICS), infrastructures and products to meet the business needs and the technical requirements.
D	Cybersecurity architecture: Skills in incorporating relevant security policies and risk mitigations into a secure architectural design while assessing the vulnerabilities of existing products and technologies.
E	Incident Response: Skills in detecting and responding effectively to cybersecurity incidents and applying incidents response plans.
F	Digital Forensic: Skills in conducting forensic analyses using forensic tools in multiple operating system environments and in electronic evidence acquisition effectively with minimum disruption to the business.
G	Cybersecurity Operations: Skills in securely configuring and maintaining information, control and communications equipment in accordance with relevant security policies, standards and guidelines.

H	Cybersecurity Network Operations: Skills in using intrusion detections tools and technologies to monitor networks and systems activity and to analyse the information and identify recognised indicators of compromise and warnings.
I	Threat Intelligence Management: Skills in assessing and validating information from various sources to predicts and prioritises threats to an organisation and reporting cybersecurity threat trends relevant to the organisation.
J	Cybersecurity Governance: Skills in performing cybersecurity related impact and risk assessments.
K	Cybersecurity Governance: Skills in developing and applying appropriate cybersecurity policies that complies with relevant standards at the level of an organisation, programme, project or operation.
L	Cybersecurity Governance: Skill in conducting cybersecurity audits or compliance reviews of technical systems.
M	Cybersecurity of Industrial Control systems and Operational Technologies (ICS/OT) (e.g. SCADA, ...): Skills in translating operational requirements into protection needs and applying appropriate measures for protecting ICS/OT environments against relevant cyber threats.
N	Cybersecurity Systems and Applications Development: Skills in developing new techniques and /or tools as security countermeasures to identified risks and in incorporating the principles of security by design in the development of systems and applications.
O	Cybersecurity Systems and Applications Development: Skills in assessing the impact of the application of new system updates and products on the organisation cybersecurity.
P	Cybersecurity research: Skills in conducting cybersecurity research and utilizing existing knowledge from available resources in experimental development to produce new or substantially improved devices, products and processes to tackle cybersecurity issues.
Q	Cybersecurity training and awareness: Skills in identifying Cybersecurity awareness, training and culture management needs and in developing and delivering training, behavioural analysis programmes and/or security culture management programmes in alignment with the organisation's cybersecurity strategies and polices and the relevant local and global standards and regulations.
R	Communication and Knowledge transfer: Skills in Communicating information clearly and in a manner relevant to the target audience and in presenting complicated concepts in a simpler way to influence senior management as well in sharing knowledge and expertise in cybersecurity with others.
S	Leadership: Skills in encouraging and supporting others to meet objectives and in developing cybersecurity professionals.
T	Leadership: Skills in collaborating with stakeholders to ensure business continuity and disaster recovery programs meet organizational requirements and in using expertise to maximize the cost effectiveness of cybersecurity strategy and relevant decisions and in negotiating effectively on cybersecurity issues and vendors agreements.

FOR T1 ONLY SHOW SKILLS = "YES" IN T0

T5. For which of the following skills do you believe your company needs further training? Please select all that applies. **List, multiple response**

	Skillset
A	Vulnerability Assessment: Skill of using commercial tools to conduct vulnerability assessments tests for public domain and assessment of the potential for exploitation.
B	Penetration Testing: Skill of conducting penetration testing against networks, infrastructures, web applications, mobile devices and control systems and participating in simulated attack exercises based on scenarios derived from threat intelligence.
C	Cybersecurity architecture: Skills in applying security architectural principles to networks, IT systems, Control Systems (e.g. SCADA, ICS), infrastructures and products to meet the business needs and the technical requirements.
D	Cybersecurity architecture: Skills in incorporating relevant security policies and risk mitigations into a secure architectural design while assessing the vulnerabilities of existing products and technologies.
E	Incident Response: Skills in detecting and responding effectively to cybersecurity incidents and applying incidents response plans.
F	Digital Forensic: Skills in conducting forensic analyses using forensic tools in multiple operating system environments and in electronic evidence acquisition effectively with minimum disruption to the business.
G	Cybersecurity Operations: Skills in securely configuring and maintaining information, control and communications equipment in accordance with relevant security policies, standards and guidelines.
H	Cybersecurity Network Operations: Skills in using intrusion detections tools and technologies to monitor networks and systems activity and to analyse the information and identify recognised indicators of compromise and warnings.
I	Threat Intelligence Management: Skills in assessing and validating information from various sources to predicts and prioritises threats to an organisation and reporting cybersecurity threat trends relevant to the organisation.
J	Cybersecurity Governance: Skills in performing cybersecurity related impact and risk assessments.
K	Cybersecurity Governance: Skills in developing and applying appropriate cybersecurity policies that complies with relevant standards at the level of an organisation, programme, project or operation.
L	Cybersecurity Governance: Skill in conducting cybersecurity audits or compliance reviews of technical systems.
M	Cybersecurity of Industrial Control systems and Operational Technologies (ICS/OT) (e.g. SCADA, ...): Skills in translating operational requirements into protection needs and applying appropriate measures for protecting ICS/OT environments against relevant cyber threats.

N	Cybersecurity Systems and Applications Development: Skills in developing new techniques and /or tools as security countermeasures to identified risks and in incorporating the principles of security by design in the development of systems and applications.
O	Cybersecurity Systems and Applications Development: Skills in assessing the impact of the application of new system updates and products on the organisation cybersecurity.
P	Cybersecurity research: Skills in conducting cybersecurity research and utilizing existing knowledge from available resources in experimental development to produce new or substantially improved devices, products and processes to tackle cybersecurity issues.
Q	Cybersecurity training and awareness: Skills in identifying Cybersecurity awareness, training and culture management needs and in developing and delivering training, behavioural analysis programmes and/or security culture management programmes in alignment with the organisation’s cybersecurity strategies and polices and the relevant local and global standards and regulations.
R	Communication and Knowledge transfer: Skills in Communicating information clearly and in a manner relevant to the target audience and in presenting complicated concepts in a simpler way to influence senior management as well in sharing knowledge and expertise in cybersecurity with others.
S	Leadership: Skills in encouraging and supporting others to meet objectives and in developing cybersecurity professionals.
T	Leadership: Skills in collaborating with stakeholders to ensure business continuity and disaster recovery programs meet organizational requirements and in using expertise to maximise the cost effectiveness of cybersecurity strategy and relevant decisions and in negotiating effectively on cybersecurity issues and vendors agreements.

T6. In your opinion what are the key elements which would make cybersecurity skills framework most beneficial to your organization? **List, Multiple Response**

Rotate Statements

1	Identify Skills by Levels of Expertise
2	Identify Skills by Cybersecurity Speciality Area
3	Identify Skills by Cybersecurity Job Role
4	Provide Suggested Training Paths
5	Other (Specify)

T7. Which constraints would you rate as most problematic in achieving your cybersecurity plans? (Check all that apply) **List, Single Response Per row**

1	Budget for Cyber Security	
2	Shortage of Skilled Employees	
3	Lack of Executive Management	
4	All of The Above	
5	Other (Specify)	

T8. How do you or *would you* keep current cybersecurity staff within your organization and how do you grow your staff capacity? **List, Single Response Per row**

1	Financial Incentives	
2	Recognition	
3	Better Salary Packages	
4	Training Opportunities	
5	Organization Stability (Governmental Job)	
6	Career Path Development / Planning	
7	Other (Specify)	

T9. Please rate the following soft skills based on their importance to cybersecurity. (From: Not Important at All to Extremely Important) **List, Single Response Per Row.**

	Skillset	Not Important at All	Somewhat Not Important	Neutral	Somewhat Important	Extremely Important
A	time management,	1	2	3	4	5
B	teamwork,	1	2	3	4	5
C	the ability to work under pressure,	1	2	3	4	5
D	communication skills and reporting?	1	2	3	4	5
E	the ability to learn new skills,	1	2	3	4	5
F	the willingness to explore in the cyber security field.	1	2	3	4	5
G	Other, please specify:	1	2	3	4	5

Training & Accreditation

T1. Do you currently have a national or internal cybersecurity training program and or academy? **Single Response.**

1	Yes
2	No

T2A. Which of the following types of qualifications or certified training do you think employees working in cybersecurity roles in your organization have, or are they working towards? **List, multiple response**

1. A specialist higher education qualification (e.g. a degree) related to cyber security
2. A general computer science, information systems or IT higher education qualification
3. A cyber security apprenticeship
4. Any other apprenticeship
5. Any other technical qualifications or certified training related to cyber security
6. Other specify
7. Don't know **(Exclusive)**

T2. What existing international or national cybersecurity frameworks for skill development are followed/planned to be followed in your organization? **List, Multiple Response**

1	NICE (USA)
2	IISP (UK)
3	Cobit5 (EU)
4	SCyWF (KSA)
5	Other (Specify)
6	None