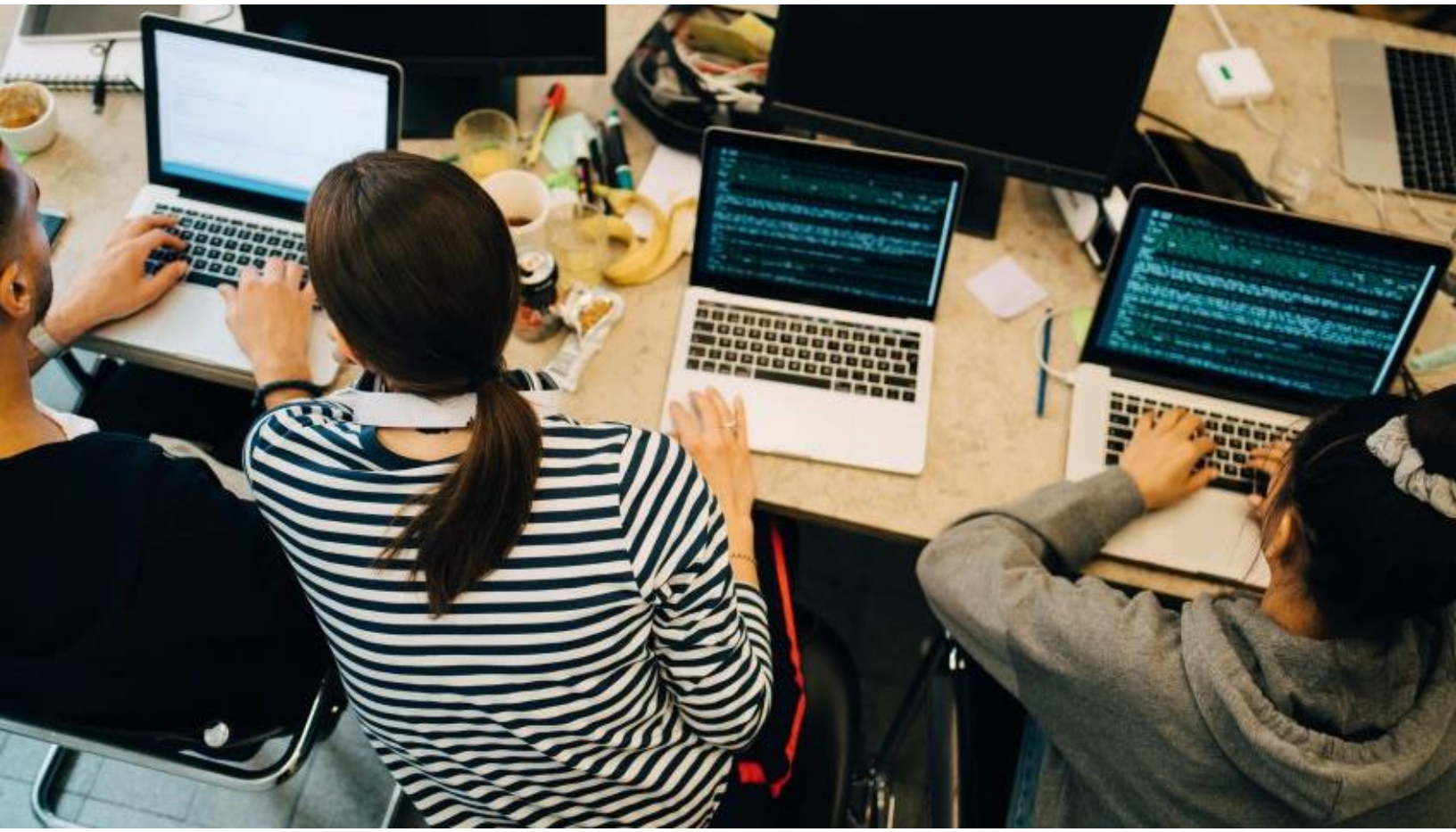
USAID FROM THE AMERICAN PEOPLE

UK International Development
Partnership | Progress | Prosperity

DAI
Shaping a more livable world.



CRITICAL INFRASTRUCTURE DIGITALIZATION AND RESILIENCE

Cyber Workforce — State of Play and Future Needs of Public Institutions in North Macedonia

This publication was produced by the Critical Infrastructure Digitalization and Resilience program under Cooperative Agreement No. 7200AA21CA00015 at the request of the United States Agency for International Development (USAID). This document is made possible by the support of the American people through USAID. Its contents are the sole responsibility of the author or authors and do not necessarily reflect the views of USAID or the U.S. Government.

CRITICAL INFRASTRUCTURE DIGITALIZATION AND RESILIENCE

Cyber Workforce — State of Play and Future Needs of Public Institutions in North Macedonia

Program Title:	Critical Infrastructure Digitalization and Resilience Program
Sponsoring USAID Office:	USAID Bureau for Europe and Eurasia
Contract Number:	Cooperative Agreement No. 7200AA21CA00015
Contractor:	DAI Global, LLC
Date of Submission:	November 9, 2023
Author:	DAI Global, LLC and Florida International University

TABLE OF CONTENTS

PROGRAM BACKGROUND

The Critical Infrastructure Digitalization and Resilience Program in North Macedonia is tasked with enhancing the nation's cybersecurity capabilities and identifying the primary cybersecurity vulnerabilities within the country's critical infrastructure. "Critical Infrastructure" encompasses virtual and physical systems crucial to the country's social and economic wellbeing and to national security. These systems are susceptible to cyberattacks. In North Macedonia, systems and servers operating in the healthcare sector, the information and communication technology (ICT) sector, and government institutions' websites are increasingly being targeted by cyberattacks. The capacity of these entities to safeguard their data and operations hinges on the presence of comprehensive and enforced cybersecurity policies and workforces that are qualified, skilled, and well-versed in their cybersecurity practices.

RESEARCH METHODOLOGY

Florida International University (FIU) visited North Macedonia in March and April of 2023 at the request of CIDR/North Macedonia. During the visit, the FIU team and CIDR/North Macedonia met with 12 local stakeholders, and relevant ministries, such as the Ministry of Information Society and Administration and the Agency for Quality in Higher Education. FIU also met with tertiary institutions to discuss the status of cybersecurity preparedness and education in North Macedonia.

To systematically assess the current need for cybersecurity personnel, the FIU and CIDR/North Macedonia teams designed a questionnaire to evaluate the cybersecurity workforce gaps in public administration institutions in North Macedonia. The survey was translated into Macedonian and conducted via the SurveyMonkey platform, targeting 1,354 public institutions under the network maintained by the Ministry of Information Society and Administration (MISA). This assessment is contributing to CIDR's identification and understanding of cybersecurity workforce shortcomings and needs in North Macedonia. Data was collected from May 22–June 19 with a sample size of 237 full and valid responses. This report provides a summary of the key findings from this survey.

SUMMARY OF FINDINGS

After conducting interviews and analyzing the survey results, several important conclusions were drawn:

- The majority of public institutions that participated in the survey reported that cybersecurity is a concern in their institution. Interviews with public sector officials indicated that public institutions are mostly concerned with the protection of personal data and other sensitive information.
- Almost all public institutions that participated in the survey noted that they lack funding, personnel, and support to address emerging cyber threats in their institution. They also forecast a growing need for cybersecurity managers to oversee an anticipated increase in organization-level cybersecurity strategies and management plans in the next five years. Detailed survey results can be found below in this document.

- The cybersecurity education ecosystem at the tertiary level is uneven and remains under development. As of April 2023, only four public universities in North Macedonia provide undergraduate programs in information technologies and computer science; traditional degrees that are related but not directly linked to cybersecurity programming. Only a handful of universities are making efforts to provide cybersecurity certificates, classes, and degrees.
- As of April 2023, two universities in North Macedonia—the Faculty of Computer Science and Engineering (Ss Cyril and Methodius University) and the University of Information Science and Technology ("St. Paul the Apostle")—provide bachelor's degrees in cybersecurity. One public university, Goce Delcev University, provides a cybersecurity degree at a graduate level.
- Like other nations around the world, North Macedonia produces an insufficient number of graduates with the skills and knowledge needed to enter the cybersecurity workforce. According to the State Statistical Office of the Republic of Macedonia, between 2018 and 2022, only 40 students received an undergraduate degree in "Communication Networks and Security" from the University of Information Science and Technology ("St. Paul the Apostle"). Similar numbers can be seen at other institutions as well. This shortage of qualified cyber workforce candidates is noticeable for all cybersecurity roles and positions throughout North Macedonia.

CYBERSECURITY WORKFORCE IN NORTH MACEDONIA

Out of the 237 respondents who completed the assessment, 51% indicated that their organization prioritizes cybersecurity. However, a more significant number of organizations reported insufficient personnel or budget to satisfy their cybersecurity needs. Out of the 237 respondents, 206 (87%) disagreed that their organization has an adequate number of skilled cybersecurity personnel, and 160 public institutions (68%) indicated that hiring new cybersecurity personnel posed a challenge. Strikingly, 94% of the North Macedonia public institutions that participated in the survey indicated they do not have a budget allocated for hiring new cybersecurity staff. *Table 1* summarizes the main challenges faced by public institutions in North Macedonia.

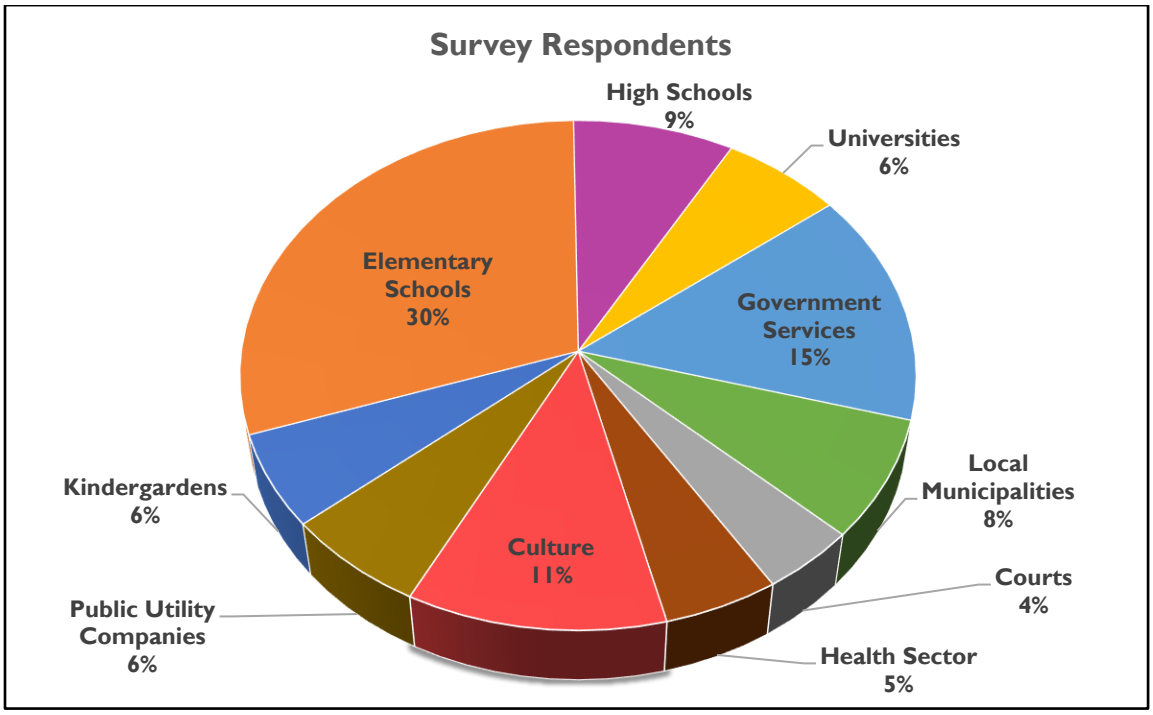
Table 1: Cybersecurity Challenges in Public Institutions in North Macedonia

	Yes	No
Cybersecurity is a priority in my institution.	51%	49%
We have enough skilled cybersecurity personnel in my institution.	13%	87%
Hiring skilled cybersecurity professionals is an issue in my institution.	68%	32%
My organization has allocated a budget to hire more cybersecurity personnel.	6%	94%

Distinct challenges exist across different levels of government and sectors. Public institutions such as courts and local municipalities often prioritize cybersecurity; however, these public institutions struggle the most to hire skilled personnel and retain current employees. Other public institutions that provide government services equally struggle with hiring cybersecurity personnel. On the other hand, despite

not prioritizing cybersecurity highly, tertiary institutions[1] and universities stand out as the most successful institutions in North Macedonia in recruiting new cybersecurity staff. Also, despite frequent cyberattack exposure, the healthcare sector and public utility companies seem to not prioritize cybersecurity; this could be explained by a lack of sufficient personnel, knowledge, and awareness of risks, or inadequate budget to hire new cybersecurity graduates.

Figure 1: Survey respondents (N=237)



[1] Faculty of Security- Skopje; Faculty of Music- Skopje; University "St. Cyril and Methodius" -Skopje; Faculty of Electrical Engineering and Information Technologies - Skopje; Faculty of Agricultural Sciences and Food – Skopje; UKIM Agricultural Institute – Skopje; UKIM Faculty of Mechanical Engineering -Skopje; Faculty of Law "Justinian First"- Skopje; Rabotnicki University "Krste Misirkov"- Kichevo; University "St. Kliment Ohridski" – Bitola; Faculty of Information and Communication Technologies- Bitola; "St. Apostle Paul" – Ohrid; University of Tetovo;

EXISTING CYBERSECURITY WORKFORCE

Out of 237 respondents that participated in this survey, 150 (63%) indicated that their organization employs some form of cybersecurity personnel; the other 87 indicated that they currently do not employ cybersecurity personnel.

Collectively, 150 public institutions that employ cybersecurity personnel use a total of 382 cybersecurity staff members. Most employees in public institutions classified as cybersecurity personnel hold positions such as data administrators (31.7%), system administrators (28.8%), and network specialists (16.5%). Regarding executive roles, only 8.9% of public institutions employ Information Security Administrators, a mere 1.8% have a Chief Information Officer, and only 1.6% of institutions have an Information Security Manager. Employees classified under "other" cybersecurity roles represent 10.7% of cybersecurity personnel.

Table 2: Existing Cybersecurity Workforce Among 237 Respondents in North Macedonia

Position	Total	Percentage
System Administrator	110	28.8%
Data Administrator	121	31.7%
Information Security Administrator	34	8.9%
Chief Information Officer	7	1.8%
Information Security Manager	6	1.6%
Network Specialist	63	16.5%
Other roles	41	10.7%
Total	382	100%

According to the respondents, women constitute 45.8% of all cybersecurity personnel in their institutions. Many of these women (46.3%) hold positions as data administrators, while 26.9% serve as system administrators. Approximately 14.3% of women are employed in other roles, with 8% working as an information security administrator. Less than 2% of women hold the position of chief information officer or information security manager position. The most significant gender disparity is among network specialists, where women account for 2.9% of the workforce. Female cybersecurity professionals are predominantly employed by elementary schools, the healthcare sector, and entities that provide government services, mainly in the position of data administrator.

Table 3: Gender Distribution of Cybersecurity Workforce in North Macedonia

Position	Total Females	Percentage
System Administrator	47	26.9%
Data Administrator	81	46.3%
Information Security Administrator	14	8.0%
Chief Information Officer	1	0.6%
Information Security Manager	2	1.1%
Network Specialist	5	2.9%
Other roles	25	14.3%
Total	175	

Looking at the distribution across sectors, most cybersecurity personnel are employed by public institutions that provide government services (45%), followed by elementary schools (15%), the court system (10%), and hospitals (8%). Many cybersecurity personnel employed by public institutions that provide government services work full-time. Part-time employees, or those dedicating six hours per week to cybersecurity responsibilities, are predominantly found in elementary and high schools. Often, these requirements are met by existing teachers or consultants provided to the schools by the Ministry of Education.

The survey also requested that respondents describe any other cybersecurity roles and job assignments within their institutions not included in the study. According to the respondents, out of the total 382 cybersecurity personnel employed in public institutions, 41 (10.7%) were employed under "other roles/job assignments." Roughly half of these roles were considered low-level positions (e.g., junior associate) or external roles that have been outsourced (e.g., advisor for information development). Some jobs listed include data protection officer, ICT support advisor, information consultant, system engineer, and cyber incident analysis officer. Other roles were described as positions that require technical knowledge and skills (e.g., cyber incident response and protection) or a combination of executive and technical proficiency (e.g., head of an information security department). Public institutions such as the Ministry of Defense, Supreme Court, State Commission for Prevention of Corruption, and others that provide government services employ most of the individuals categorized under these roles/job assignments.

FUTURE NEEDS IDENTIFIED

The assessment invited participants to indicate whether their institution plans to hire cybersecurity professionals and to specify the total number of cybersecurity personnel they require. The respondents were also asked whether they are planning to hire new cybersecurity personnel within the next six years. Out of 237 survey respondents, 66% stated a need for additional cybersecurity personnel, with an expectation to hire new staff within 1-4 years. The biggest challenges to hiring new personnel, as reported by the respondents, are budgetary constraints and lack of government understanding of cybersecurity needs. For instance, a striking 94% of all public institutions in North Macedonia do not have funds budgeted to hire cybersecurity personnel. Out of 237 public institutions, around 28% stated they do not have a need or intention to hire new cybersecurity personnel within the next six years. These institutions do not prioritize cybersecurity in their organization, and they do not have a designated budget for cybersecurity.

Furthermore, the respondents indicated a growing need for certain cybersecurity positions, suggesting that the cybersecurity workforce in public institutions in North Macedonia will continue to expand. *Figure 2* demonstrates how the cybersecurity workforce in North Macedonia may expand and change over the next five years. The most significant demand reported by the respondents was for information security administrators and network specialists. Currently, in 237 public institutions in North Macedonia, these two roles make up approximately 25% of the total cybersecurity workforce. However, projections indicate that in the next five years, these two roles will constitute roughly 38% of the total cybersecurity workforce in North Macedonia. According to the public institutions that participated in this survey, their institutions will have a requirement to hire an additional 110 information security administrators and 140 network specialists over the next five years.

Public institutions in North Macedonia also seek cybersecurity personnel who possess executive skills, technical understanding, and the ability to lead organizational cybersecurity policy. Like other managerial roles, there will be an increased demand for chief information officers and information security managers. Currently, chief information officers represent 1.8% of the total cybersecurity workforce among public institutions that participated in the survey. Information security managers represent 1.6% of the respondents' total cybersecurity workforce. When asked about their future needs, respondents suggested that within the next five years, chief information officers will represent 4.9% of the total cybersecurity workforce, and information security managers will represent 8.8% of the total cybersecurity workforce. According to the public institutions that participated in this survey, their institutions will have a requirement to hire an additional 32 chief information officers and 58 information security managers over the next five years.

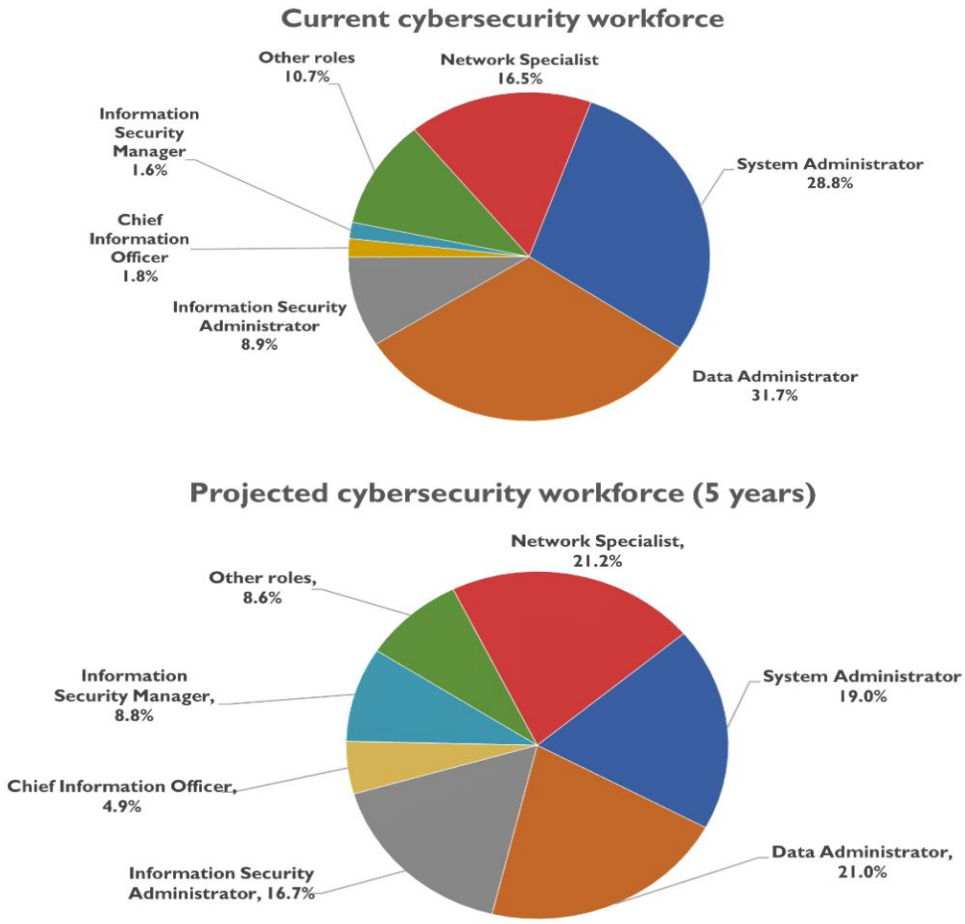
Much of the current cybersecurity workforce in North Macedonia is comprised of data administrators and system administrators (60.5%). However, the assessment indicates a gradually declining need for these roles in the future, mainly due to the growing demand for other cybersecurity positions, such as network specialists and information security administrators. *Figure 2* demonstrates that data administrators currently represent 31.7% of the cybersecurity workforce in North Macedonia, but according to the respondents, data administrators will decrease to 21% of the workforce over the next five years. Comparably, system administrators, who currently account for 28.8% of the cybersecurity workforce, are expected to represent only 19% of the workforce in the next five years. To be precise,

within the next five years, according to the respondents, there will be a need for 29 additional data administrators and two system administrators.

This report represents the first effort to capture the characteristics of the cybersecurity workforce in public institutions in the Balkan region, and while the report did not specifically address the reasons for the projected five-year trends, it can be posited that they are influenced by a handful of reasons. For example, most respondents of the survey were from small public institutions that had between 1–100 employees and underdeveloped cybersecurity policies, and so it is not surprising that the bulk of the cybersecurity responsibilities in these institutions fall onto data and system administrators. In our sample, only 6% of survey respondents indicated that their institution currently allocates the budget to hiring cybersecurity personnel; the few institutions that have allocated a budget for cybersecurity are more likely to already employ cybersecurity personnel that have executive and managerial responsibilities, while many of the institutions that do not are projecting to fill those managerial voids. It can also be posited that there will be a greater need for information security managers because public institutions are recognizing that they lack a comprehensive cybersecurity strategy and management plan to face cyberattacks in the next five years.

The examples above demonstrate that university graduates and professionals entering the cybersecurity workforce in North Macedonia will need to have skills and knowledge that will prepare them for managerial/executive roles vs. administrator roles. In the next five years, there will be an increased demand for network specialists, information security administrators, and information security managers in public institutions in North Macedonia. There will be a relatively decreased need for data and system administrators. For example, *Figure 2* demonstrates that data and system administrators will represent 40% of the total cybersecurity workforce in the next five years (down from 60.5%). According to the respondents, network specialists, information security administrators, and information security managers will represent 45% of the cybersecurity workforce (up from 27.0%). This has implications for the development of the cybersecurity workforce in North Macedonia and for educational institutions that need to produce enough qualified candidates.

Figure 2: Current and Projected Cybersecurity Workforce in North Macedonia



Lastly, cybersecurity needs vary across sectors and entities that provide government services to the citizens and elementary schools have the greatest need for cybersecurity professionals. In the upcoming 6 years, for example, government entities that provide services to the citizens have the greatest need for network specialists (90), system specialists (59), and information security administrators (59). Elementary schools have the greatest need for system administrators (40), data administrators (29), and information security administrators (25). On the other hand, the health sector, kindergartens, and public utility companies in North Macedonia do not prioritize cybersecurity. And although these institutions have the greatest need for data and system administrators, these institutions do not have the budget nor the pathway to hire new cybersecurity professionals in the upcoming five years.

RECOMMENDATIONS

BUDGET

Although most of the responding public institutions recognize the importance of cybersecurity within their organizations and acknowledge the need for skilled cybersecurity personnel, approximately 94% of these institutions lack a dedicated cybersecurity budget. The primary means for many of these institutions to enhance their cybersecurity is to secure adequate resources for cybersecurity personnel and training. Regarding hardware and software, these public institutions also indicated the need for resources to obtain software updates, hardware upgrades, and new equipment purchases.

However, before advocating for an increased government budget for cybersecurity, and based on interviews with key local stakeholders and relevant personnel from ministries and tertiary institutions, the authors recommend that public institutions take a more holistic view of their cybersecurity needs and challenges. Public institutions in North Macedonia should assess their human capital and needs, formulate cybersecurity policies tailored to their organizations, and identify and rank potential threat actors. Only through such comprehensive self-evaluation and prioritization will these institutions effectively present an understanding of their specific requirements and make a strong case for additional funds and other resources for cybersecurity enhancement.

THE ROLE OF THE GOVERNMENT

Interviews conducted for this assessment combined with the survey results suggest prioritizing cybersecurity within the Government of North Macedonia and that cyber preparedness by the public institutions responsible for citizen services is a fiscal responsibility. Rather than solely focusing on increased resource allocation for cybersecurity personnel and equipment, there is a suggestion for the government to demonstrate leadership and commitment in bolstering and sustaining the nation's cybersecurity capabilities. This applies uniformly to all government levels and organizations delivering public services.

For example, findings from a recent survey underscore the need for recognizing and systematizing the cybersecurity profession and related roles in North Macedonia. Feedback from participating public institutions indicates a substantial requirement for assistance in recruiting and retaining cybersecurity personnel. Within these institutions, cybersecurity is currently not uniformly recognized, and the profession appears fragmented, making it challenging for employers to articulate their needs in the limited job market. The lack of recognition, awareness, and standardization directly impacts the budget allocation for cybersecurity personnel in public institutions. Additionally, the approval process for new employment within these institutions, often involving their respective ministries, is both time-consuming and frequently unproductive.

A suggested approach involves the government considering the introduction of new systemization acts that define and expand cybersecurity roles within public institutions. Furthermore, there is a recommendation to establish a comprehensive roadmap for hiring cybersecurity personnel in all public institutions, encompassing clear procedures, standards, and budgetary requirements. To achieve this, the report suggests leveraging frameworks such as the NICE Workforce Framework for Cybersecurity and ENISA's European Cybersecurity Skills Framework. In the interim, adopting a framework tailored to the

country's needs is deemed crucial. This approach involves dedicating additional resources to the recruitment and retention of new cybersecurity professionals, as well as training existing employees who assume cybersecurity responsibilities in public institutions. Additionally, allocating funds and resources to facilitate training and job shadowing is proposed as a means to foster talent sharing across public institutions.

THE ROLE OF ACADEMIA

This survey estimates that 237 public institutions that participated in the survey will require approximately 700 new cybersecurity employees within the next 1-4 years. The primary approach to meeting this demand will be to increase the quantity and quality of graduating cybersecurity students. As such, tertiary institutions, training providers, and high schools must identify strategies to rapidly close the labor gap within the country's cybersecurity workforce.

This survey reveals an ongoing and imminent need in North Macedonia for entry-level positions, such as junior advisors or data administrators. Roles such as data administrators and system administrators, which represent 60% of the current workforce can be filled by high school graduates who may lack hands-on experience or the means to pursue a bachelor's degree. Increasing the short-term candidate pool for entry-level positions is vital to the public institutions responsible for protecting personal and sensitive information. However, as demonstrated in *Figure 2,* the demand for entry-level positions in North Macedonia is expected to flatten in the next five years. As shown in *Figure 2*, the cybersecurity workforce in North Macedonia is expected to be more equally distributed among different job roles in the next five years. The biggest demand is expected for network specialists and information security managers since most of the public institutions that participated in the survey indicated a greater need for graduates possessing executive, managerial, or technical knowledge and skills. Balancing these demands for positions at various levels against limited or non-existent budgets will pose a significant challenge for nearly all public institutions that participated in the survey.

All institutions that provide cybersecurity education in North Macedonia, such as tertiary institutions and training providers, are the source for qualified applicants with the executive, technical, and soft skills necessary to implement and lead cybersecurity efforts in public institutions. These educational bodies need to be prepared to provide more professionals and graduates entering the workforce with the knowledge and skills needed to navigate the organizational and budgetary constraints of public institutions in North Macedonia. Upon graduation, there should be incentives for graduates and prospective employees who meet the cybersecurity needs of public institutions to pursue employment in public institutions rather than the private sector. More than training providers, tertiary institutions will play a crucial role in bridging this gap as they offer environments conducive to long-term learning and development.

This report recommends that tertiary institutions in North Macedonia take the following actions:

1. Provide continuous opportunities for current and prospective students to participate in cybersecurity boot camps and certification programs. These programs should equip students with the skills and knowledge required to enter the workforce upon graduation. They should also place an emphasis on hands-on experience and practical learning.

2. Implement one-year or two-year professional or academic programs to ensure a consistent supply of prospective employees with a practical understanding of cybersecurity and the ability to support cybersecurity measures within organizations.

3. Incorporate cybersecurity electives into curricula and/or accredit cybersecurity curricula at their institutions to attract new students seeking to enter the cybersecurity workforce.

WOMEN AND THE CYBERSECURITY WORKFORCE IN NORTH MACEDONIA

This report has identified a significant gender gap in the cybersecurity workforce in North Macedonia. While women make up 45.8% of all cybersecurity personnel in the responding public institutions, their roles are predominantly concentrated in data administration (46.3%) or system administration (26.9%). Less than 10% of women employed in public institutions hold executive or managerial cybersecurity positions. Furthermore, women are less likely than men to occupy roles that require technical knowledge and application. For example, less than 3% work as network specialists. The data suggests that women are more likely to be placed in entry-level roles such as data and system administrators and are less likely to hold executive or managerial positions.

This is alarming since the greatest workforce needs in North Macedonia over the next five years lie in the executive and managerial positions rarely occupied by women. As the cybersecurity ecosystem in North Macedonia evolves, women risk being confined to entry-level roles or dismissed as unqualified candidates for future executive or managerial positions. There must be a clear professional development pathway beyond entry-level positions for women seeking to advance their careers and take up leadership roles in the cybersecurity workforce. This includes facilitating significantly more accessible access to the cybersecurity workforce for women, regardless of their level of education, and creating opportunities for women in entry-level positions to advance within their organizations. Providing women with professional development and practical skills is crucial, making them qualified and competitive candidates for executive roles.

This report recommends that the government formulate a clear pathway for women to enter and advance in the cybersecurity workforce. This pathway should aim to: 1) increase women's representation in the cybersecurity workforce, allowing women of all educational backgrounds to enter the workforce, including at entry-level positions, and 2) provide incentives and opportunities for women employees to seek professional and technical development. The endeavor to provide easier entry into the cybersecurity workforce for women and close the gender gap by including more women within the cybersecurity workforce will have a cascading effect on the ICT labor market and the nation’s prosperity. Furthermore, preparing women to take on more demanding cybersecurity roles should be viewed as a shared responsibility between the private sector industry, government, and academia.