Teaching the Cybersecurity Courses at the University in Georgia

Girshel Chokhonelidze[1*], Giorgi Basilaia[1],
Mikheil Kantaria[1], Marine Dgebuadze[1]
Business and Technology University (BTU)
Tbilisi, Georgia

Abstract:- As current trends show, cybersecurity poses a challenge to the modern world, both to the public and private sectors. Every year the number and impact of attacks on the government networks increases, so do financial losses caused by the activities of cybercriminals. The lack of human resources and the number of unoccupied vacancies around the world is also a challenge, as evidenced by several studies. Therefore, one of the necessary ways to solve this problem is to create an appropriate educational component in universities, which will ensure the creation of competent staff. Cybersecurity requires a complex approach and the relevant knowledge of all the required domains that are needed to ensure its effectiveness, such as network technologies, system architecture and administration, programming, databases, and more. We would like to introduce you to the approach of cybersecurity teaching, which we have implemented at the university and which is being executed successfully.

Keywords:- *Cybersecurity, Cybersecurity in university, Cybersecurity teaching, Cybersecurity educational component;*

I. INTRODUCTION

The development of the field of cybersecurity is a challenge to support the needs of the State and requires a comprehensive approach for the creation of appropriate intellectual resources, which must involve both, human resources and technology. [1]

Current trends around the world show that the stability of cybersecurity is a challenge for advanced countries or military alliances [2]. To address this issue, the states have begun to classify their infrastructure as a critical infrastructure [3], to ensure its security, special state structures (for example United States Cybersecurity and Infrastructure Security Agency) are created [4], legislation is being improved and new regulations are being developed [5].

Intellectual / human resources are one of the main factors in cybersecurity [6].

The aforementioned is a critical problem for Georgia, both for the public and private sectors. This is evidenced by growing statistics on cybercrime [7] and several attacks on networks of State organizations and infrastructure [8].

Therefore, it is important to train specialists in the field and to create sufficient intellectual resources.

To avoid these threats and strengthen the cybersecurity sector in the country, it is necessary to create factual knowledge in the form of educational components. The purpose of the article is to recommend one of the models of cybersecurity training to higher education institutions.

Digital transformation and growing dependence on computer technology pose new challenges that are critical for both individuals and the private sector, as well as for states and international military-political unions [9].

One of such critical challenges in the field of cybersecurity [10]. The demand for specialists in this profession is growing day by day, both in public and private sectors [11].

As the 2019 Cost of a Data Breach Report [12] by the IBM Security and Ponemon Institute shows, the average loss of data breach amounts to 3.92 million. (Fig. 1)

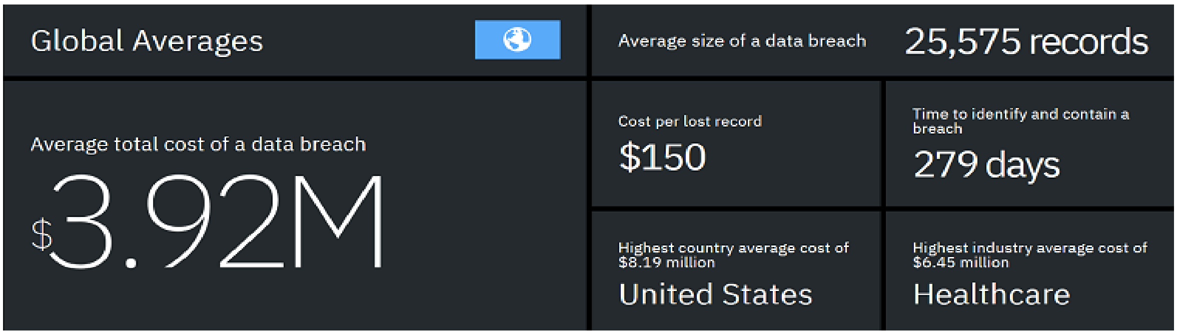

Fig 1:- Average total cost if a data breach

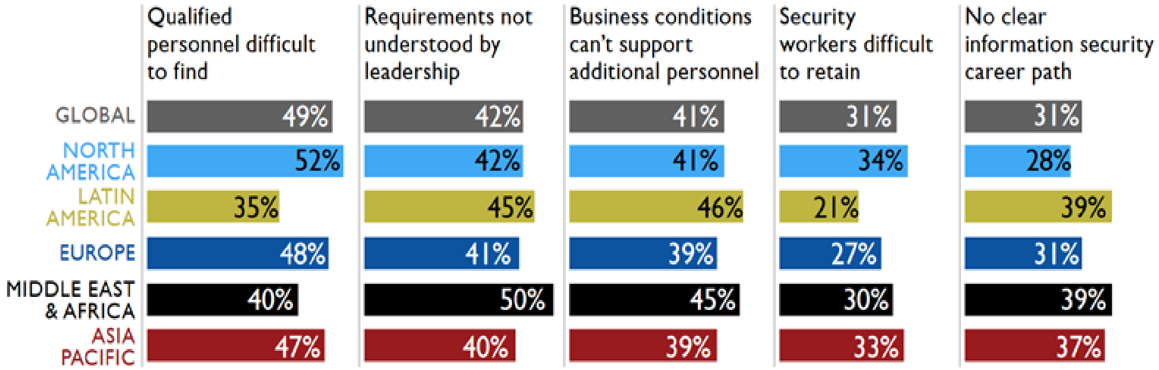

Fig 2:- Global information security Workforce study (2017) n=12,709

The average time it takes for the organizations to record and respond to an incident is 279 days, which can have a critical and devastating effect on both the organization and its customers. Consequently, delayed actions reduce the effectiveness of implemented security measures.

According to research, the challenge is to fill the cybersecurity-related vacancies. According to a 2017 study of the Center for Cyber Safety and Education [13], the shortage of staff for cybersecurity vacancies will reach 1.8 million by 2022, which shows up to 20% growth since 2015, when the shortage of staff was 1.5 million (Fig. 2)

All the above-mentioned demonstrates the critical importance of the training and mobilization of new workforce and specialists in the field of cybersecurity.

II. MATERIAL AND METHOD

In recent years, there has been a significant increase in the interest among students in the field of computer science in Georgia, and there is a growing trend in terms of the number of enrolled students. The statistics on the enrolment of students for the bachelor's degree programs in the field of technology, which were requested from the National Assessment and Examinations Center, were analyzed. The obtained materials show that 1800 students were enrolled in the bachelor's program in information technology in 2018 and 2170 students – in 2019, which is about 20% more and indicates the growing interest in the field.

Consequently, the demand for subjects of cyber and information security is growing. Therefore, it is advisable to offer the students effective systematic education in the field of cybersecurity.

Cybersecurity is a complex subject that requires a certain level of competence in various domains of information technology, such as network technologies, system architecture/administration, programming, databases, and more. Relevant competence in various domains of information technology allows the cybersecurity specialist to provide the security of relevant infrastructure and information systems as efficiently as possible.

To meet the abovementioned needs, it is important to develop a curriculum for university education, which includes both, general education and the acquisition of specialized and specific practical skills in cyber and information security. Given that the field is completely new, it requires innovative approaches and proactive development in the education sector. For the development of practical skills, students need to have a basic general knowledge, practical laboratory work shall be provided to realize the acquired theoretical knowledge in practice, which will help the growth of students' motivation to master this specialty.

To ensure the abovementioned, we have implemented the following practice at the University of Business and Technologies.

The academic year at UBT consists of 2 semesters and includes 60 ECTS credits (30 credits per semester). Depending on the characteristics of the student's study program, the annual workload may be less than 60 credits or more, but not more than 75 credits (1 credit in UBT = 25 hours). Program Duration - 4 academic years (8 semesters). Bachelor's academic degree, considered by the program is granted by fulfilling the requirements of the undergraduate program as a result of accumulating established credits.

The distribution of compulsory subjects according to semesters is shown in Table 1.

The basic principle of the approach is for the students to accumulate relevant knowledge and practice of those domains, the security of which should be ensured by them directly after studying the subject of cybersecurity. Subjects have a corresponding prerequisite, which also provides the abovementioned.

It is noteworthy that some of the subjects directly related to security are presented in the form of elective subjects, which also have the corresponding prerequisites. For example, in the third semester, interested students are allowed to choose a basic course in information security, where the students receive both theoretical and practical knowledge. The courses are shown in Table 2.

Compulsory courses - Semester I	**Course Pre-requisites**
Introduction to programming (Python)	No prerequisite
Introduction to computer networking	No prerequisite
Mobile Applications	No prerequisite
Principles of Digital Technologies	No prerequisite
Compulsory courses - Semester II	
Introduction to databases (Oracle)	Introduction Digital Technologies
Programming (Python)	Introduction to programming (Python)
PC architecture / design	No prerequisite
Compulsory courses - Semester III	
Computer networks (CCNA I)	Introduction to computer networking
LINUX	Principles of Digital Technologies
Data structures and algorithms (I. C)	Introduction to programming (Python)
Compulsory courses - Semester IV	
Data structures and algorithms (II. C++)	Data structures and algorithms (I. C)
Front End Development	Introduction to programming (Python)
Compulsory courses - Semester V	
JVM Programming	Programming (Python), Introduction to databases (Oracle)
Introduction to machine learning	Programming (Python)
Compulsory courses - Semester VI	
Cybersecurity	LINUX; Introduction to computer networking
Database administration (OCA)	Introduction to databases (Oracle)
Compulsory courses - Semester VII	
Information technologies audit (planned)	Cybersecurity, Data structures and algorithms (II. C++), Computer networks (CCNA I)
Compulsory courses - Semester VIII	
IT service management	Computer networks (CCNA I)

Table 1:- Courses and prerequisites (as of 2019-2020 academic year)

Elective courses	**Course Pre-requisites**
Information security	Introduction to computer networks
Server operating system (Windows Server)	Principles of digital technologies
Wireless Communications (CWNA)	Computer networks CCNAI
Computer networks (CCNA II)	Computer networks CCNAI
Digital Transformation	PC architecture/design
Mobile application development on Android	JVM Programming, Mobile applications
Information security management	Information security
Cloud systems (AWS I)	Linux, Introductions to Computer networks
Digital Art	Principles of digital technologies
Cloud systems additional services (AWS II)	Cloud systems (AWS I)
Web Programming II (React)	Front end development
Java programming II	Introduction to programming (Python)
Information systems analyses and design	JVM Programming
Cybersecurity strategy basics	Introduction to computer networks, Principles of digital technologies
Machine learning	Introduction to machine learning

Table 2:- Elective courses (as of 2019-20 academic year)

The aforementioned subject gives the student a general idea about cyber and information security, which gives the student a clearer picture of what cybersecurity deals with and what prospects does it have. In the following semesters, besides the mandatory subjects, they have the opportunity to choose the subjects that are directly related to cybersecurity, all this allows the student to fully cover all the domains, the knowledge of which will increase the student's effectiveness in the cybersecurity domain.

III. RESULTS AND DISCUSSION

This approach has shown that students can effectively master the subjects directly related to cybersecurity, which is reflected in their academic achievement. They are also competitive in cybersecurity vacancies and meet the relevant requirements.

University statistics show that with each passing year, the demand is growing for elective subjects that are directly related to cybersecurity. Students are interested in international certification courses and programs (eg Offensive Security Certified Professional) and are actively preparing to obtain these certificates. They are also actively pursuing internships in cybersecurity in both private and public sectors, and it should be noted that several students were employed at cyberspace-related positions in parallel with their studies at the university. Overall, it became clear that the statistics on student employment in the field of cyber and information security are growing.

IV. CONCLUSIONS AND RECOMMENDATIONS

Given all the above, it is obvious that the demand for cybersecurity specialists in the world market is much higher than the supply.

Therefore, higher education institutions must offer students an effective cybersecurity training program, for this purpose it is possible to use this program, as it is effective and successful at the University of Business and Technologies.

REFERENCES

[1]. U.S Government Accountability Office, “HIGH-RISK SERIES Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas“. GAO-19-157SP. 2019

[2]. NATO, “Defending against cyber attacks”. 2020 Available: https://www.nato.int/cps/en/natohq/topics_118663.htm

[3]. Critical and Infrastructure Security Agency, 2013 “critical infrastructure sector”. Available: https://www.cisa.gov/critical-infrastructure-sectors

[4]. US CISA, “About CISA”. 2020. Available: https://www.cisa.gov/about-cisa

[5]. Laurene Kalmnan, “New European Data Privacy and Cyber Security Laws: One Year Later“, Communications of the ACM, April 2019, Vol. 62 No. 4, Page 38 10.1145/3310326

[6]. M. J. Assante and D. H. Tobey, “Enhancing the cybersecurity workforce,” IT Prof., vol. 13, no. 1, pp. 12–15, 2011, doi: 10.1109/MITP.2011.6.

[7]. Business Media, 2020, “RECORDED CYBERCRIME DOUBLES IN GEORGIA”. Available: https://bm.ge/en/article/recorded-cybercrime-doubles-in-georgia/25838

[8]. Przemysław Roguski, 2020. “Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace” Available: https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

[9]. Hofmann, Sara & Ogonek, Nadine. “Different But Still The Same? How Public And Private Sector Organisations Deal with New Digital Competences”. Journal of E-Government. 2018. 16. 127-135.

[10]. Ervural, Beyzanur & Ervural, Bilal. “Overview of Cyber Security in the Industry 4.0 Era”. 2018. 10.1007/978-3-319-57870-5_16.

[11]. William Crumpler & James A. Lewis, “The Cybersecurity Workforce Gap”, Center for Strategic and International Studies. All rights reserved. 2019

[12]. IBM, “How much would a data breach cost your business?”, 2019. Available: https://www.ibm.com/security/data-breach

[13]. Center for Cyber Safety and Education, 2017. “Global information security workforce study”. Available: https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/02/14/Global-shortfall-of-cybersecurity-workers-to-reach-1-point-8-million-in-five-years