Education in Cyber Security. Possible Approaches to the Topic.

Nikolay Krushkov
Intellectual Property and Technology Transfer Department
University of National and World Economy, Sofia, Bulgaria

Abstract:
Modern holistic education in cyber security must ensure the ability of students and young professionals to be successful in taking on leadership roles to assure business continuity of any organization's operations. Cyber security becomes a sub-system of growing crucial importance. Another aspect of great significance are the corporate obligations of the position of a Chief Security Officer - a dynamically evolving professional field of activity. This position includes cyber security obligations, and the leadership of the Cyber Security Unit of any middle or large organization and this area increasingly finds its important place and role in the system of corporate management and communications.

Keywords: *Education; cyber security; security management; teaching cyber security; chief security officer*

1. Introduction

After two years of "social distancing" imposed by the global COVID pandemic and "home office" practices around the world, which quickly led to better electronic connectivity in day-to-day business activities, a holistic professional approach to cyber security emerged. As a result, nowadays, there is an almost unlimited demand for cyber security professionals from the academic sector, from the business sector, and from the state agencies all around the world. Modern holistic education in cyber security must ensure the ability of students and young professionals to be successful in taking on leadership roles to assure the security of any organization's operations.

2. Current approach towards teaching cyber security

The programs of cyber security globally cover many and completely different aspects in a vast range of scientific fields, relevant to the focus of academic interest of departments in various universities, institutes, faculties around the world, which as of April 2022 may be illustrated as follows:
Engineering and Technical Science - Master of Science in Cyber Security, College of Technology, University of Huston [2]
Law - "Cyber Security Law", School of Law, Boston University [3]
Management - "Cybersecurity Management and Leadership" Master of Arts, Cyber Security and Management Faculty, University of New Haven [4]
Sociology - "Socio-Technology of Cyber Security: An Experiential Learning Course", Department of Sociology, College of Arts and Sciences, Case Western Reserve University [5]
Economics - "Cybersecurity and Economics" Bachelor of Science, Northeastern University, USA [6]
Forensic - "Cyber Security", Forensic Science Programs, Forensic Science Schools by state, USA [7]
Security – Cyber and Data Security, Homeland Security Academy, The Academic College of Wingate, Israel [8]
The current academic reality is the consequence of academic specialization and unfortunately the result of science's partial readiness to respond to the rapidly growing demand of a holistic interdisciplinary approach in the field of cyber security planning, organization, and management as a whole.

3. Possible approaches towards teaching cyber security

Cyber security is in essence an interdisciplinary field and as such should be taught from different perspectives and in different scientific fields. As digital technologies penetrate deeply into almost every

aspect of human experience, a broad range of social-political-economic-legal-ethical-military and other considerations have come to envelop the cybersecurity landscape [1]. Today cyber threats surround every business activity, every organization, every person, and every communication. This reality demands from universities, institutes, and faculties to apply a comprehensive approach providing interdisciplinary knowledge and skills for the system of systems in cyber security. Cyber security faces enormous variety of challenges, and the academic teaching and research must be focused on the whole range of security controls and countermeasures mitigating cyber risks. All principles of the decision-making process in cyber security, including specification of the resources that need to be invested to achieve the necessary level of security, should be included in the syllabus of the academic courses taught. The modern holistic approach relies on multiple strategies when planning, organizing, and deploying cyber security. These multiple strategies put together a system of systems with separate but coordinated objectives. The objectives are managed by the Corporate Security Department, where the in-house Cyber Security Unit is placed. Usually, the key activities of the in-house Cyber Security Unit are implemented within the following systems (sub-systems):

- legal and regulatory compliance and proper policies and procedures
- ensuring technical projects in various areas
- identifying and setting risk indicators in every key business process
- risk assessment and risk management
- vulnerability assessment and penetration tests in every sector of an organization
- internal and external audits, and reporting
- cyber security best practices awareness and implementation
- training of leaders and all employees.

4. Interdisciplinary modules of a modern holistic cyber security syllabus

Every modern holistic academic Cyber Security Course should be perhaps structured in modules combining different scientific approaches, so that it includes knowledge from all relevant scientific areas such as:

Engineering and Technical Science
Theory of computer science
Information system architecture
Hardware and software labs
Programming
Elements of machine learning
Cryptography
Law
Data and Compliance
Intellectual Property
Unfair competition protection
GDPR
Civil, Administrative, and Penal Procedures in Cyber Security
Management
Planning and Budgeting
Coordination
Selection and Deploying of Systems
Auditing
Incident Management
Sociology and Marketing
Ethical-societal-policy implications of cyber attacks
Social Engineering
Segmentation
Targeting
Telecommunications
Networks
Wire, Optic, Radio, and Satellite
Electronic Transmission of Voice, Data, Text, Images, Video

VPN
Security
Data Structures
Vulnerability Analysis
Investigation and Digital Forensics
Physical, Technical, Information and Procedure Security
Penetration Testing
Information Warfare
The position of the Chief Security Officer
Job description
Coordination within the C-Suite of an organization
Internal audit system organization and reporting
Corporate Communications

5. Practical cases

- Additionally, any modern holistic Cyber Security Course should include practical cases focusing on practical issues in the cyber security area, such as:
- In-house Corporate Security Department - structure, functions and budgeting
- Formulation and coordination of the tasks within the Corporate Security Department
- The position of a Chief Security Officer – internal and external, horizontal, and vertical coordination Deployment of an integrated corporate security system - physical and digital. Rules and procedures
- Identification of intellectual property objects; of know-how; and of trade secrets of an organization; internal rules preparation principals and controlling
- Social media registrations of the members of the organization's management and of the employees
- Corporate e-mail system - two primary components that reside in an organization's IT infrastructure: mail clients and mail servers
- Corporate devices: computers, tablets, smartphones, flash memory sticks – security concept
- Customization, proper selection and systemic monitoring of key performance indicators and key risk indicators of an organization
- The role of the internal audit. Planned and ad hoc auditing of the cyber security system of an organization
- Preparation and implementation of penetration tests of the interactive corporate infrastructure – principles of testing
- Initial and ongoing training in cyber security of the organization's employees
- Response: organizations with a solid understanding of cyber security principles and robust technology investment may also fall victim to a security incident or data breach - plan to respond and ensure business continuity so that users and customers are not disrupted, and to apply lessons learned so that the incident is not repeated.

6. Conclusions

Cyber security is an extremely important aspect of any security system. Cyber security has an impact on business continuity, the security of people, corporation's assets, and corporate information. A high level of cyber security ensures stability and reliability of the interconnected environment we live and work in. That is why the field of cyber security teaching demands a multidisciplinary approach integrating fundamental technical knowledge, economics, management, law, sociology, and security modules with a strong holistic foundation. Students must study both the behavior of individuals and the collective behavior of industries and governments, utilizing computing, social, managerial, and legal skills to ensure the reliability and security of cyberspace.

References

- [1] Professors Jennifer M. Urban & Chris Jay Hoofnagle, Cyber Security In Context, Course Syllabus, Berkley University of California, USA. Available: https://bcourses.berkeley.edu/courses/1471305/assignments/syllabus
- [2] University of Huston, USA. Programs. Available: https://www.uh.edu/technology/programs/graduate/cybersecurity/
- [3] Boston University, School of Law, USA. Available: https://www.bu.edu/law/expertise/cybersecurity-law/
- [4] University of New Haven, USA. Programs. Available: https://onlinedegrees.newhaven.edu/programs/ms-masters-cybersecurity-management-leadership/
- [5] Case Western Reserve University, USA. Available: https://sociology.case.edu/2022/01/socio-technology-of-cyber-security-an-experiential-learning-course/
- [6] Northeastern University. Programs. Available: https://catalog.northeastern.edu/undergraduate/computer-information-science/computer-information-science-combined-majors/cybersecurity-economics-bs/
- [7] Forensic Science Schools, USA. Available: https://www.forensicscienceonline.org/specialty/cyber-security-forensics/
- [8] Homeland Security Academy at The Academic College of Wingate, Israel. Available: https://www.hls-academy.com/security/en/about/