Chapter 18
Interdisciplinary Training and Mentoring for Cyber Security in Companies

Ileana Hamburg
Institute of Work and Technology, Germany

ABSTRACT

Cyber security is interdisciplinary, and it is to expect that security professionals and other employees working with computers to have suitable knowledge. In this chapter an interdisciplinary training program in cyber security curriculum and an interdisciplinary mentoring program to be included in entrepreneurial learning will be proposed. It helps to produce synergy in groups and generates ideas to solve complex problems. Entrepreneurial learning is a basis for education of entrepreneurs, and it should also include such interdisciplinary programs. The author explained the advantages of interdisciplinary training and mentoring programs in this context particularly in the field of cyber security. Such programs are missing both in education as well as in companies. Two examples of European projects with the participation of the author will be done to improve entrepreneurial education and training and encourage SMEs to be innovative. The programs are supported by digital learning platforms, and interdisciplinary trainers and mentors help the learners. The main method is interdisciplinary problem-based learning (IPBL).

INTRODUCTION

Cyber security which historically was technical a subfield of computer science gained importance in fields like law and business management, as well as areas of technology such as smart grids, cars, and other cyber-physical systems (also due to pervasive computing technology).

The study field Ethics helps to distingue right from wrong, and good from bad. It analyzes the morality of human behaviors, policies, laws and social structures (Brey, 2005; Bynum, 2003; Hamburg & Grosch, 2017).Computer/Information ethics focuses on questions of responsibility for defects in the work of software, on preventing access to private information stored in computer databases, centralization and decentralization of power in computerized environments, as well as copy right, intellectual prop-

DOI: 10.4018/978-1-7998-5728-0.ch018

erty, and commercial confidentiality issues. The ethical right and responsibility referring information technology are related with legal responsibility and legal rights. Legal acts tend to be assessed on their ethical merits, while amendments to existing laws or legal acts or introduction of new ones increasingly require ethical grounding.

Ethics should be is a critical part of every cyber security defense strategy in organizations because without clear ethical standards and rules, employees cannot protect systems and data.

Due to their connections to computer systems and the Internet, all these areas must consider unanticipated security vulnerabilities (https://www.interpol.int/Crimeareas/Cybercrime/Cybercrime). Necessary quickly protecting measurements against cyber-crime requires collaboration between disciplines but at the same time, the field of cyber security is still relatively new and certain aspects cannot be standardized.

Literature study shows that traditional technological research in cyber security is not connected with companies´, public and private sectors' nontechnical tasks dealings with cyber security (Ramirez, 2017).

Based on literature review Ramirez (https://www.semanticscholar.org/paper/Making-cyber-security-interdisciplinary-%3A-for-a-and-Ramirez/6dbd08f328672d8cc3ac0fc164a7212c4b0888cf) summarized follow categories of cyber security research:

- The Public category includes issues of concern to governments: work regarding laws, international norms, and national security. Global technical standards produced by bodies like W3C, while often specifying norms, are in the Infrastructure category.
- The Business category includes most of the articles that address technological problems of cyber security; specifically, those problems referring the actual infrastructure of cyberspace.
- The Infrastructure category includes papers that discuss various aspects of cyber security of critical infrastructure, as well as security issues concerning the operation of cyberspace, such as cryptography.
- The General category contains all papers with issues which pervade the entire realm of cyber security, as well as descriptions of the field in general, and characterizations of cyberspace and humans' interactions with it and includes also most articles from social sciences.

This disconnect between traditional technological research in cyber security and the public and private sectors' nontechnical dealings with cyber security results from neither technical researchers nor management in business or government reaching out to communicate to the other parties, but there is also a communication problem between researchers in the same category (Ramirez, 2017). Communication among researchers and between research fields and other sectors of society should be improved. In order to facilitate cross-disciplinary communication, Ramirez recommended authors to harmonize their jargon usage. This change would improve idea flow between authors from different disciplines, who work solutions, but who write for separate audiences in their publications. To identify areas in this context of harmonization, Ramirez (https://www.semanticscholar.org/paper/Making-cyber-security-interdisciplinary-%3A-for-a-and-Ramirez/6dbd08f328672d8cc3ac0fc164a7212c4b0888cf) examined the extent of differences used keywords in articles from each the four security sub disciplines, analyzed time-series trends of terminology in cyber security journal articles, and developed a methodology for authors or standards bodies to use when deciding whether a word or phrase is appropriately interdisciplinary, or has been accepted by the general cyber security community. Because security is inherently interdisciplinary (Dalal & Tetrick, 2016) it is to expect every security professionals and other employees working with computers to have knowledge in many other domains and understand fields that refer their