Archives of Business Research – Vol.5, No.10
Publication Date: Oct. 25, 2017
DOI: 10.14738/abr.510.3818.

Hamburg, I., & Grosch, K. R. (2017). Ethical Aspects in Cyber Security. *Archives of Business Research,* 5*(10),* 199-206.

SOCIETY FOR SCIENCE AND EDUCATION

Ethical Aspects in Cyber Security

Ileana Hamburg
Institut Arbeit und Technik, WH Gelsenkirchen, Munscheidstr. 14,
D-45886 Gelsenkirchen, Germany

Kira Rosa Grosch
Institut Arbeit und Technik, WH Gelsenkirchen, Munscheidstr. 14,
D-45886 Gelsenkirchen, Germany

ABSTRACT

Cyber Security (CS) industry increases every year employment chances as well as the requirements at staff working in this field and at education. In January 2013, Cyber Security Strategy has been prepared by European Commission and it is decided that vocational and academic trainings in cyber security field should be improved also by including of topics in the curriculum like ethical, social and psychological ones. Ethics helps to distingue right from wrong, and good from bad. It analyzes the morality of human behaviors, policies, laws and social structures, in this paper we consider Ethic aspects in Information Security (IS)/ Cyber security (CS) being one of our research and development domain. A European project aimed at improving CS courses and knowledge of students in Ethics is presented.

Keywords: Information Security, Cyber Security, Cyber Security Professionals, Ethics

INTRODUCTION

The companies and public offices have taken some cyber security precautions in order to strengthen security within information technologies field. Cyber Security (CS) industry increases every year the both employment chances as well as the requirements at staff working in this field and at education.

In January 2013, Cyber Security Strategy has been prepared by European Commission to take precautions against the cyber-attacks which are performed continuously to companies, public offices and other strategically important offices. Within the context of this strategy, it is decided that vocational and academic trainings in cyber security field should be improved. One of the improvements should be the including of topics in the curriculum like ethical, social and psychological ones or to.

Ethics helps to distingue right from wrong, and good from bad. It analyzes the morality of human behaviors, policies, laws and social structures (Bray, 2005; Bynum and Rogerson, 2003). It is based on ethical principles of theories like **consequentialism** and **deontology. Consequentialist approaches** assume that actions are wrong to the extent that they have bad consequences. **Deontological approaches** assume that people have moral duties that exist independently of any good or bad consequences that their actions can have (Johnson, 2006).
Ethical principles are linked with legislation, but legislation is not a substitute for morality. So, it is important that individuals and organizations consider not only the legality but also the morality of their actions.

“As we probe the implications of a world closely connected electronically and increasingly dependent on these electronic connections, it is important that we not sit passively by, watching and predicting what it will all mean, rather than actively engaging in shaping it. We should be asking what form we want these electronic connections to take. Who should have control? What values should the system embody or promote? Who should have access? What social or 1995 introduce personal interests should these connections serve?" (Computers, Ethics and Social Values, the section "The Net World").

In this paper we consider Ethic aspects in Information Security (IS)/ Cyber security (CS) being one of our research and development domain. A European project aimed at improving CS courses and knowledge of students in Ethics is presented.

IS and CS are very closely related terms and are used sometimes interchangeably.

Richard Kissel gave following definitions for IS and CS (https://www.quora.com/Whats-the-difference-between-cyber-security-and-information-security).

Cyber Security is defined as the ability to protect or defend the use of cyberspace from cyber-attacks. It deals with protection of cyberspace and use of it against any sort of crime.

Information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Because most of the information today is saved electronically and most of the cyber-attacks are executed to disclose confidential information and harm its integrity there is sometimes confusion between these terms.

CS has as purpose to protect goods and resources of organizations from the organizational, human, financial, technical point of view, so that to allow them to continue their mission. Organizations must ensure that no significant prejudice is caused to them.

CS is a process involving the entire society, and everyone should be involved in supporting it and the development of a cybernetic code of conduct for the appropriate use of information and communication technology and in spreading an authentic security policy providing the standards for the users of cybersecurity (partners, entities, suppliers).

DEVELOPING A CYBER SECURITY STRATEGY

Within a cyber security process, it is important to correctly identify the goods and the resources which must be protected, so that the scope of the security necessary for an efficient protection is precisely determined. This requires a global approach of security, which should be multidisciplinary and comprehensive.

A cyber security strategy is necessary due to:

a. society's dependence on cyberspace, which means that security, resilience and trust in information and communication field represent a problem of national interest,
b. economic role and possibilities of information and communication technologies to maximize benefits and exploit their opportunities,
c. the fact that cybernetic attacks, especially those committed against critical information infrastructure, could represent a threat to the national security,
d. the necessity of protection of confidentiality, integrity and availability of data and information systems, in order to enhance security, resilience, authenticity and trust in

the field of information and communication technology (Himma, 2007; Laurie et Graeme, 2002),

e. objectives like the protection and promotion of human and state of law rights,
f. attention on the protection of critical information infrastructure within the public and private.

Often a cyber security strategy tends to focus on the technical, procedural and institutional measures, such as risk and vulnerability analyses, early warning and response, incident management, exchange of information, creation of bodies in the field of cybersecurity, such as *Computer Emergency Response Teams* (CERTs) and *Computer Security Incident Response Teams* (CSIRTs), which contribute to the intensification of international cooperation and other measures in order to ensure protection of cybernetic space.

A cyber security strategy should have as priorities also criminal justice or other measures that should be taken against cybercrime and which are not always included.

Referring ethics in CS strategies, a set of basic principles relating to ethical behavior, responsibility and transparency, incorporated in an adequate legal framework, and a practical set of procedures and norms are required which must be applied both at national level and at the level of the international community, and must be compatible with international directives in force.

Ethics— moral principles that govern a person's behavior should be a critical part of any cybersecurity strategy. Without clear ethical standards and rules, cybersecurity professionals (CSP) have difficulties to fight against criminals to protect systems and data.

ETHICS RESPONSIBILITIES OF CS PROFESSIONALS AND ORGANISATIONS

CS professionals (CSPs) are individuals who maintain systems and IS/CS.

They have a professional responsibility to assure the correctness, reliability, availability, safety and security of all aspects of information and information systems. This responsibility has a moral dimension: professional activities in computer security should protect people from morally harms but not causes such harms, and protect not *v*iolate people's moral rights.

In case of safety-critical systems, the decisions of information security professionals could have a great importance for life or death.

Moral responsibilities of CSP professionals as part of their profession are reflected in codes of ethics used by various organizations for computer and CS. These codes of ethics are not always explicitly detailed, i.e. the code of ethics of the Information Systems Security Association (ISSA), an international organization of information security professionals and practitioners, only states that members should "[p]perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles" but does not go on to specify what these ethical principles are or how they should be applied and balanced against each other in specific situations (International Telecommunication Union, 2009).

CSP professionals, as well as other computer professionals who have a responsibility for computer security, should be trained in information security ethics.

The training helps professionals:

- to get clear about interests, rights, & moral values that are at stake in computer security,

- to recognize ethical questions and dilemmas in their work,
- to balance different moral principles in resolving such ethical issues (Bynum et Rogerson, 2003).

Referring Ethics in organizations, aside from their employees, businesses must fulfill certain ethical and legal requirements in the event of a security incident, particularly a data breach. Time is undoubtedly a key factor in responding to cyberattacks. However, notifying customers and clients about any serious, immediate implications, such as stolen data and credentials, is also an integral part of the incident response process. When a company not informs the customers after a catastrophic breach, they remain vulnerable.

When a company's data is compromised, it may face lawsuits, reputational damage and questions about its ethical standards. Delaying public announcement can strength these consequences. Those responsible for overseeing information security practices within organizations, such as CISOs and supporting executive management, must be engaged and lead by example to develop a culture of high ethical standards.

Cyber security is a critical issue for all businesses and will become more important as more devices are connected to the Internet.

Rapid technological developments have provided vast areas of new opportunity and potential sources of efficiency for organizations but have also brought unprecedented threats.

An effective cyber security strategy should be oriented to the risks faced by each organization, and should be based on the results of a risk assessment.

Organizations could be attacked deliberately due to a high profile and having valuable data (or there is some other publicity benefit in a successful attack).

Virtually every Internet-facing entity will have exploitable vulnerabilities unless it has been specifically tested and secured.

Cyber criminals observe weakness and try to exploit it. Therefore, all organizations need to understand the cyber threats.

Effective cyber security can protect critical assets of organizations, customer details and operating systems and help them to win new business by providing assurances of their cyber security commitment to their supply chain, partners, stakeholders and customers.

In order to achieve real cyber security, today's organizations have to r**ecognize that special software alone is not enough to protect them from cyber threats**.

The three fundamental domains of effective cyber security are:

- people,
- processes and
- technology.

ISO 27001

- is the internationally recognized best-practice standard for information security management.
- forms the backbone of every intelligent cyber security risk management strategy. Other standards, frameworks and methodologies need ISO 27001 to deliver their specific added value.
- will help organizations to protect their information assets in cyberspace, comply with their regulatory obligations, and thrive by assuring customers and stakeholders that the organization is cyber secure.

ETHIC PROBLEMS OF CS IN EDUCATION

Ethical aspects of using information technologies (IT) and teaching CS in education, particularly those related to production of national information resources and ensuring access to these resources are discussed in some papers (Voronkov, 2002).

People with different jobs, age groups and educational backgrounds from different countries, have different cultures in using resources available through the global computer network. This makes complicate the developing of universal standards of behavior and a system of ethical norms, which could be widely recognized in the World Wide Web (Voronkov, 2002).

By using Internet browsers there is no effective way to control the quality of such publications or to adopt particular standards and earlier mistakes requiring the development of ethical guidelines?

Woodbury (2002) believes that the “net ethics” should contribute to promoting ethical standards and increase the probability of ethically acceptable behavior of software developers and Internet users. It means that the question of quality of information sources is acquiring greater importance. The quality of information sources used in education should be of particular concern. Their reliability must be ensured.

Referring **psychological issues** additionally to individual experience in using computers, at every transition to a new objective or program with the use of computer technology it is necessary

- either to assign a special preparatory stage,
- or to allocate time and place in the educational process itself where the student could master this technology as applied to the subject he or she is studying.

Otherwise to employ computer technologies as a means of teaching can be less effective.

It is not always possible to determine the cause of the failure to achieve expected results from the use of computer technologies in the educational process when such failures occur. Such negative results can be explained by the fact that the specific learning situation cannot produce the kind of results we hoped for.
Causes could be:

- the employed technologies have limited capabilities and cannot produce the desired effects
- the incompatibility between the content of learning and the use of computer technology.

To find a **psychologically valid explanation** of the failure and to continue effectively using computers in teaching it is necessary:

- to examine the technological resources employed, the particulars of the educational

material (its objectives and tasks),
- to compare the subject and the capabilities of the employed technologies,
- to find out if and where the technologies can be successfully used.

Another important aspect of computer technology application in education is the **use of direct and mediated forms of activity**. The logic of the psychic development of human being syndicates that first, as a rule, man masters some activity and only later this activity can become mediated. For instance, first a child learns to communicate and only after he/she has mastered the skills of communication, this ability can be used as an educational means. There are similar data on the development and use of games and other forms of activity (Hanson et Palm, 2005).

Numerous psychological studies show that the direct mastering of an activity is subject to the certain logic of development. For instance, without mastering direct communication individuals cannot learn to play. If an individual cannot play, he or she will not be able to join in an organized educational process. The peculiarities of mastering computer technologies in education have not received much attention in the literature (Voronkov, 2002).

Thus, **the use of computers in education is rather ad hoc today and has little grounding in scientific analysis**. Neither is there evidence of attempts at introducing psychological control over it.

Another psychological issue is the question of the **collective and individual modes of education**. Considering the effectiveness of learning, the choice between the modes depends on the student's psychic age and on the subject to study. In one case frontal teaching is more effective, in another – work with micro-groups (a group is divided into several teams); still another case would require individual tuition.

RESEARCH RESULTS ABOUT TEACHING ETHICS IN CS

Students are taught in education the skills necessary to get them through life i.e. reading, writing, mathematics and basic social skills as parts of education. In the last years schools have integrated computer courses into their main curriculum but they are not being taught about the threats they face when using these technologies.

Research results show that fundamentals of computer science should be the higher priority but there are aspects of CS that are independent of computer science. Students are taught never to share their personal information online or to click on unfamiliar links. Cyber threats are always changing, and the students need to be taught about social engineering i.e. obtaining confidential information by manipulating and/or deceiving people.

Students have access to mobile phones, media players, televisions and game consoles, most of which can access the Internet so it is almost inevitable that they will be faced with cyber threats at multiple points in their lives. A cyber security-based curriculum could help to develop a digitally secured future workforce.

Referring formation of CSP, outside of university courses and industry certifications, there is little standardized training or formal accreditation required working as a CSP.

Computer science students, or students specializing to become a computer professional need to have, in addition a required course or some modules in computer ethics. Ethics could be a form of social and humanistic studies of CS aimed at a theoretical understanding of ethical aspects of CS or aimed at developing practical professional tools in this domain. Optimally a course in computer ethics would integrate both dimensions (Brey, 2000).

In teaching a course in computer ethics, one may of course emphasize either the more fundamental or the more applied dimension of computer ethics. In a professional program for CSP students, a course in computer ethics that is mostly applied, and that focuses on problems and dangers in CS is more adequate.

Regarding privacy, for example, it would both teach general moral theory on privacy, specific moral analyses of informational privacy, and the various ways in which privacy considerations come up in contempt rary. Computer systems and their uses, existing privacy law and policies, and professional responsibilities for CSP and ways in which professionals may deal with them.

This is necessary because they face daily ethical dilemmas unique to their line of work. Cybersecurity professionals are the technological gatekeepers in their respective organizations, entrusted with great responsibility and the high levels of access needed to carry out their roles effectively (Tavani, 2004).

How an individual manages this authority comes down to his or her own ethical yardstick, which is why organizations must carefully select security experts who exhibit sufficient standards and technical competency. But in this context, more should be done also through international projects in CS.

PROJECTS

The European project Cyber Security (www.) with partners from Education, Research, and Industry/ Business supports the European Cyber Security Strategy.

The partner'countries of the project Cyber Security have a strong strategy which is the sum of all national and international measures taken to protect the availability of information and communications technology and the integrity, authenticity and confidentiality of data in cyberspace.

Referring cyber security in VET, the project partner countries also Germany does not have any body responsible for educational and professional training programs for raising awareness with the general public, promoting CS courses and ethics in CS. There are no CS courses in vocational schools, this is a gap in the present, nor is a cyber security discipline included in the curricula of professional courses. So, one of the objectives of ERASMUS + Project cyber Security to disseminate cyber security issues in formal and non-formal education and fostering the development and skills of teachers and trainers will contribute to make progress in introducing cyber security in HE and VET.

Through short research in European Practices and Education, development of a curriculum in cyber security education including Ethical aspects, organizing seminars and conferences in schools, VET and HE institutions, development and distribution of a Book about cyber security, the project will contribute in improving knowledge and skills of students and teachers in avoiding cyber attacks. The cooperation with industry assure a practical character of the project outcomes (Hamburg and Bucksch, 2016).

CONCLUSIONS

Without codified CS ethics guidelines in place at the industry and training of students and at employer levels, it is difficult to develop the most ethically response to a given incident.

An integrated module of ethics in CS course it is also crucial to cultivate ethical teachings among students and the security professionals of tomorrow. By promoting awareness of CS ethics at the early stages of learning and professional development, it will support that future white hats stay on the right side of the ethical divide.

References

Brey, P. 2000. Disclosive Computer Ethics. Computer and Society, 30:4. pp. 10-16

Brey, P. 2005. The Importance of Privacy in the Workplace. In *The Ethics of Privacy in the Workplace*, ed S. O. Hansson, S., Palm, E.. Brussels, Peter Lang. pp. 97-118

Bynum, T., Rogerson, S. 2003. Computer Ethics and Professional Responsibility: Introductory Text and Readings. Blackwell.

Hamburg, I., Bucksch, S. 2016. Approaches for bridging research an industry. In *Archives of business research 4*, no. 1, pp. 209-215

Hansson, S., Palm, E. 2005. The Ethics of Privacy in the Workplace. Brussels, Peter Lang.

Himanen, P. 2001. The Hacker Ethic: A Radical Approach to the Philosophy of Business. New York, Random House.

Himma, K. (ed.), 2007. Readings on Internet Security: Hacking, Counterhacking, and Other Moral Issues. Jones & Bartlett.

International Telecommunication Union 2009. Cybersecurity: The Role and Responsibilities of an Effective Regulator. *The 9th ITU Global Symposium for Regulators*. Beirut, Lebanon. pp.16

ISSA: ISSA Code of Ethics. In *Information Systems Security Association Website.* http://www.issa.org/codeofethics.html (2005). Cited 14 Mar 2006.

Johnson, D. 2009. Computer Ethics, 3rd edn. Upper Sadle River, Prentice Hall.

Laurie, Graeme T. 2002. Genetic Privacy: A Challenge to Medico-Legal Norms. Cambridge UK, Cambridge University Press.

Voronkov, Y. 2002. State-of-the-Art in Ethical and Legal Aspects of ICTs n Education. In *Analytical Survey ETHICAL, PSYCHOLOGICAL AND SOCIETAL PROBLEMS OF THE APPLICATION OF ICTs IN EDUCATION.* Unesco.

Woodbury, Cook, M. 2002. Computer and Information. Ethics, Volume 1. Stipes Pub.