Role of Ethics in Information Security

Conference Paper · September 2016

CITATIONS
0

READS
3,276

2 authors, including:

Tunç Aşuroğlu
Baskent University
14 PUBLICATIONS **8** CITATIONS

Role of Ethics in Information Security

Tunç Aşuroğlu, Cemal Gemci

Computer Engineering Department, Başkent University
Ankara, Turkey
{tuncasuroglu, cgemci}@baskent.edu.tr

***Abstract*—Information is power. Nowadays, main concern of cyber community is to protect this valuable asset. Technical and technological security measures are sometimes insufficient to protect an information system. Because there is a human factor in information system. Ethics are set of moral rules that guide people. With the help of ethics a better and robust security can be achieved. In this paper role of ethics in information security is discussed. First of all law, ethics and information security concepts are briefly introduced. Later, some ethical concerns and perspectives in information security are given. To emphasize role of ethics in information security, several studies are reviewed. Finally, mechanisms to make ethical rules effective in an organization/community are discussed with several case studies.**

***Keywords*— Ethics, Ethical Issues, Information Security, Cyber Security, Information Systems.**

I. INTRODUCTION

With the advance of Information Technology, new threats and unauthorized actions arise each day. To be able to protect information assets against these threats and actions is one of the most important issues nowadays. But sometimes technical and technological measures are not enough to protect an information asset. Additional measures must be employed because there are a lot of parameters when it comes to information security. One of these parameters is people. These people can be system administrators, security professionals, employees and users. These are the people that interact with information system. In order to secure people parameter in an information system, a measure that employs moral judgment must be introduced. Computer and information ethics are studied by many researchers, scholars and practitioners [1]. To include ethical layer to information security is very important because it can fill the gap that people create.

In this paper role of ethics in information security is discussed. First of all law, ethics and information security concepts are briefly introduced. Some ethical concerns and perspectives of several researchers in information security are given. To emphasize role of ethics in information security, several studies are reviewed. Mechanisms to make ethical rules effective in an organization/community are discussed. Finally, paper finishes with conclusions and references.

II. LAW & ETHICS

Laws are a form rules that prevent certain behavior and actions happen. They are created from ethical structures. The major difference between law and ethics is: law needs an authority to process and ethics don't [2]. Ethical behavior comes from individual's conscience. Ethics are defined in the light of a group's cultural customs. But as in laws it's different, many laws are universal across the world.

Laws are the rules that all of the people must oblige to follow. If they don't follow, they will be punished. That's not the case in ethics; in ethics all people have their own will. They can choose to follow or not follow code of ethics. In ethics, it depends on a moral decision, many people agree upon ethical behaviors but some people can disagree on these.

Ethics can be seen from different approaches. These approaches are consequentialism and deontological [3]. Consequentialism claims that if actions have bad consequences they are bad after all. Deontological approaches don't think like that. They assume that actions of people have neither good nor bad consequences they have only moral duties independent of their actions.

There exists a blurriness of ethics in individual's mind but with the help of the laws and regulations security and safety can be achieved. In a cyber world, law and ethics work together to form a security layer. Ethics can fill the void where laws cannot be applied.

III. INFORMATION SECURITY

Rapid growing of information technology enables many organizations, government and civilians exchange important information every day. So security issues arise when sharing information [4]. Nowadays relationship of organizations depends on computer and information systems, many organizations are concerned about information security because they use technologies like e-commerce, mobile and virtual private networks. With the increase of involvement of these technologies, number of threats to organization's valuable assets also increases [4]. Information security protects confidentiality, integrity, and availability of information assets against various threats. Technical protection measures are not enough to provide information security. There must be other measures. To develop a robust and good information security; in addition to technical measures; operational, ethical, sociological and legal measures must be considered [5].

Organizations depend on processes, technology and people. Even if we have top of the line information systems and security, there are people operating these information systems [4]. They control daily activities and thus the entire information system. They need to have moral and ethical conducts, if they don't have these conducts they will make information system vulnerable to threats. There is no efficient technical protection of information security because people are involved [4]. People are critical on ensuring a robust

information security. So there comes ethics to rescue. People that act with ethical conscience in information systems ensure information security.

IV. Some Ethical Concerns of Information Security

A. Hacking and Computer Crime

Computer security mainly interested in protection of computer assets and important data against leaks and unauthorized access. These leaks and unauthorized actions are called hacking. Hackers are computer users that gain unauthorized access to a system and share knowledge to other users or hackers in the process. As it sounds a negative action, hacking can be beneficial in some ways [3]. White hat hackers or self-identified hackers suggest that their actions cause no harm to community. On the contrary they claim that they help development of a better security system. Because they think hacking can be used to release data to benefit all in a community [3]. They've even developed a code of ethics for hackers. They are suggesting that hackers should use a code of ethics when hacking. There is a gray area in this manner some researchers think hacking can't be ethical, some claim otherwise [6]. This is an ethical issue that information security researchers argue on.

B. Privacy & Ethics

There is no precise definition for privacy but privacy term mainly refers to "right to be left alone" [7]. Privacy doesn't only apply to personal data. It also concerns with human relationships, private belongings, actions and even our homes. Ethical issues arise in many areas of privacy including surveillance, medical privacy, internet privacy and work privacy [3].

V. Different Ethical Perspectives in Information Security

There are different ethical views in information security. Researchers proposed several models to achieve better information security.

Hartmann [8] stated that security levels couldn't consist of only a technical layer. It consists of technical, technological, organizational, legal, social and ecological levels. In addition to these levels Hartmann suggests ethical scope must be included in information security. The researcher also suggests that ethics is a so large question that developers, users and system admins cannot answer separately. Entire community should answer this question by discussing together. So Hartmann suggests that ethics should span an entire community and ethical rules should be prepared with a mixture of individuals from different areas.

Another ethical view in information security is proposed by Kowalski [9]. Kowalski stated several ethical problems and also stated that information security is threatened if these problems occur in information technology systems. These problems are as follows;

- There is a control gap in information systems and it is getting wider with every new technology. This control gap can cause problems in retaining security in information systems.
- Ethics must be a common language among individuals from different expertise. Ethics should also understandable by individuals from other communities besides computer society.
- Nowadays information systems are getting so large that it is getting harder to manage with only technological control mechanisms. So control mechanisms should be built on individuals control mechanism that can be achieved by ethical frameworks.

If these problems don't answered right there can be an opening that leads to information security issues.

As seen from given perspectives complete security of information can only be achieved by the help of ethics and ethical frameworks.

VI. Frameworks for Establishing an Ethical Baseline in Different Environments

Many researchers stated that information security is lacking without an ethical concept. So in order to establish a better security, they proposed frameworks that include ethical principles. These frameworks exist in many information environments like biomedical, e-banking and health and etc. Example frameworks will be discussed in this chapter to emphasize the importance of ethical principles in information security.

France [10] discussed ethical violations in biomedical area that leads to violation of patient privacy and medical records. He also stated some ethical codes and suggestions to overcome this security issue. These ethical codes include doctor and hospital staff jurisdictions, patient record storage, etc.

Abreu and co-workers [11] discusses fraud (phishing) in e-banking services. They point out several threats, vulnerabilities, incidents and impact of threats on e-banking services. Researchers suggested ethical rules and trainings on clients and bank personnel to overcome frauds in e-banking services. They also stated that Public discussion on incidents will develop awareness and creates a security behavior among e-banking service users.

Kluge [12] developed a code of ethics for health information professionals. He discussed several problems in health informatics domain and proposed code of ethics for several information security problems. He suggested that in addition to technical security layer in a health information system there must be an ethical layer that protects privacy of patients. He created this ethical layer on health information professionals.

VII. Making Ethical Rules Effective in Community

Making ethical rules effective in a community plays an important role in security of information. Being able to give

individuals a set of ethical rules to follow and provide an awareness of ethics will surely establish a better security layer in organizations. To provide a better and robust security of information, there are two ways: Developing a code of conduct/ethics and provide trainings to individuals so they can gain awareness in security and ethics.

A. Code of Conduct

Nowadays many organizations and communities develop code of conduct for its members to follow [13], [14]. Without the development of these codes information security will have gaps because of laws couldn't fill some gaps and ethics can. For example; in order to fill these gaps, computer ethics institute developed Ten Commandments of Computer Ethics [15]:

1. Thou Shalt Not Use A Computer To Harm Other People.

2. Thou Shalt Not Interfere With Other People's Computer Work.

3. Thou Shalt Not Snoop Around In Other People's Computer Files.

4. Thou Shalt Not Use A Computer To Steal.

5. Thou Shalt Not Use A Computer To Bear False Witness.

6. Thou Shalt Not Copy or Use Proprietary Software for Which You have Not Paid.

7. Thou Shalt Not Use Other People's Computer Resources without Authorization or Proper Compensation.

8. Thou Shalt Not Appropriate Other People's Intellectual Output.

9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.

10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans.

This code of ethics guides individuals when interacting with an information system. Code of ethics is applied to all of the members in an information system including system administrators, developers, users and security professionals. Instead of applying general code of ethics, organizations can develop their own code of conducts. In our opinion this can be prove to be most effective because to target and fill specific gaps in information security, specific ethical codes must be defined. But in order to make users abide code of ethics and to a standard there is a need for collaborative effort [16]. Awareness training helps to establish this collaborative effort.

B. Awareness Training

Awareness training and security training takes a major part in establishing security. In order to provide security there must be awareness among individuals. This awareness spans to a large definition including; ethics, threats and how to deal with them, security incidents and so on.

Awareness training must provide an appropriate security and ethics behavior to all individual in an organization in order to full commitment to security policies [17]. There are some research that focuses on awareness training and how it is effective in providing security. Stephanou and Dadaga [17] have asked the question "to what extent does information security awareness training influence information security behavior?" and they discuss existing awareness training research and proposed a model to examine the impact of training on security behavior among individuals.

Aliyu and co-workers [18] conducted a study that inspects security and ethics behavior among students. They conducted several experiments among students to find out that is awareness actually affects security. The experiments showed that the awareness training created a conscience of security among students. Because of security awareness trainings and ethics courses students are more aware of security concerns and ethics than the students who receive no training.

So according to these studies that we mentioned above, we can say that awareness training actually can affect the security behavior of individuals. Also they are crucial in making ethical rules effective in community. Because this training also gives a conscience of ethics to individuals and in our opinion is crucial to establish information security.

VIII. CONCLUSIONS

Ethics play an important role in our lives and also in cyber technology domain. Ethics fill gaps in an information system that laws can't be able to fill. In this paper the importance of ethical principles in information security has discussed. Different ethical perspectives in literature are inspected to show how ethical layer can be built on security layer. Also in this paper, to provide a solid proof that ethics complete information security, several ethical frameworks are inspected. Finally, methods to make ethical rules effective in a community are given. Several examined studies showed that awareness training and code of conducts are effective in this manner.

REFERENCES

[1] H. Taherdoost , S. Sahibuddin, M. Namayandeh and N. Jalaliyoon," Computer and Information Security Ethics' Models", International Conference on Advanced Computer Science Applications and Technologies, pp. 145-149, 2013.

[2] M. E. Whitmann and H. J. Mattord, *Principles of Information Security,* 4th edition, Course Technology Cengage Technology, 2012.

[3] P. Brey, "Ethical Aspects of Information Security and Privacy", in: *Security, Privacy, and Trust in Modern Data Management*, M.

Petković and W. Jonker (Eds.), Springer Berlin Heidelberg, pp. 21-36, 2007.

[4] E. W. Wildauer and F. B. H. da Silva, "Ethical, Social, Privacy, Security and Moral Issues in an E-Society", 8th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-6, 2013.

[5] J. Leiwo and S. Heikkuri, "An analysis of ethics as foundation of information security in distributed systems", Proceedings of the Thirty-First Hawaii International Conference on System Sciences, vol.6, pp. 213 – 222, 1998.

[6] H. T. Tavani, *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology,* 4th Edition, Wiley, 2012.

[7] B. C. Stahl, "Privacy and security as ideology", *IEEE Technology and Society Magazine*, Vol.26, pp. 35-45, March 2007.

[8] A. Hartmann. "Comprehensive information technology security: A new approach to respond ethical and social issues surrounding information security in the 21st century", 11th International Conference of Information Systems Security, pp. 580-602, 1995.

[9] S. Kowalski. "Computer ethics and computer abuse: A Longitudinal study of Swedish university students", 6th International Conference on Information Systems Security, pp. 590-602, 1990.

[10] F. H. R. France, "Ethics and biomedical information", *International Journal of Medical Informatics,* vol. 49, pp. 111-115, 1998.

[11] R. Abreau, et al., "Ethics and Fraud in E-Banking Services", 10th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-6, 2015.

[12] E. H. W. Kluge, "Fostering a security culture: a model code of ethics for health information professionals" *International Journal of Medical Informatics,* vol. 49, pp. 105-110, 1998.

[13] ACM Code of Ethics
https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct
Last accessed: 23.5.2016

[14] IEEE Code of Ethics
http://www.ieee.org/about/corporate/governance/p7-8.html
Last accessed: 23.5.2016

[15] CEI Ten Commandments of Computer Ethics
http://computerethicsinstitute.org/publications/tencommandments.html
Last accessed: 23.5.2016

[16] A. R. Philip, "The Legal System and Ethics in Information Security", SANS Institute, pp. 1-14, 2002.

[17] T. Stephanou and R. Dagada, "The Impact of Information Security Awareness Training on Information Security Behavior: The Case for Further Research", Innovative Minds Conference, 2008.

[18] M. Aliyu, et al., "Computer Security and Ethics awareness among IIUM Students: An Empirical Study", International Conference on Information and Communication Technology for the Muslim World, pp. A52 - A56, 2010.