DOI: https://doi.org/10.15388/OS.LAW.2020.5

THE DEFINTIONS OF INFORMATION AND SECURITY; HISTORY OF INFORMATION SECURITY DEVELOPMENT

Aytakin Nazim Ibrahimova[1]

Abstract. Taking into consideration its historical evolvement, it is evident that information security is not a new concept. Starting from the very moment of writing down the information, it presents by itself a data that can be protected, stolen, or destroyed. Throughout the whole history, without even perceiving it people had to take steps to guarantee the security of important information that they have been able to maintain. The concept of information security is quite dynamic. A behaviour that is generally accepted today can be a peril to an entity that we will work with tomorrow. Developing technology brings along the continuous innovation. Everyone handles personal information when it comes to technology development or service provision. Besides already existing services, it includes banking and other activities. Therefore, we should bear in mind that personal security cannot be ensured without guaranteeing security within each organization.
Keywords: information, information security, data carriers, coverage area, information systems, information infrastructure, computer and network security, history of information security development.

INTRODUCTION

Information security signifies identifying persons who possess information security, detecting soft points, preventing hazards and undertaking preventive measures and researches to guarantee information security and protection against unwanted threats (Baykara et. al., p. 233). In other word, information Security means undertaking relevant measures to protect information covered by information systems against acquisition without approval, use, modification and damage (White, 2011, p. 394). Here one should take into consideration, that notion of information security should be considered despite of the form of saving of information. In spite of the fact whether the information saved on paper or in electronic form, it is always in need of protection from those who carry and use this information in case of threats posed by them. The initial area of use of information security is issues of diplomatic and military character. Here the notion of privacy and secrecy is crucial. Initially, information security was merely a review of all measures that were meant to protect national security. However, with the development of information and communication technologies, as a result of the digitization and storage of information in the system, the problem of securely storing, protecting and using information has become a common issue for anyone who has access to information systems. With the transition to the information society and digitalization process, considering all information

[1] *PhD in Law; Deputy Dean of Law Faculty of Baku State University (BSU); Professor at the Department of "Constitutional Law" of BSU; Member of the Scientific Council of the Law Faculty, email: aytakin_ibrahimli@yahoo.com, ORCHID i-D: 0000-0002-3134-8486.*

systems, starting from personal computers to the most sophisticated information technologies that carry the information, the notion of information security has becoming significant.

1.1. THE NOTION OF INFORMATION

To grasp better the concept of information security, firstly, it is significant to understand the notion of information that is the basis of information and communication technologies. The words of information used in English (data, information, knowledge) is used as the Azerbaijani equivalent of information (Canbek, Sagiroglu, 2006, p. 168). Although, the use of such notions as data, information, and facts in relation to these terms in our language will be more appropriate.

Data: Data is digital networks that are not connected with each other. The data contained in this information system is made up of figures and does not have any meaning. (for example: 1.400; 6.3 or 29,000 AZN). On the other hand, data provided by information technology can be explained as still unrelated information about one issue or, to put in short, as existing and moving signals in the digital environment.

Information: structured and correlated data. In order to be used data should be transformed into information. One data must be converted into an information form so to be used and applied. The data contained in the information system provided in the form of text message can be transmitted to the user in a cogent and structured way

Knowledge: Knowledge can be defined as the acquisition of experience and knowledge or perceiving realities, truth by internal observation. The knowledge can be divided into 4 classed depending on identifying what is to be known, why, how it should be known and who is the actor. The answer to these four main questions delineates the area of knowledge.

The mentioned concepts, such as data, information, knowledge, in addition to being theoretical, have a number of practical implications.

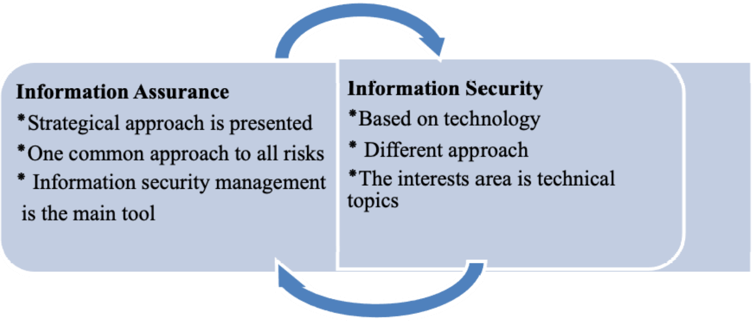
Data carriers

These are the carriers that constitute whole management system and cover all information in one information system that can be appreciated, written down. Some of these carriers are essential for ensuring the operating system and they are called key information carriers. The main target of information security is to ensure that the information in the information system is fully accessible and secure. Network browsers that are used to access such sources as databases, e-mails, and network servers given in one information system can be regarded as the main data carriers of the information system.

1.2. INFORMATION SECURITY AREA

The concept of information security signifies the notion of security that includes the personal computers and networks, corporate and national networks and covers information systems in a broad sense (Asia-pacific publication catalogue. 2008). Information system on the corporate level includes also software, users as a third party and technical support systems. Information security means guaranteeing secure storing and processing data without distorting it and preventing unauthorized access to it in the digital environment.

To guarantee this relevant security policies should be defined and applied. These policies namely reviewing activities, following up the process of acquiring data, evaluation of the registration process of updates, deleting data are presented as limitations to some rules of application. In general, information security can be considered as a part of "security establishment" that overall covers security topics (Canbek, Sagiroglu, 2006, p. 171). On the other hand, information security in the broadest sense of the word connected with cryptology, risk management, security culture. The notion is still extending. The concept of "information security" in English is being translated into Azerbaijan using the similar wording. It would be relevant to translate the notion "information assurance" in an analogous way. To consider on a strategical level technical and temporary needs that are important to guarantee information security in the information systems in the realm of information assurance, the notion "information security" should be interpreted in more tactical way.


Information Assurance
*Strategical approach is presented
*One common approach to all risks
* Information security management is the main tool
Information Security
*Based on technology
* Different approach
*The interests area is technical topics

Source (Information Assurance versus Information Security, 2011).

Furthermore, the main definitions connected with information security are information systems and information infrastructure.

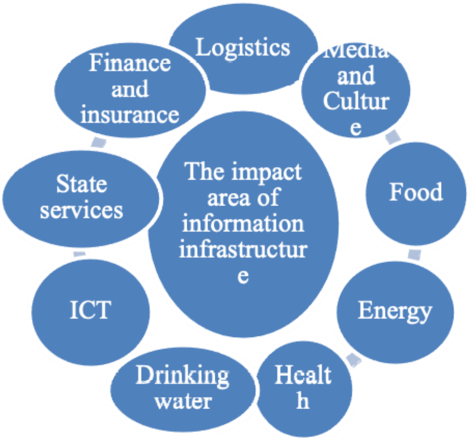
1.3. INFORMATION SYSTEMS

An information system is a tactical, controlling and supportive system applied among user and information technologies in reciprocal interaction (Trustworthy Refinement Through Intrusion-Aware Design). In this sense, the information system cannot be considered as only about the problems of information and communication technologies, but also as the ways in which people use them to interact with these technologies that support their work life. Nowadays, information systems are increasingly computer based. However, along with computers internet, world wide web, equipment, connection systems are significant for activity of digital based information system. On the other hand, besides personal computers powerful information systems such as technologically complicated super computers possess such qualities as maintaining information, accessibility of information, storing.

1.4. INFORMATION INFRASTRUCTURE

From the perspective of information security, the role of information infrastructure is crucial. There is still no common approach to this infrastructure around the world. Each country has its concept of an information infrastructure within its own terms and needs (National Information Security Center, Japan, “Second Action Plan on Information Security Measures for Critical Infrastructures”, 2009, p.10). However, while considering common features, it is possible to give an overview of networks, systems and structures that may have a negative impact on the continuity of public order or the performance of public services in case they do not perform their functions partially or completely (Ünver, Canbay, Özkan, 2011, p.4).

The impact area of information infrastructure (Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe):



Sustainability of information infrastructure and adaptation to the community need are of the utmost significance. The aftermath of incidents such as the electrical breakdown in the Northeast America in 2003 and the nuclear leak as a result of the tsunami in Japan further underscores the importance of infrastructure security in ensuring information security. One should also emphasize, to guarantee infrastructure security one should take complex approach to the issue (Turhan, 2010, p.8).

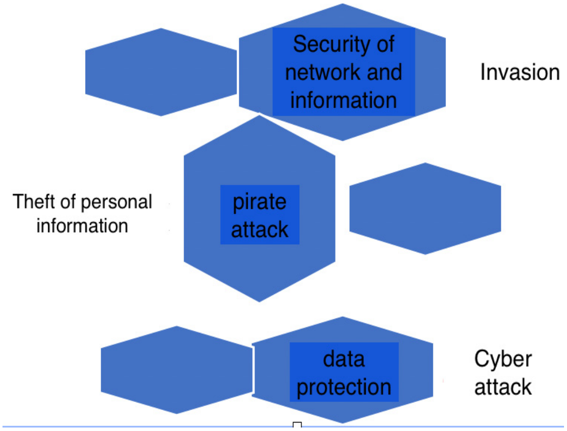
1.5. THE AIM OF INFORMATION SECURITY

The purpose of information security is to provide continuous, secure and qualitative service while implementing activities of the information system. On the other hand, maintaining professional image and reliability, protection of data carriers, and preventing unauthorized access are also key goals and priorities of information security.

The main issue targeted by information security is to prevent any attacks on the integrity, confidentiality and usage of the information system, and to eliminate any security weaknesses that may cause these threats. Although from the perspective of the definition itself one might find it easy, the security of information systems is increasingly difficult to maintain in the age of increasing cyber-attacks. From this point of view, it is potent to know what the risks and threats to information systems are in order to make information security activities more efficient. There are numerous regulations and policies regarding information security. Among them the following can be considered as of main significance: computer and network security, information security management systems, information security management, cryptology, cyber security, cybercrime, data confidentiality and protection, national security and international relations.

1.6. COMPUTER AND NETWORK SECURITY

As a result of the application of information security to computers and networks, the concept of network and computer security has emerged. Computer and network security is series of activities directed at preventing unauthorized access to network equipment and programs that interconnect computers, modification or deletion of system data. Computer security is also a way to secure and to provide safe access to information protected in information systems in case of unforeseen events such as natural disasters.


Security of network and information
Invasion
Theft of personal information
pirate attack
data protection
Cyber attack

Network security technically differs from the concept of computer security. Computer security protects the computer-based information system against threats and attacks, while network security protects the network used by more than one computer to interconnect from potential hazards. Network security implements detecting threats to the network and preventing mechanisms while, on the one hand, securing safe accessibility to the network and, on the other hand, analysing protecting and preventing undertakings against security threats (Joshi, 2008, p. 62). The need to ensure the security of network technologies has a great impact on shifting from the concept of national information security to the national cyber security concept in the process of the development of internet technologies which are widely used in the network. In fact, the crosscut for all close definitions such as information technology security, cyber security or digital security is the security of information systems. Implementing areas and reciprocal impact of information security policy (Commission of the European Communities, Brussels, 2001) (see figure).

1.7. HISTORY OF DEVELOPMENT OF THE INFORMATION SECURITY

Although the notion of information security became more popular after the introduction of computer the our lives, it is well known that information has been used since the first times of the history of humanity as a social and economic value, and it has always been prevented from being disclosed to the people, who were not supposed to have it. The discovery of writing provided the opportunity to store information and experiences, transfer it to others and use again when needed. Nevertheless, it is reality that this opportunity is granted only to those, who are literate. The articles found through archaeological excavations show that ancient human used more complicated alphabets, compared to the modern alphabets. According to Canadian historian Harnold Innis, ancient humans achieved to keep the power of information within certain group or class in society, by creating "information monopoly". The hieroglyphs in Ancient Egypt formed quite a complicated and difficult alphabet and was able to be read by Jean Francois Champollion only in 1820 (Harold, 2007, p.44).

During ancient times, the confidentiality of the written communication among kings, leaders and politicians were being protected with special seals and glues. The characteristics of "Caesar coding technology", named after its inventor Roman military general Julius Caesar, were very effective for its time, and was never decoded by his competitors. During the Middle Ages, there have been special security methods such as coding, special locked boxes to protect the written communication between kings and their ambassadors. Invention of electricity during industrial revolution enormously contributed the development and spread of communication technologies, thus resulted breakthrough in information security in the sector of communication with signals, voice and image carried through electrical current. Created with the usage of electricity, simple communication devices, telegraph and radio were used with trade purposes at first, and there were well-spread believes that these devices were highly secure. In 1903, there was a long-lasting professional rivalry between two famous inventors of these times in England, Sir John Ambrose Fleming and Nevil Maskelyne. The first computer hacking happened during the public introduction of radio receiver and transmitter, the devices which were considered of maximum security, invented by another eminent inventor of this time, Guglielmo Marconi, when Fleming secretly hacked the security and voiced rude messages in front of the spectators (Dot-dash-diss: The gentleman hacker's 1903 lulz, 2011).

The hacking of the Enigma Encryption System by Polish cryptology experts and mathematicians Marian Rejewski, Henryk Zygalski and Jerzy Rozycki, which played huge role in defeating Germans before the World War II is one of the accepted turning points in the history of information security.

Called Enigma and used by Nazi Germany for the coding and decoding of communication, this code machine had very complicated encryption algorithm for this time.   It is accepted that, this hacking which led to the revolution in the field of encryption had a big role in changing the results of the World War II.

Scientists such as Alan Mathison Turing, who is considered one of the founders of computer science and the inventor of the World's first digital and programmable computer Colossus, Thomas Harold Flowers are well-known mathematicians were the members of the team who hacked complicated German encryptions during the war.

The information period starting with the introduction of the first computers to human life after the World War II led to the introduction of the notion of information security as well. Surely, these computers were not used to store information and communicate through internet as in our times, and mostly appeared as a product of the encryption technology, which had vital importance during the World War II. During this period, within the circle of information security notion, using the opportunities of any type of audiovisual technology, including encryption technologies was limited with the purpose of preventing unauthorized entrance to civil and military areas where sensitive information regarding state security was preserved. Thus, information security at this period can be described as the actions against the risks of spying, information theft and sabotage. On the other hand, with the spreading usage of computers in military bases and the development of the opportunity to store documents in computers, prevention of gaining access to these documents and their unauthorized copying entered to a stage of adaptation with information security.

Developed by USA as a military project product and aiming to protect military communication even during nuclear attack Advanced Research Procurement Agency-ARPA and Advanced Research Projects Agency Network-ARPANET were created as the first form of the modern internet in 1968. Initially the was confidence regarding the security of ARPANET, however later on it was discovered he has time risks as well. A detailed report was created regarding these information security risks and actions to prevent them.

With this report, which was name as "RAND report R-609-1" it was certainly disclosed for the first time that even though the information systems look secure when they are disintegrated from each other, then these systems are connected through terminals, unpredictable information security risks can appear. This finding mentioned in a 45 years old report regarding the risk factors concerning information security when the systems are integrated in the project that was called as the first form of internet, ARPANET is very important to understand the coverage area and the scale of the concept of information security.

In 1990, when with the efforts of Tim Berners-Lee the global network project (world wide web-www) was implemented by a group of scientists in the European Organization for Nuclear Research (CERN), the ideas of science-fiction writer Sir Clark regarding a global network communicating through internet since 1970 came to life[2]. Called World Wide Web, this project enabled personal computers and information systems located in various places of the world to contact each other and in short, completed the establishment the network which we call internet.

The global information exchange stepped int a new development stage with the commercialization and civil usage of the internet. This also created opportunity for the increasing usage of internet for economic and social benefits. On the other hand, internet technologies lead to both quantitative and qualitative increase of information risk for the information systems and technologies. After the wide spread of internet, physical contact and accessibility need to gain information have been removed. It is a common case to face an attack against one information system by a hacker located in other side of the world. Even though governments turned blind eye for the computer attacks in the beginning of internet era, in our times cyber criminals are brought to justice and are being judged with cyber-crime laws, added to the traditional crime laws of pre-internet times. In previous times, governments preferred implementing punishments for the criminals, instead of taking effective precautions. The ineffectiveness of this method and the need for solution was not skipped by international organizations such as OECD, UN, NATO and EU, and several researchers have been started in this field. In this regard, with the international cooperation OECD has prepared Instructions regarding the Security of Information Systems and Networks, which was the first document with international status (OECD Guidelines for the Security of Information Systems and Networks, 1992), resulting from the importance of need for developing a legal procedure for the fight against cybercrimes and creation of international standards, which should be followed by all countries.

With the spread of internet usage in 1990s, the dangers aiming information systems appeared on internet as well. A number of organizations which discovered the commercial side of internet got involved a tense competition for taking the maximum share from this field of trade. The side effect of this competition was the very speedy innovations of information systems and transition to a new stage to make the best usage of these newly developed programs.

Nevertheless, the development and modernization of information systems and the applications presented by these systems with this modern approach could not be followed by the modernization security precautions and the level of security was overlooked as a result of the development period which did not match the main principles of information security: confidentiality, integrity, accessibility. If the usability-security balance, which is one of the main topics of information security is disturbed for the benefit of usability, facing several serious problems in terms of security is inevitable (Cavelty, 2012, p. 72).

[2] According to Clark, it would be possible to have the devices in our houses, which would bring all information to our hands and would combine the functions of photocopy, telephone, TV and small computers. These devices would allow people to contact other people on the other side of World via satellites.

1.8. CONCLUSION

Since the beginning of 2000s, as a result of interaction between information systems and computer networks as well as their users through internet, a large cyber space called internet was formed. Thus, both internet technologies, which made the life easy by offering unbelievable opportunities and a favorable condition for attacking humans or groups were formed. As a result, there was a boom in the cyber-attacks made through internet. The connection of information security with national and governmental security was understood in a more precise way. National security was enlarged with maintaining the security of information systems, which simply interacted with each other and worked on interdependence.

Bibliography

1. Baykara, M., Daş, R. Ve İ. Kardoğan., Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. 1st International Symposium on Digital Forensics and Security, Elazığ.

2. Canbek G., Sağıroğlu Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Gazi Üniversitesi Politeknik Dergisi, Cilt: 9 Sayı: 3.

3. Turhan, M. (2010). Siber Güvenliğin Sağlanması, Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri, Bilgi Teknolojileri Kurumu Uzmanlık Tezi, Ankara.

4. Ünver, M. Canbay, C. Özkan, H.B. (2011). Kritik Altyapıların Korunması, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, 1 basın.

5. Commission of the European Communities, Brussels (2001). Accessed 14 November 2019. Accessible via the internet at: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwigy-WwtenlAhWKw6YKHQ90BbgQFjAAegQIBBAC&url=http%3A%2F%2Fwww.europarl.europa.eu%2Fmeetdocs%2Fcommittees%2Fdeve%2F20020122%2Fcom(2001)366_en.pdf&usg=AOvVaw3wWb9jOR0RiZtKkGDqPIEy>.

6. White, Daniel M. (2011). The Federal Information Security Management Act of 2002: A Potemkin Village 79 Fordham. Rev.

7. Harold, I. (2007). Empire and Communications, Dundurn Press, Toronto.

8. Joshi, J. (2008). Network Security: Know It All, Morgan Kaufmann.

9. National Information Security Center (2009). Japan Second Action Plan on Information Security Measures for Critical Infrastructures, The Information Security Policy Council, Japan.

10. New Scientist Magazine (2011). Issue 2844, Dot-dash-diss: The gentleman hacker's 1903 lulz, accessed 11 November 2019. Accessible via the internet at: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjH_92WsunlAhVNURUIHS2PDkMQFjAAegQIAxAB&url=https%3A%2F%2Fwww.newscientist.com%2Farticle%2Fmg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz%2F&usg=AOvVaw33_n52yFHQWmPjM1goV8pE>.

11. OECD (1992). Guidelines for the Security of Information Systems and Networks, accessed 9 November 2019. Accessbile via the internet at: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=2ahUKEwiq8LjdzdrlAhWq5KYKHaTcBnQQFjAEegQIBRAC&url=http%3A%2F%2Fwww.oecd.org%2Fsti%2Fieconomy%2F37418730.pdf&usg=AOvVaw3GxN5f6STT9j3yxKZqdmx1>.

12. Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, Schutz Kritischer Infrastrukturen, accessed 6 November 2019. Accessible via the internet at: <https://www.kritis.bund.de/SubSites/Kritis/DE/Home/home_node.html>.

13. Cavelty M.D. (2012). Cyber (Un)Sicherheit: Grundlagen, Trends und Herausforderungen, Polit Bild.

14. Asia-pacific publication catalogue (2008). Accessed 17 October 2019. Accessible via the internet at: <http://ina.bnu.edu.cn/docs/20140520102905252150.pdf>.

15. NovaInfosec, Information Assurance versus Information Security (2011). Accessed 10 October, 2019. Accessible via the internet at: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjk_b7OsOnlAhXhVBUIHSXCBm4QFjAAegQIABAB&url=https%3A%2F%2Fwww.novainfosec.com%2F2011%2F08%2F30%2Finformation-assurance-versus-information-security%2F&usg=AOvVaw0gcGPgp69kWnGsIVnZFZrU>.

16. Trustworthy Refinement Through Intrusion-Aware Design, accessed 13 November, 2019. Accessible via the internet at: <http://web.archive.org/web/20070903115947/http://www.sei.cmu.edu/publications/documents/03.reports/03tr002/03tr002glossary.html>.