CYBERSECURITY IN EDUCATIONAL SETTINGS

Ahmet YILDIRIM[*]

Abstract

Cyber security has gained currency recently since technology and internet started to play a pivotal role in our lives. Moreoever, as most of the organizations carry out their operations and store their work in cyber settings, the notion "cybersecurity" has become more significant. Educational settings are the places in which "cybersecurity" has gained importance as databases of educational settings involve the data about students, staff, parents, resources and budget. Furthermore, the fact that educational settings are the places in which new information is created and databases of educational settings include data about this new information renders educational settings more and more vulnerable to cyber threats. In addition to that, students as shareholders of educational settings may confront cyber threats such as cyber bullying more in their daily lives. In the present article, cyber security was defined, the aims of cyber threats were summarized. How vulnerable educational settings and students are to cyber threats was put forward. Lastly, what could be done so as to provide cybersecurity at the nation level and especially in educational setting was discussed.

Keywords: Cyber security, cyber threats, educational settings.

EĞİTİM ORTAMLARINDA SİBER GÜVENLİK

Özet

Teknolojinin ve internetin yaşamımızda daha fazla rol almaya başlaması ve pek çok kurumdaki işlerin siber ortamlarda yürütülmesi ve saklanmasıyla birlikte siber güvenlik, daha önemli bir konu haline gelmiştir. Siber güvenliğin önemli bir kavram haline geldiği yerlerden biri de eğitim ortamlarıdır. Eğitim ortamlarına ait veri tabanlarında; öğrenciler, personel, veliler, kaynaklar, bütçey ve bilginin üretildiği yer olarak üretilen bilgiyle ilgili pek çok verinin bulunması, eğitim ortamlarını siber tehditlerle karşı karşıya bırakmaktadır. Bununla birlikte, eğitim ortamlarının bir paydaşı olan öğrenciler siber tehditlerle, siber zorbalıkla gündelik yaşamda daha fazla karşılaşabilmektedirler. Bu yazıda, siber güvenlik kavramı tanımlanmış, siber tehditlerin amaçları ortaya konulmuş ve eğitim ortamları ile öğrencilerin siber tehditlere karşı nasıl savunmasız oldukları tartışılmıştır. Son olarak da ülke genelinde ve özellikle eğitim ortamlarında siber güvenliğin sağlanması için yapılması gerekenlere kısaca değinilmiştir.

Anahtar Kelimeler: Siber güvenlik, siber tehditler, eğitim ortamları

[*] PhD, Ministry of National Education of Turkey. Can be accessed via yildirimahmat@yahoo.com.

Introduction

The information technology has developed recently and offered many opportunities and threats. Technology is everywhere and an integral part of life. However, information and computer technology is vulnerable to attacks. As a result, concerns about preserving information systems from cyber attacks have been addressed by many experts and policymakers (Fischer, 2016). According to Saluja, Bansal and Saluja (2012) we are getting more and more cyber generation. As a result, youth is getting more and more exposed to latest technology. This fact enables them to utilise the internet for different purposes. However, this also puts them at risk. With the onset of internet for personal purposes, there has emerged a new language. Computer pirates known as hackers investigated the mysterious world of the internet and demonstrated what could be done via the use of internet. The target of the hackers has sometimes been an individual internet user and sometimes corporates or pivotal institutions of the countries. The first hacking operations were conducted for personal interests. However, now hacking operations have posed a threat for countries' security and safety (Kara, 2013).

The principal elements of internet are computer, users and net. In the first years of development of internet, solely one computer could reach the main computer. The concept "net" emerged with the development of processors and communication protocols necessary for the access of two computers to the one computer simultaneously. With the development of "file transfer protocol" and "transmission control protocol", many users started to connect the main computer. With the development of wireless communication, net technology has gained much more importance (Bıçakcı, 2014).

Industrial age reigning 19th century was replaced with information age in the last quarter of 20th century. Capital, raw materials and workforce representing power in the industrial age were replaced with data and information in information age. As a result, information has become a factor of production and started to provide input for socioeconomic activities and facilities. Information age enables every kind of information (data, visuals, sounds etc.) to be expressed in numerical terms, stored and communicated in electronic spaces. Internet allowing numerical information to be communicated to various systems has been the dominant technology in aforementioned technological facilities. Information age has led to many significant changes in many different parts of life and it rendered many critical

infrastructures such as the fields of finance, electronic communication, transportation, energy, education and health dependent on itself (BTK, 2009). Critical infrastructures correspond to physical, technological services, systems that may influence the health, security and economic wealth if they are harmed. Information and communication are some of the critical infrastructures all around the world.

The fact that computers have been portable and access to internet has been common all around the world has been shaping the communication and exchange of information. Information technology makes people closer to each other, alters the communication habits. However, it may also cause unexpected problems (Bıçakcı, 2014). Organizations and institutions have become e-organizations and e-institutions with the use of network technologies. Schools and educational settings also provide many services on internet via internet pages (Çetin, Gundak and Çetin, 2015). The birth of cyber space has brought about many security risks for both individual users and national states. Those who organize cyber attacks may target financial institutions or they may capture national secrets and destroy the internet and national infrastructure (Bıçakcı, Ergun and Çelikpala, 2015).

Cyber Security and Cyber Crimes

The number of internet users has reached 2.3 billion. The number of internet users and the high dependence on internet have led to some security concerns. The first threats were about the physical infrastructure of internet. However, now the threats range from malicious codes and softwares to computer viruses. One of the problems faced within the framework of cyber security is the balance between freedom and cyber security. While trying to uphold cyber security, it is also necessary to keep the right to freely reach information and fight against cyber censorship (Öğün and Kaya, 2013). Cyber security refers to the all policies, security concepts, security instructions, approaches to risk management, training activities serving the aim of preserving the institutions in cyber spaces. The institutions, with the dependence on information technology, store the information about their personnel, infrastructure, practices and services in cyber space. Cyber security entails the formation of security properties in the way that resists security risks in cyber space. Moreover, the principal aim of cyber security is to ensure accessibility, integrity and confidentiality of information. Accessibility of information refers to the reachability of information when the need arises even if the malicious cyber attacks occur. The integrity of information refers to the completeness and

remaining of information unchanged. Especially for the sectors that are sensitive to the correctness of the information such as health and industrial design, the integrity of information is vital. The confidentiality of information corresponds to the prevention of the information from being captured by the unauthorized people (BTK, 2009).

Bardas and Ou (2013) assert that cyber security has become a priority for nations and organizations. Cyber security is a term that entered our lives in the post-cold war in a reaction to a mixture of technological developments and altering geographical conditions. Cyber security was first coined by computer scientists in the very beginning of 1990s so as to highlight a variety of insecurities relevant to networked computers (Hansen and Nissenbaum, 2009). Cyber security is the capacity to preserve and defend an institution's use of cyber space from a cyber attack committed via cyber space with the objective of "disrupting, disabling, destroying or malevolently controlling a computer environment/infrastructure; or destroying the integrity of the data or stealing controlled information" (IIROC, 2015).

Cyber crimes take place in Turkish Criminal Law under the heading of "Crimes in Information Technology". In the legislation, it is stated that the capture of computer programmes, data or other elements from a computer illegally or using, transferring or copying these data sources in contrary to law is a crime (Bıçakcı et al., 2015). In order for the precautions against cyber attacks to be successful, national policies and strategies should be developed (Yılmaz and Sağıroğlu, 2013).

The amount of data continues to increase without stopping. Businesses are getting basically more and more dependent on information technologies. Cyber criminals are aware of these susceptibilities. Cyber criminals are driven by lots of motivations to cyber attack such as obtaining financial gain, raising the profile of an ideology and terrorism. Individual cyber criminals, activists or organized hackers and states are attacking government and corporate networks with increasing frequency (KPMG, 2014).

Aims of Cyber Threats and Crimes

Cyber crimes include sexual crimes, child abuse and terrorism (New York State Office of Homeland Security and New York State Board of Education, 2004). Cyber threats consist of

cyber attacks and cyber crimes committed in cyber space. Cyber threats could be categorized to five subgroups (BTK, 2009; Öğün and Kaya, 2013):

- Denial of service,
- Malicious software,
- Phishing,
- Spam e-mail,
- Monitoring the network traffic.

Denial of service attacks render information technologies busy via data traffic and make the provision of services impossible. Malicious software could be grouped as the following:

- Computer viruses,
- Worms,
- Trojans,
- Key logger software,
- Adware sent for commercial purposes,
- Spyware used for collecting information for the purpose of intelligence.

Computer viruses are software programs involving codes which are possible to give harm to the confidentiality, integrity and accessibility of data stored in computers. They can reach other computers and they are contagious.

The ultimate aims of cyber threats are the following (BTK, 2009):

- Unauthorized access to information and communication systems,
- Replacement, elimination and disclosure of data,
- Denial of the service.

Cyber threat is not only about a cyber attack, harm or an undeserved gain as a result of this attack. In addition to that, internet may be used by cyber terrorists as a means of communication and propaganda (Öğün and Kaya, 2013).

IIROC (2015) defines the risks of cyber threats as the following:

- Disclosure of confidential account or customer data- risking an institution's most valued relationships,
- Counterfeiting,
- Loss of cognitive and mental property,
- Destruction of central infrastructure,
- Financial loss,
- Devastation of financial organization's cyber assets,

- Causing embarrassment and reputation risks for organizations.

Both the accessibility and distribution of the numerical information available in information technologies and the increase in infrastructures and systems dependent on information technology has made information technology vulnerable to cyber risks and attacks. Dependence on information technologies has posed a threat for social, political, economic and military institutions. Therefore the magnitude of cyber attacks and risks has made the concepts “cyber security” and “protection of critical information and infrastructures” central issues in the field of information technology (BTK, 2009).

The cases of cyber threats occur as in the following (Öğün and Kaya, 2013):

- The deletion of main pages of internet sites which are accessible to public,
- Capturing the files available in the aforementioned internet sites and stealing them,
- Changing the available files,
- Making the internet sites unaccessible by cyber attacks,
- Loading viruses or malicious software to the personal or institutional computers,
- Conducting cyber propaganda or disclosing confidential information about institutions.

Cyber Security and Schools

As the significance of electronic information and network technologies improve, cyber security is increasingly getting more and more pivotal for the success of all institutions (Universities UK, 2013). Cyber security in internet use is a fact that emerged after the design of internet. Internet is a system that is based on the fact of accessibility. So, while internet was developed, the developers gave priority to user-friendliness, cost-effectiveness and universality. The developers of internet did not consider the fact that internet users may give harm to internet systems (Öğün and Kaya, 2013).

Security of data and information is exceptionally vital for all businesses. Many businesses keep the records of customer information, personal files, bank account details. Schools keep the records of students, their personnel, families of the students. If these records were captured by criminals or hackers, it could be have dangerous results.

Electronic data is in the heart of a university’s facilities. As a result of this fact, protection and safety of this electronic data is pivotal for a number of reasons (Universities UK, 2013):

- Universities produce data as a core intellectual resource that is required to be kept, reached and utilised decently to understand its academic value,

- Universities depend on attainability to sensitive data from third-party organizations such as clinical data which is supplied by medical institutions,
- Universities collect data relevant to their work stuff such as data about students, budgets or personnel.

As a result of the fact that schools and universities are the producers and users of massive data sources, they are more vulnerable to cyber threats and attacks. That's why, it is necessary for them to develop cyber security facilities.

Saluja et al. (2012) recommend a curriculum of cyber security to be implemented at schools. The curriculum should include the following:

- Cyber threats,
- How users can preserve themselves and their computers,
- Cyber ethics,
- Cyber crimes.

Now in Turkey many schools have internet access, computer labs and multimedia learning centers. To be able to make learning and teaching more effective, most schools were provided with internet access services. However, there are many risks that cyber space brings about.

Cyber Security and Students

Cyber crimes have risen recently. Most of the students are unaware of the risks internet poses for them. As a result, the students are more vulnerable to cyber attacks and threats. They share lots of information, pictures in social media and other cyber spaces. However, they need to think before sharing. They need to use strong passwords and backup their data.

Given the fast and constant increase of cyber threats to schools; organizations and institutions urge the relevant people to develop security education and awareness programs that are persistent and compelling (Payne, 2003). Cyber security in the educational settings include many components. They include the privacy and security of personnel and student information and administrative information such as financial systems, grades of the students and confidential correspondence between school administration and other stakeholders (New York State Office of Homeland Security and New York State Board of Education, 2004).

Cyber-stalking, cyber bullies and sexual harassment in internet are also threats for students. The malicious people may create fake identities in internet. The students are susceptible to these threats. Moreover, cyberbullying is also a problem students confront in especially social

media. The anonymity of the internet causes the exploitation of the students (New York State Office of Homeland Security and New York State Board of Education, 2004).

The Provision of Cyber Security

The magnitude of dependence on cyber space and internet has made cyber security indispendable for institutions and nations. It is nearly impossible to detect those who conduct cyber attacks because the cyber attackers rarely leave traces behind them and even try to hide their own locations (Bıçakcı et al., 2015).

Cyber security is an immature field. There is a lack of trained personnel in this field. So, the first thing to do against cyber threats is to raise awareness in individual and institutional level. Moreover, cooperation of schools with other institutions may provide exchange of information about precautions about cyber security.

Erol, Şahin, Yılmaz and Haseski (2015) and IIROC (2015) recommend the following in order to keep cyber security high:

- Having an antivirus program,
- Keeping security software up to date,
- Having complex passwords,
- Making a backup of the files in the computers,
- Deleting insecure e-mails,
- Keeping away from sharing private pictures in social media,
- Keeping away from doing shopping based on the advertisements in social media sites,
- Appealing to the law in case of cyber threats.

As software-based precautions are not sufficient, the physical infrastructure of internet should be protected as well (Öğün and Kaya, 2013). To reach schools' information technology security purposes, it is necessary to take security precautions on the following different security controls (The Government of the Hksar, 2007):

- Physical security – preventing direct access from circumventing cyber security,
- Access control – preventing unauthorized reach to system resources.
- Data security – preventing data from destructive viruses, power failure, software failure and malicious software,
- Network and communication security – monitoring internet users at schools,
- User awareness and education – providing education and training for internet users.

Moreover, internet users should get training in the field of firewall and port. Web applications should be constructed in a very secure way that is out of reach for irrelevant users. Softwares

should be developed in a secure way and confidentiality of source codes shouldn't be violated. Private sector and public sector should cooperate to eliminate the risk of cyber threats. Schools or educational institutions should get technical support from private companies or competent institutions (Öğün and Kaya, 2013).

Training is one of the effective ways of fighting against cyber threats. The equipment of personnel, students and teachers with information about cyber security in both individual and institutional level may minimize cyber threats. Risk assessment and probable cyber attacks should be anticipated and possible action plans should be developed. Bardas and Ou (2013) argue that setting up a cyber security lab so as to give the students the possibility to realize various offensive cyber security activities is necessary. Moreover, they argue that cyber club could be set up and cyber defense courses might be planned. In the club, hands-on activities and tools could be used. Moreover, schools may prepare cyber security action plans, security programs aiming to preserve school or school-related internet pages from cyber threats or attacks. Furthermore, cyber security intervention teams may also be established. Limited information or data could be shared with the outsiders.

Tikk (2011) recommends ten rules for cyber security. They are listed as the following:

- *The territoriality rule*: Territoriality tenet makes institutions and nations more powerful to foist their dominance on information infrastructure taking place within their terrain.
- *The responsibility rule*: It refers to the fact that a cyber attack that has been performed from an information system taking place in a state's terrain is an evidence showing that the act could be attributed to that state or institution.
- *Cooperation rule*: It refers to the fact that a cyber attack which has been committed via information systems taking place in a state's terrain leads to the duty to collaborate with the victim state.
- *The self-defence rule*: Every nation and organization has the claim to self-defence.
- *The data preservation rule*: The data available in an internet site of an institution or an organization should be perceived as personal unless they are supplied for other people or organizations.
- *The mission of "care rule"*: Every organization has the charge to implement a reasonable level of cyber security in their organizational information infrastructure.
- *The early warning rule*: It is necessary to warn possible victims about unknown and probable cyber threats.

- *The attainability to information rule*: The public has the right to be made knowledgeable about the threats to their life and safety.
- *The delinquency rule*: Every nation has the duty to involve the most prevalent cyber crimes in their criminal and delinquency law.
- *The mandate rule*: Every institution has the duty to cooperate and coordinate in global cyber security.

If schools are designed as e-organizations, security systems should be established by taking into consideration the following (Çetin et al., 2015):

- The users should be identified,
- Access to the systems should be controlled,
- Alternative servers should be used,
- Users should be monitored,
- IP addresses of computers should be kept.

New York State Office of Homeland Security and New York State Board of Education (2004) recommends schools to pay attention to the following:

- Protect your user ID and password and change it constantly,
- Never share your password with anyone and don't write it down,
- Create a strong password that is difficult to guess,
- Don't reuse your previous passwords.

Conclusion

As educational settings have become more and more dependent on cyber space, they have accordingly become more and more susceptible to cyber threats. The magnitude of the data educational settings keep in their data base and the students of these educational settings who are vulnerable to cyber threats motivate cyber criminals to target educational settings. In order to protect educational settings and students from cyber criminals and not to short-circuit educational facilities, cyber precautions aforementioned should be taken.

REFERENCES

Bardas, A. G. and Ou, X. (2013). *Setting up and using a cyber security lab for education purposes*. Retrieved December 30, 2017, from http://people.cs.ksu.edu/~bardasag/publications/cdc2013.pdf

Bıçakcı, S. (2014). Nato'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. *Uluslararası İlişkiler*, 10(40), 101-130.

Bıçakcı, S., Ergun, D., Çelikpala, M. (2015). *Türkiye'de siber güvenlik*. Ekonomi ve Dış Politika Araştırmalar Merkezi. Technical report.

BTK (2009). *Siber güvenliğin sağlanması: Türkiye'deki mevcut durum ve alınması gereken tedbirler*. Bilgi teknolojileri ve iletişim kurumu raporu.

Çetin, H., Gundak, İ. and Çetin H. H. (2015). E-işletme güvenliği ve siber saldırılar üzerine bir araştırma. *Çankırı Karatekin University Journal of Institute of Social Sciences*, 6(2, 223-240.

Erol, O., Şahin, Y. L., Yılmaz, E. and Haseski, H. İ. (2015). Personal cyber security provision scale development study. *International Journal of Human Sciences*, 12(2), 75-91.

Fischer, E. A. (2016). *Cybersecurity issues and challenges: in brief*. Congressional Research Service Report.

Hansen, L. and Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, 53, 1155-1175.

IIROC (2015). *Cybersecurity best practices guide for IIROC dealer members*. Technical report.

Kara, M. (2013). *Siber saldırılar – siber savaşlar ve etkileri*. (Unpublished master's thesis). İstanbul Bilgi University, İstanbul.

KPMG (2014). *Cyber security: it is not just about technology. The five most common mistakes*. Report. Sweden.

New York State Office of Homeland Security and New York State Board of Education (2004). *Best practices for school safety and security*.

Öğün, M. N. and Kaya, A. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. *Security Strategies*, 9(18), 145-181.

Payne, S. (2003). Developing security education and awareness programs. *Educause Quarterly*, 4, 49-53.

Saluja, S., Bansal, D. and Saluja, S. (2012). Cyber safety education in high schools. *International Conference on Computer Technology and Science*, 47, 107-112.

The Government of the HKSAR (2007). *Information technology in education project, IT security in schools*. Education Infrastructure Division Education Bureau.

Tikk, E. (2011). Ten rules for cyber security. *Survival*, 53(3), 119-132.

Universities UK (2013). *Cyber security and universities: managing the risk*. Retrieved December 31, 2017, from http://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2013/cyber-security-and-universities.pdf

Yılmaz, S. and Sağıroğlu, Ş. (2013). *Siber güvenlik risk analizi, tehdit ve hazırlık seviyeleri*. Paper presented at the 6th International Information Security and Cryptology Conference. Ankara, Turkey.