*Journal of Learning and Teaching in Digital Age, 2016, **1**(2), 57-65*

# Determination of cyber security awareness of public employees and consciousness-rising suggestions

Huseyin Kuru
Gazi University
yigit.cagatay04@gmail.com

Mehmet Akif Ocak
Gazi University
maocak@gazi.edu.tr

**ABSTRACT**

The aim of this study is to measure Turkish government employees' awareness of cyber security and cyber space elements. Participants were 71 Turkish public employees working for various ministries. Both qualitative and quantitative research methods were used to get the most detailed information from the participants. A survey was administered to cyber security officers in chosen state institutions. For qualitative research, open-ended questions were administered to the participants. Reliability and validity issues were established for both surveys. Results show that employees have enough information about cyber security and cyber warfare. Findings clearly suggests that cyber defense policy should be planned in coordination with other state institutions and experiences should be shared. In order to create feasible and realistic cyber security policy at institutional level, experts at cyber security must be trained, hired and help must be requested from specialized individuals and institutions. This study recommends that rapid reaction teams (RRT) should be established to take care of cyber systems, to react against cyber breaches in time, to alert staff for cyber-attacks in order to establish effective recovery.

***Keywords:*** *cyber security, cyber warfare, hacker, hacktivism, critical infrastructure*

## INTRODUCTION

In last twenty years, technology has become indispensable element for public's daily life. Owing to common use of internet (TUIK, 2014) and transformation of information and communication systems, every individual can reach and use the internet; and also it lets governments to serve through internet technologies (Figure 1).

Regarding the dependency of critical government services in internet technologies, countries should concern systems' physical and cyber protection. The term *"cyber security"* is defined as protecting of internet technologies for cyber-attacks, securing the confidentiality, integrity and accessibility of data processed in *cyber space*, detecting *cyber-attacks* and cyber security events that took place in this systems, activating reaction elements for threats, recovering the systems from damages to situation before security events (SOME[web], 2013).

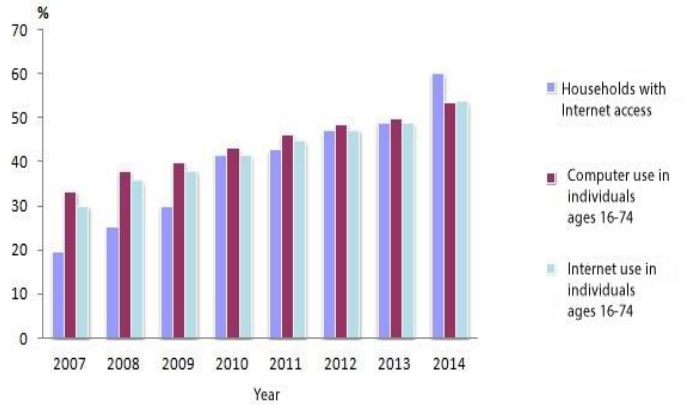


**Figure 1.** Percentage of Internet and computer usage between 2007 and 2014 years (age 16 to age 74) in Turkey (TUIK[web], 2014).

In other words, *cyber security* should be considered from a broader perspective including hardware and software technologies, technics, tactics, procedures

***Correspondence to*****:** *Huseyin Kuru, Department of Forensic Computing, Institute of Information, Gazi University, Ankara, Turkey, E-mail: yigit.cagatay04@gmail.com*

and instructions followed by the units for preventing cyber-attack from crippling essential critical infrastructure services (Vural ve Sagıroglu, 2013). Since critical infrastructures are vital for community, they have become most significant target for cyber-attacks (Ogun and Kaya, 2012). In this regard, it is mostly happening that financial service providers, social and economic infrastructures, electricity plants, water and nuclear plants, communication systems, governmental institutions and military organizations are experiencing every kinds of cyber-attacks.

Since the computer systems has widely engaged in our lives, not only the real users are benefiting from these systems but also terrorists are acting in cyber space. Terrorist groups transform their activity from real world to cyber space and they establish ties between real and cyber world (Collin, 1997). *Cyber terrorism* is characterized as crippling critical infrastructures by using computer systems for the aim of intimidating governments and citizens (Lewis, 2002). Within cyber terrorism, terrorist organizations take advantages of cyber space by planning attacks, communicating, practicing for their next target, recruiting, collecting information about the topics they need to know; and even they use cyber world to get donations from their sympathizers and for propaganda (Command, 2005).

Because of *cyber espionage countries*, terror groups and private firms steal information by using computer systems; so, in this manner, they can easily make money, time and ultimately taking ill-gotten gains (infoworld [web], 2013) Within cyber terrorism, hackers can get valuable technology to steal high trade secrets; thus, this valuable information is obtained by individuals, governments, even firms easily, without making any effort and research (Yayla, 2014).

Nowadays, *cyber capabilities* provide malicious users new opportunities to applicate new ways of crime known as cyber-crime. The concept of cyber-crime includes illegal actions aiming a system or data or a user by means of computer systems (Yasar, 2014).

When we look into Turkish Penal Code under which cyber-crimes are explained in details and collected under several titles such as intrusions or infiltrating into information technology (IT) systems; modifying, erasing, stealing the data in targeted systems; adding data without any permission; blocking access or encrypt information in databases, by using hacked computers and copied IP addresses sending numbers of requests to targeted system which cannot be answered; offenses defined as child pornography; gambling in net; taking over personnel financial data with fake e-mails and malicious software; wiretapping and recording the data sent by information systems by unauthorized persons; copying magnetic cart data or perpetrating same act by using IT systems are all defined as cyber-crime (Yasar, 2014).

Technology has also affected the delivery and expression of responses to social problems. People started to communicate in cyber nets to voice their ideas, suggestions, critics and protest about any social problem and thus led the emergence of the new concept: *"Hacktivism"* (Demirkiran, 2013). In this sense, *Anonymous* hacker group is the one of the most well-known hacktivist groups in the world. Starting with their first action as the intend of fun to scientology, *Anonymous* movement has become a trend quickly spreading around the world (Demirkiran, 2013).

Besides Anonymous, one of the most popular examples of *Hacktivizm* in the world is the *WikiLeaks* leakage. Revealing its main goal as to fight oppressive regimes in the world via the internet, Wikileaks has launched a major *political debate* all over the world from the moment they unveil the USA's confidential diplomatic documents (Akgun, 2011).

Looking at literature review, it seems very crucial what the employees in state establishments know about *cyber security* and at which level their awareness while they operate with databases containing sensitive and classified and mostly confidential information. When we review Turkish Education system, neither compulsory education curriculum nor period of university education include any education regarding cyber security. It can be easily seen that cyber security is not learned enough in Turkish Higher Education. For not getting adequate cyber security education through work-time period, Government employees are the


 

weakest chain in institutions' cyber defenses. In this sense, the purpose of this study is to investigate the importance of cyber security at institutional level.

## RESEARCH METHODOLOGY

### Context

A mixed model was used for research design. Both qualitative and quantitative research methods were used to get the most detailed information from the participants. The questionnaire was used as a measurement tool developed by researchers for quantitative research aspect. For qualitative research, open-ended questions were administered to the participants.

### Purpose of the Study

The aim of this study is to measure government employees' awareness of cyber security and cyber space elements. Employees who are operating with databases containing sensitive classified data are selected to emphasis the importance of constituting collective cyber security plans and clearly defined responsibilities.

### Questions of the study

In this study, the research questions are as follows:

1. What is the level of cyber security awareness of Turkish public employees? (cyber security, cyber warfare, siber terrorism, wikileaks, malewares, securing personnel IT systems, and concerning the adequacy of individual cyber security training)
2. Which policies ought to be implemented by institutions to rise education and awareness level of employees?

### Participants and Procedure

Turkish public employees working for Ministry of Education, Ministry of Interior, Ministry of Finance, Ministry of Health, and other ministries are chosen from various provinces. Since it is technically not possible to reach all the public officers, purposive sampling technic was used for the study' intent. Descriptive information about participants attending data collection process is presented in Table 1.

**Table 1.** Descriptive statistics for participants attending the research

| sex | Ministry of Interior | Ministry of Finance | Ministry of Education | Ministry of Health | Other Ministries | Sum |
|---|---|---|---|---|---|---|
| | ***f*** % | ***f*** % | ***f*** % | ***f*** % | ***f*** % | ***f*** % |
| **Male** | 17<br>24 | 5<br>7 | 13<br>18,4 | 2<br>2,8 | 8<br>11,2 | 45<br>63,7 |
| **Female** | 3<br>4,3 | 4<br>5,7 | 10<br>14 | 7<br>9,8 | 2<br>2,8 | 26<br>36,6 |
| **Sum.** | 20<br>28,3 | 9<br>12,7 | 23<br>32,4 | 9<br>13,7 | 10<br>14 | 71<br>100 |

### Data Collection

In order to evaluate public employees' awareness, the researchers created a survey for the determination of cyber security and cyber warfare awareness of public employees. In the first part of the survey, participants were directed to questions including definitions about cyber security, familiarity with hacker groups, qualifications in terms of their institutions' cyber security level, their cyber security education, and to what extend they can follow the new technologies created in cyber space. In the second part, qualitative approach was used to put forward proposals on precautions to be taken by both private sector and government.

**Validity and Reliability of the Survey**

Survey was checked by two lecturers who are expert in their fields. To reflect main goals, necessary adjustments were made in response to feedback received and then it was finalized. For the determination of the reliability of the scale, a reliability analysis was conducted with the help of SPSS 24 program. The result of the scale' Cronbach's alpha value was 0,79. When studies concerning the reliability of the scale are analyzed, the reliability coefficient of 0.70 and above for specific or general research goals is recommended.

**RESULTS**

Data analysis is presented in related subscales.

**Findings regarding the awareness of cyber security subscale**

By the awareness of cyber security concept subscale, it is intended to reveal whether officers working in state institutions have any information or familiarity related to cyber security which means only permitted operations in the system can be done in terms of both user and data aspect.

Table 2 presents percent (%) and frequency (f) values of data collected from the staff working in public institutions related to the awareness of cyber security concept subscale.

**Table 2.** Descriptive statistics for cyber security awareness

| Questions (N=71) | Strongly Not Agree<br>f<br>% | Not Agree<br>f<br>% | Neutral<br>f<br>% | Agree<br>f<br>% | Strongly Agree<br>f<br>% |
|---|---|---|---|---|---|
| I have enough information about cyber security concept. | 4<br>5,6 | 12<br>16,9 | 15<br>21,1 | 32<br>45,1 | 8<br>11,1 |

Table 2 provides a descriptive analysis of the public employees' perceptions about cyber security. More than half of the surveyed staff has an idea about what the cyber security is; but almost one-fourth of the attendees admit that they have no familiarity with the subject. As a matter of fact, findings show us that capacities of public staff about the cyber security is in need of improvement since any vulnerability can result big defects in cybersecurity chain.

**Findings regarding the awareness of cyber warfare subscale**

Cyber warfare, which includes state-to-state cyber conflict or taking down critical infrastructures by state sponsored hacker groups or cyber-attacks via cyber technologies, is now part of conventional warfare. So, in this part, it is aimed to reveal the awareness of cyber warfare of state employees.

Table 3 presents percent (%) and frequency (f) values of data collected from the staff working in public institutions related to the awareness of cyber security concept.

**Table 3.** Descriptive statistics for cyber warfare awareness

| Questions (N=71) | Strongly Not Agree | Not Agree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|---|
| | f<br>% | f<br>% | f<br>% | f<br>% | f<br>% |
| I have enough information about cyber security concept. | 2<br>2,9 | 12<br>17,1 | 16<br>22,9 | 37<br>52,9 | 3<br>4,3 |

Table 3 suggests that staff working for governmental organizations have some idea about what the cyber warfare is; nevertheless, big portion, that we cannot underestimate, of the participants who use cyber technologies every work day is not aware that one day they can be the target of complex and destructive cyber-attack.

**Findings regarding the awareness of cyber terrorism subscale**

In this part, it is aimed to explain the awareness of cyber terrorism which means using of internet by terrorist groups to communicate, to plan, to share their ideology, to collect donations, and to gather intelligence about their target etc. Terrorists group can use cyber technologies to facilitate their actions. So, what is the consciousness level of officials in government institutions which are the most potential prominent targets of cyber terrorism?

Table 4 presents percent (%) and frequency (f) values of data about cyber terrorism awareness.

**Table 4.** Descriptive statistics for cyber terrorism awareness

| Questions (N=71) | Strongly Not Agree | Not Agree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|---|
| | f<br>% | f<br>% | f<br>% | f<br>% | f<br>% |
| I have enough information about cyber terrorism | 2<br>2,9 | 13<br>18,6 | 18<br>25,7 | 35<br>45,7 | 5<br>7,1 |

In the light of data presented at Table 4, we can claim that almost half of the participants (52,8%; n=37) has some education or know something about cyber terrorism. What is important in this subscale that nearly twenty percent (21,5%; n=15) of public officers has no education or background affiliated with cyber terrorism. Therefore, it is urgent that every officers operating on sensitive databases must be educated in work-time period about cyber terrorism and modern cyber-attack tools.

**Findings regarding the awareness of WikiLeaks subscale**

In 2010, *WikiLeaks* internet web page has started to release USA' confidential documents containing very secret and important data about US foreign politics. In term of cyber security, it was milestone to take drastic measures to avoid leaks via cyber space. WikiLeaks security breach showed that even US who is very prominent security expert has some vulnerabilities in cyber space. So, through this part, it is intended to find out public employees' awareness of WikiLeaks that alerted world


 

countries for taking necessary steps to secure data in cyber environment. Table 5 presents percent (%) and frequency (f) values of data about WikiLeaks awareness.

**Table 5.** Descriptive Statistics for WikiLeaks awareness

| Questions (N=71) | Strongly not agree | Not agree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| | f<br>% | f<br>% | f<br>% | f<br>% | f<br>% |
| I have enough information about WikiLeaks leakage | 7<br>9,9 | 30<br>16,9 | 15<br>21,1 | 12<br>42,3 | 7<br>9,9 |

Analyzing the results in terms of cyber espionage by Wikileaks event, nearly half of the public employees heard something about WikiLeaks. While 52,2% (n=37) of participants have answered the WikiLeaks question as agree and strongly agree, 25,8% (n=19) of the sample has answered as not agree and strongly not agree. Table 5 indicates that 20,1% of the participants have no idea about Wikileask awareness. The results indicate that the fact that of the likelihood of similar events is likely to happen in the later period, the staff making process on sensitive information should be educated on similar incidents.

**Findings regarding the awareness of malwares used for cyber-attacks in cyber space subscale**

Preparing this section's question, it was intended to reveal public employees' knowledge about malwares that can snake into computer systems in various ways to steal, change data and to watch process streaming in targeted systems etc. Malwares are sometimes created as complex programs and equipped with artificial intelligence like *Stuxnet*. Every kind of computer used in institutions has some vulnerabilities against the malwares; therefore, users (employees) must have to be alerted about malware intrusion ways. Table 6 presents percent (%) and frequency (f) values of data about malware.

**Table 6.** Descriptive Statistics for awareness of malwares used for cyber-attacks in cyber space

| Questions (N=71) | Strongly not agree | Not agree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| | f<br>% | f<br>% | f<br>% | f<br>% | f<br>% |
| I have enough information about Malwares used for cyber attacks | 6<br>8,7 | 15<br>21,9 | 18<br>26,1 | 23<br>33,3 | 7<br>10,1 |

It is inferred from the findings that less than half of the public workers (43,4%; n=30) were alerted with cyber-attack tools. Almost one-third has no idea about malwares that can break down computers and end a system. These results clearly show that related precautions must be taken into account for public officers in order to aware of and prevent the threats in cyber space. If you do not know the enemy, you cannot take over him; so, you cannot take necessary precautions. Moreover, every single day, a new malware is created for various aims in cyber space. If you cannot follow the innovations, it is impossible to cope with attacks in cyber war land.


 

**Findings regarding the personnel computer systems security subscale**

In this part of the survey, the study intended to find out how the participants manage to protect their smart phones, laptop or personnel computers and increase consciousness level about the threats. Table 7 presents percent (%) and frequency (f) values of data about personnel computer systems security.

**Table 7.** Descriptive statistics for awareness of personel computer systems security in cyber space

| Questions (N=71) | Strongly Not Agree | Not Agree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|---|
| | f<br>% | f<br>% | f<br>% | f<br>% | f<br>% |
| I can manage to secure my computing devices that I use in my daily life | 17<br>23,9 | 23<br>32,4 | 20<br>28,2 | 9<br>12,7 | 2<br>2,8 |

Not surprisingly, only a little portion of sample says that they are aware of the treats that can harm personal computing devices and they can manage to protect databases from the attack. Thinking of answers as Strongly Not Agree and Not Agree, more than half of the participants feels vulnerability in terms of cyber security. Remembering that the *Stuxnet* attack started with an engineer's personal laptop, public employees must keep in mind that little security bug can lead to complex cyber-attacks.

**Findings for satisfactoriness of individual education at cyber security**

In this part of the survey, this study searched for the adequacy of cyber security and cyber warfare training in public officer's lifelong learning. It was aimed to find out whether, for their point of view, they get necessary education and training and have the theoretical and practical capacity to protect their institutions' computer systems from cyber-attacks. Table 8 presents percent (%) and frequency (f) values of data about personnel cyber security education.

**Table 8.** Descriptive statistics related to personel cyber security education

| Questions (N=71) | Strongly not agree | Not agree | Neutral | Agree | Strongly agree |
|---|---|---|---|---|---|
| | f<br>% | f<br>% | f<br>% | f<br>% | f<br>% |
| I have been trained enough at cyber security during my education period | 32<br>45,1 | 30<br>42,3 | 6<br>8,5 | 0<br>0 | 3<br>4,2 |

As Table 8 indicates, only 4,2% of participants (public employees) claimed that they have gained talents during their education about cyber security so they can operate well to defend against cyber security. Besides that, 87,4% of the public officers acknowledged that they have not been trained enough at cyber security. A large proportion of the public staff surveyed on this issue think that the Turkish education system does not bring them to a sufficient level. They clearly indicate that related curriculum in education programs in university must be revised in terms of cyber education.

**Cyber security suggestions for policy makers at instutions subscale**

Qualitative part of the study part aimed to collect proposals and suggestions from public employees in order to create efficient cyber security policy at institution level. In this regard, content analysis approach was used to evaluate the data. Similar answers were coded and put in the same group. Table 9 presents (%) and frequency (f) values of data we collected about cyber security policy suggestions.


 

**Table 9.** Descriptive statistics about Cyber security suggestions for policy makers at instutions

| | f | % |
|---|---|---|
| Cyber defense policy should be planned in coordination with other state institutions and experiences should be shared | 8 | 12 |
| Must be based on international information security standards. | 6 | 9 |
| Institution personnel must be trained at this subject. | 16 | 25 |
| Experts at cyber security must be hired and help must be gotten from specialized individuals and institutions. | 14 | 21 |
| Trusted software and hardware must be used. | 10 | 15 |
| Must be prepared upon institution's real needs. | 5 | 7 |
| Must have the capacity to retaliate for cyber attacks | 2 | 3 |
| No idea | 3 | 4 |

Table 9 shows title of suggestions in order to create feasible and realistic cyber security policy at institutional level. As Table 9 indicates, most of the Public employees who contributed this survey suggest the officers must be trained at cyber security subjects. They think the biggest problem or deficiency is to get not enough education in cyber security field. Secondly, the experts from private sectors and other organizations may be adopted to cyber security systems of institutions; besides, governmental organizations may benefit from specialized company's experiences. This study suggests that there must be some kind of organic collaboration and cooperation among state institutions and private sector in terms of cyber security. In this regard, it is hard to be expert in every field of cyber security. This kind of cooperation allows to get the support from experts who may facilitate and ease the work to be performed. The other result suggests, mostly, to use the secured national software and hardware. This policy requests investment in technology, research and development (R&D). One of the prominent idea in the responses was coordination and sharing experiences of institutions in order to create a stable investment in technology. In this sense, a shared response system can alert the other system users to take necessary precautions regarding the new developments and as well as attacks aiming the other state departments. Following international information security standards is another important idea that would ease to keep up with the cyber security standards of nations which are pioneers in cyber security field. While making the policy, institutions must think about their real needs in terms of cyber security. Lastly, the results clearly suggest that state departments have to think about both defensive and offensive components to retaliate with cyber-attacks.

## CONCLUSION AND SUGGESTIONS

The purpose for this study was to collect information from public employees about cyber security and cyber warfare. In this regard, this study offered necessary measures and arrangements to boost institutions' cyber security and cyber warfare capacity. For this purpose, education and training of public officers regarding cyber security seemed most important issue. Moreover, sufficient training during their career must be provided and necessary arrangements related to curriculum in universities must be revised without any hesitation.


© 2016, *Journal of Learning and Teaching in Digital Age*, ***1***(2), 57-65

Developments in information and communication systems are very fast. Thus, it gets more crucial for public officers to work on these systems very carefully and consciously. Governmental organizations are supposed to hire their workers very carefully. Persons who are talented, educated and expert in their fields must be chosen to give responsibility of systems in cyber security. To boost the cyber security capability of all departments in government, it is vital to get support from specialized persons and enterprises during the establishment of cyber security policy.

One of the most important elements in ensuring a country's cyber security can be achieved through the use of national information and communication technologies. For this reason, cyber security policy should be based on self-made and secured information systems. In order to improve the cyber security capabilities to keep up with the new developments in cyber space and find solutions for rivalries tactics in cyber war land, national investments should be encouraged in search and development projects, and budget allocated by government should be augmented year by year.

Rapid reaction teams (RRT) should be established to take care of cyber systems, to react in time against cyber breaches, to alert staff for cyber-attacks and direct them for effective recovery; finally, measures should be taken to improve the quality and ability of these units. Cyber events and cyber-attacks experienced in the past should be examined in terms of methodology and used tools to generate action plans. In the light of experience gained, there should be a corporate memory. Coordinated with all institutions within the national borders, cyber security plans should be organized and responsibilities for every department should be declared openly. Responsibilities of all sectors should be identified in order to be ready for large-scale cyber-attack and awareness raising activities should be performed for all ages.

## REFERENCES


Akgun, B. (2011). Wikileaks and Assangists. *Strategic Thinking Journal*, *2*(14), 22.

Amoroso, E.G., (2012). *Cyber-attacks: protecting national infrastructure*. UK: Butterworth-Heinemann, 13-17.

Collin, B. C. (1997). The future of cyberterrorism: Where the physical and virtual worlds converge. *Crime and Justice International*, *13*(2), 14-18.

Command, D. (2005). *Cyber Operations and Cyber Terrorism*. DCSINT Handbook No. 1.02.

Demirkiran, P., (2013), *Anonymous ve Hacktivizm*, A.R. Keleş, F. Sayılan. (Editors) *Hacker Culture and Hacktivizm*. İstanbul: Alternative Informatics Association Headquarters, 288-291.

Infoworld, (2013). *Cyber-espionage moves into B2B*, Retrieved from http://www.webcitation.org/query?url=http%3A%2F%2Fwww.infoworld.com%2Farticle%2F2642608%2Ftechology-business%2Fcyber-espionage-moves-into-b2b.html&date=2016-02-13. 13.02.2016.

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic and International Studies, 8-9.

Ogun, M. N., & Kaya, A. (2012) Significance of Cyber Security for National Security: A Study Concerning the Necessary Measures. *Security Strategies Journal*, 9(18), 145-180

SOME (2013). 2013-2014 *Action Plan*, 2016-02-13 Retrieved from http://www.webcitation.org/query?url=http%3A%2F%2Fwww.udhb.gov.tr%2Fdoc%2Fsiberg%2FSOME_2013-2014_EylemPlani.pdf&date=2016-02-13. 13.02.2016.

TUIK (2014). *Turkey Statistical Institute Household Information Technology Usage Survey*, Retrieved from http://www.webcitation.org/query?url=http%3A%2F%2Fwww.tuik.gov.tr%2FPreHaberBultenleri.do%3Fid%3D16198&date=2016-02-12. 12.02.2016.

Vural, Y., & Sagıroglu, S. (2013). *Cyber Security Risk Analysis, Threat and Readiness Levels*. presented at Conference of International Participation Information Security and Cryptology, September 20-21th, Ankara.

Yayla, M., (2014). Cyber War and its difference from malicious acts in the Cyber environment. *Hacettepe Law School Journal*, *4*(2), 181-197.

Yasar, H. (2014). Corporate Cyber Threats and Prevention Methods and a Case for Enterprise Security Cyber Security Action Plan. *Master's Thesis*, Gazi University, Computer Forensics Institute, Ankara.