INCREASING AWARENESS OF INSIDER INFORMATION SECURITY THREATS IN HUMAN RESOURCE DEPARTMENT

Burcin Cetin Karabat
Sakarya University
Human Resources Management Department
Faculty of Business, Sakarya, Turkey
burcin@sakarya.edu.tr

Cagatay Karabat
TUBITAK BILGEM UEKAE
cagatay@uekae.tubitak.gov.tr

─Abstract ─

An insider threat for companies is defined as a threat caused by malicious user who is an employee company. In recent years, there are number of work on insider threats in information security technologies. These works shows that companies should increasingly and seriously should take into account these threats. Human factors in companies constitute one of the weakest links in information security technology and its products used in human resource (HR) management departments. In the literature, insider threats are generally classified into two main categories: 1) Intentional insider threats and 2) Unintentional insider threats.

In this work, we address the employees working in HR departments of various companies from different sectors. Since HR departments are one of the critical departments for insider threats, we focus on the scenario that a malicious insider accesses critical, important and/or personal data. In this scenario, a malicious employee of HR department may change or misuse of the data belonging to his/her company (product data, marketing data, strategy documents etc.) and/or the data belonging to the other employees (e-mails, ID numbers, birth dates, salaries, health data etc.) by intentionally or unintentionally.

By taking into account the previous works done in the literature, we prepare new questionnaire for this work. The questionnaire is applied to HR managers and employees of various sectors. Our aim is to increase HR managers and HR employees awareness of insider information security threats.

Key Words: *Information Security, Insider Threats, Human Resource Department*
JEL Classification: M12, D83.

1. INTRODUCTION

The data confidentiality, integrity and availability are very important for the companies. In recent years, companies encounter serious information and network security threats which cause them to loss, change and misuse of their critical data. Especially, the insiders threats, which are caused by employees of the companies, are increased at unprecedented rate nowadays. According to the 2011 Cyber Security Watch Survey, most of the attacks are achieved by outsider attackers, on the other hands insider attacks (employees or contractors with authorized access) are more costly and more damaging (%46) than outsider attacks.

The companies screen their employees for insider threat risk. As a special case, Human Resources (HR) departments are very fragile against insider information security attacks. Since HR employees have rights to access the personal data belonging to employees, this make possible that they may change and/or misuse these data. In order to overcome the aforementioned threats, the number of companies invest more money on the information and networks security solutions especially focusing on access control systems and monitoring systems.

In the literature, there are lots of works on information security of the Human Resource Information System (HRIS), (Ball, 2001; Kavanagh & Thite, 2008). However, there are not sufficient work on policy adaptability and ensure adaptability. On the other hand, there are number of works on "information security management impacts on customer habits".

In this paper, we address insider information threats caused by employee of HR department. In this scenario, an employee of HR department (as an insider) may access to the critical/sensitive data belonging to either the company or the other employees. Thus, they may change or misuse the company specific data (product data, marketing data, strategy documents etc.) or personal data of the other employees (i.e. ID number, birth date, health data, salary etc.).

This work is a horizontal research work which consists of various HR departments in different sectors i.e. telecommunications, automotive, textile, tourism, health, food etc. In this work, we prepare our new questionnaire for the HR department

employees and ask them to fill these out. Our questionnaire is based on the works done by (Loch et al., 1992; Whitman, 2003 and Kraemer et al. 2007) and the interviews with the employees of HR departments working in various sectors. Therefore, it is novel and be particularly prepared for the research which is done in this paper. To the best of our knowledge, in the literature, there is not such a questionnaire which is suitable for our proposed work.

Finally, we analyze the results the questionnaire by reliability test and correlation analysis. With respect to our analysis results, we conclude the work in the last section. The proposed questionnaire-based work aims to increase the awareness on information and network security threats caused by the insiders.

2. INFORMATION SECURITY IN THE COMPANIES

In modern digital era, companies make huge investment in order to follow up the recent achievements in information technologies. The importance of the role of information technologies (IT) in companies is constantly evolved since IT enables some businesses to differentiate themselves from their competitors. Therefore, the companies can respond to today's environment of rapidly changing business conditions.

On the other hand, IT system creates its own set of problems such as data security, confidentiality, integrity and availability. Nowadays, new threats come from the users who are authorized to gain access to IT services. These threats are generally called as insider attacks and they are extremely difficult to detect or protect against. The insider attack can affect all components of IT systems of a company. On many IT systems, the access control settings for security-relevant tasks do not reflect the companies' security policy. In other words, most of the IT systems are not designed as a role-based system. This allows the insider to browse through sensitive and critical data belonging to the company (confidential data) and/or the other employees.

There are really critical and sensitive data, which belong to company itself and employees, in the IT systems of the companies. Companies are responsible for storing, maintaining and protecting these data. The attacks against the IT systems can cause financial damages for the companies and other employees. In order to cope with such threats, the companies uses information security technologies but even these technologies cannot solve the problems caused by insider attacks most of the time.

Enterprise information security technologies are type of IT security technologies especially used by companies. Since companies are often use different IT systems and these systems are mostly connected to the Internet, it is really difficult to find a common enterprise security solution that fits to all companies. Besides, enterprise information security technologies are affected from different factors such as human factors, education, and technology. These make enterprise information security technologies really complex. The standardization activities have received a lot of attention from various stakeholders in order to manage the complex structure of enterprise security information security systems and ensure high level information security.

Insider attacks are one of the serious types of attacks against IT systems. Due to economic crises in recent years, malicious employees, who currently or previously worked for, tends to achieve attacks to the IT systems of the companies. The treats caused by careless and untrained employees are another type of insider attacks. All types of insider attacks are very serious and it is difficult to cope with the threats of malicious insiders completely.

The adequate information security policies should be defined and associated procedures should be deployed in order to avoid from insider attacks. In that sense, IT systems should be investigated and end-to-end risk analysis should be done. The access control systems which incorporates with recent IT security technologies, i.e. biometrics, e-signature, one time passwords etc., can be efficient solutions for these threats.

3. INSIDER THREATS IN INFORMATION SECURITY TECHNOLOGIES: HUMAN FACTORS

Information technologies are one of the emerging technologies in today's world. They play a major role on digital data transmission, storage and sharing. Thus, citizens and companies can easily access to the data. On the other hand, these services of information technologies can bring new threats to our life since they contain their own risks like uncontrolled change of data, illegal usage, intellectual property problems, unauthorized access to critical data etc. (Schultz, 2002; Kraemer et al. 2007). All these problems seriously threats both users and companies.

Recent years show that as the number of works done in digital domain increases, companies and users face with increased number of problems by using

information technology services. According to the press release of Deloitte (Deloitte Turkey, Media Press, "Kurumların bilgi güvenliğine yaklaşımı zayıflıyor" – (The approach of enterprises against information security is getting weaker) www.deloitte.com) in 2011, the top five security threats are mobile devices, security threats to the third parties, employee fault and careless, rapid deployment of emerging technologies, and IT systems and misuse of data by employees as shown in the Table 1.

Table 1: The top five security threats according to the press release of Deloitte in 28.12.2011

Security Threats	Percentage (%)
Mobile Devices	%34
Security Threats Related to the Third Parties	%25
Employee Faults or Careless Employees	%20
Rapid Deployment of Emerging Technologies	%18
IT Systems and Misuse of Data by Employees	%17

Information security threats against companies are generally categorized into two main groups: 1) Internal threats, 2) External threats.

In our work, we focus on internal information security threats for companies. There are number of definitions for the term "insider threat" in the literature. Cole and Ring (2006) defines insider threat as someone who has special access or knowledge with the intent to cause harm or danger. According to Schultz and Shumway (2001), an insider attack can be defined as the intentional misuse of computer systems by users who are authorized to access those systems and networks. By taking into account these definitions, it can be stated that insider threats are generally caused by employees, consultants, short-term workers and even personnel from third-party business partners and their contractors. But with all the outsourcing that is occurring, it is becoming increasingly difficult to maintain a hard and fast distinction between insiders and outsiders. When an attack by someone such as a former consultant occurs, for example, should the attack be considered an internally- or externally- initiated attack? Additionally, many so-called "insider jobs" have turned out to be the result of complicity between an insider and an outsider (Schultz, 2002).

In the concept of information security, insider threats caused by employees of a company can be classified into two main categories: 1) Intentional threats, 2) Unintentional threats. The most common intentional insider threats to information security system of organizations are computer abuse and fraud. User errors and

negligence are arguably the two most common unintentional insider threats. Some of the underlying reasons behind user errors are lack of experience in utilizing security tools, complexity of the security tools, and job stress due to time pressure and workload. On the other hand, although reasons behind negligence are complex, lack of awareness and motivation to use security tools due to their performance hindering characteristics can be considered as important factors (Yayla, 2011).

Several industry reports indicate that both intentional and unintentional insider threats are considered as one of the top ranked threats to information security over the past decade. Unintentional insider threats carry as much significance as intentional insider threats. The 2009 CSI Computer Crime and Security Survey revealed that about 66% of the respondents attributed at least some of their losses to non-malicious insiders, and 16% of the respondents claimed that all their losses were due to non-malicious insiders (Richardson, 2008).

4. METHODOLOGY OF THE RESEARCH

In this work, we make interviews with HR department managers and employees. We aim to analyse and determine the common insider threats and data security threats caused by these threats in these companies. We prepare a new questionarie for this work. This questinarie is based on the outcome of the aforementoned interviews as well as the work done in the literature (Loch et al. (1992), Whitman (2003) and Kraemer et al. (2007)). To the best of our knowledge, in the literature, there is not such a questionarie which is suitable for our proposed work. That's why, we prepare new questionarie.

The data were collected through HR employees via semi structured interviews from January 10, 2012 to January 27, 2012 and mailed out and/or send by fax and during February 1, 2012 to March 1, 2010 a number of 63 HR employees have responded. Since the employees of HR departments have right to access the private information (salary, birth data, health data, family data etc.) of other employees, they have more chance to be classified as potential insider attackers. For this reason we select to work on the employees of HR departments from various sectors in this work.

The questions in our questionnaire can be classified into three main categories: 1) Information security threats, 2) Insider threats, and 3) Protection mechanisms. These are discussed in detail in the following paragraphs.

In the concept of information security threats, we define several items as follows: a) Employees' mistakes and errors, b) Introduction of erroneous data by users, c) Intended software attacks, d) Software bugs and errors, e) Spy software, f) Deliberate acts of sabotage or vandalism, g) Malicious codes, h) Social engineering attacks, i) Technical hacker attacks, j) Physical damage by accident, h) Inefficient and weak control systems.

The threats in the concept of insider threats, which are used to test the hypothesis, are defined as follows: a) Employees tend to make mistakes unintentionally (accidents, employee mistakes), b) Employees are lack of technical expertise and experience in information security technologies, c) Employees have difficulties in adapting to company policies, d) The policies are not correlated with management board, e) The policies which are prepared by inexperienced people, f) To use complex risk analysis methods, g) Low salary, bad working conditions and unhappy employees due to similar reasons, h) Equipment failure, i) Bugs and code problems, j) The deployment of old fashion technologies.

Information security protection mechanisms which are obtained from the Whitman's work in 2009 are summarized in Table 2.

Table 2: Protection Mechanisms

Use of passwords	100%	Publish formal standards	43.8%
Media backup	97.9%	Control of workstations	40.6%
Virus protection software	97.9%	Network intrusion detection	33.3%
Employee education	89.6%	Host intrusion detection	31.3%
Audit procedures	65.6%	Ethics training	30.2%
Consistent security policy	62.5%	No outside dialup connections	10.4%
Firewall	61.5%	Use shrink-wrap software only	9.4%
Encourage violations reporting	51.0%	No internal Internet connections	6.3%
Auto account logoff	50.0%	Use internally developed software only	4.2%
Monitor computer usage	45.8%	No outside network connections	4.2%
No outside Web connections			2.1%

The aforementioned topics, which are classified under three main categories, are scaled by using a five–point Likert scale (ranging from 1-5). Then, the work on the awareness level of HR department employees on information security threats is done in this work. With respect to the obtained results, we propose suggestions to the HR department employees, the companies, which are from different sectors, suffering from information security threats.

In this work, we test the following hypothesis:

Hypothesis 1

H_1: The awareness level of HR department employees, who can be considered as potential insider attackers, on the information security technologies varies according to the sector of the company that they work for.

Hypothesis 2

H_1: As the experience of the employees of HR department, who can be considered as potential insider attackers, increases, the awareness level of them increases.

Hypothesis 3

H_1: As working position of the employees of HR department, who can be considered as potential insider attackers, increases, the awareness level of them increases.

5. FINDINGS

The six medium scale companies, which are located in Turkey, are the base for our research in this work. These companies work on different sectors (telecommunications, automotive, textile, tourism, health and food) and they prefer to be anonym. In order to avoid from misleading, we code these companies from X1 to X6.

The companies with respect to their sectors	Tele-communications Sector **X1**	Automotive Sector **X2**	Textile Sector **X3**	Tourism Sector **X4**	Health Sector **X5**	Food Sector **X6**
The number of employees working in HR department	18	12	9	7	11	13
The number of employees who attend our research	16	11	6	7	10	13
The percentage of the attended employees %	**%89**	**%92**	**%67**	**%100**	**%91**	**%100**

The demographic information of the 63 respondents involved in the analysis is as follows: female 61.9% (N=39), male 38.1% (N=24); regarding age ranges: ages 18-25 7.9% (N=5), ages 26-33 42.8% (N=27), ages 34-41 28.6% (N=18), ages 42-upper 20.7% (N=13); regarding average job experience: 1-5 years 26.7% (N=23), 6-10 years 24.4% (N=21), 11-15 years 48.8% (N=42); regarding tenure: 0-5 years 47.6% (N=30), 6-10 years 39.7% (N=25), 11-15 years 12.7% (N=8); regarding

positions: HR director 9.5% (N=6), HR generalist 12.7% (N=8), HR specialists 33.3% (N=21), HR assistant 44.4% (N=28).

Statistical analyses are performed by using SPSS 17.0 Statistical Package. Correlation analysis is used to test the relationship between the awareness of employees on the information security threats and the sector of their companies worked for. In this work, the alpha coefficient of reliability of the awareness of the employees on the information security threats scale is 0.803. Since obtained the alpha values are more than 0.7, they fall into the acceptable range suggested in the literature.

As a result of the correlation analysis; the correlation between of the awareness of the employees on the information security threats and the sector of their companies worked for is statistically significant. Therefore, it shows that the sector of the companies for which they work is positively associated with the awareness of the employees on the information security threats ($r = .647$, $p = < .001$).

According to our finding in this work, the HR department employees working for telecommunication sector have the highest awareness level on information security threats. On the other hand, HR department employees working for tourism sector have the lowest awareness level on information security threats. Apart from these, the correlation between the awareness of the employees on the information security threats and working experience and working position is statistically significant ($r_1 = .545$, $r_2 = .58$, $p = < .001$).

6. CONCLUSION

In this work, we address insider information security threats in HR departments of various companies working on different sectors. We make interviews with HR department managers and employees and create a new questionnaire. Then, we apply it to them. By using statistical methods, we analyze the outcomes of the questionnaires.

According to our findings, the awareness level of the employees of HR department on insider information security threats are highly correlated with the sector of the company that they work for, their experience and their position in the department. In order to increase the awareness level of HR department employees, the short courses would be very useful.

BIBLIOGRAPHY

Ball, Kirstie S. (2001), "The Use of Human Resource Information Systems: A Survey", *Personnel Review*, Vol.30, No.6, pp.677-693.

Cole, Eric and Ring, Sandra (2006) Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft, Canada: Syngress Publications.

Deloitte Turkey, Basın Bülteni, "Kurumların bilgi güvenliğine yaklaşımı zayıflıyor", http://www.deloitte.com, [Accessed 28.12.2011].

Kavanagh, Michael J. and Thite, Mohan (2008), Human Resource Information Systems: Basics, Applications and Future Directions, Sage Publications.

Kraemer, Sara; Carayon, Pascale (2007), Human Errors and Violations in Computer and Information Security: The Viewpoint of Network Administrators and Security Specialists, *Applied Ergonomics*, Vol.38, No:2, pp.143-154.

Loch, Karen D., Carr Houston H. and Warkentin Merrill E. (1992), "Threats to Information Systems: Today's Reality, Yesterday's Understanding*", MIS Quarterly*, Vol.16, No:2, pp.173–186.

Richardson, Robert (2008), 2008 CSI/FBI Computer Crime & Security Survey, http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf, [Accessed 18.03.2012]

Schultz, Eugene E. and Shumway, Russell (2001), Incident Response: A Strategic Guide to Handling for System and Network Security Breaches, Indianapolis: New Riders Publications.

Schultz, Eugene E., (2002) "A Framework For Understanding and Predicting Insider Attacks" *Computers and Security*, Vol.21, No:6, pp. 526-531.

Yayla, Ali (2011), Controlling Insider Threats with Information Security Politicies" ECIS 2011 Proceedings, http://is2.lse.ac.uk/asp/aspecis/20110246.pdf, [Accessed 27.03.2012].

2011 Cyber Security Watch Survey, magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.