INVESTIGATING THE SECURITY THREATS IN E-BANKING GATEWAYS

Jafar Esmaeeli¹, Ahmad Assadzadeh², Shahram Gholinezhad³*

¹²³PHD student in Industrial Management, Islamic Azad University, East Azarbaijan Science and Research Branch, Associate Professor, Faculty of Economics, Business and Management, University of Tabriz (IRAN)

*Corresponding author: shahramgholinejad@yahoo.com

DOI: 10.7813/2075-4124.2015/7-2/A.87

Received: 11 Dec, 2014
Accepted: 04 Feb, 2015

ABSTRACT

Information systems, frequently engaged in various types of threats that can be caused by a variety of injuries and cause significant financial losses for the organization. Security vulnerabilities could lead to a distortion or destruction of part of the information system completely. Recently companies, especially banks are struggling to identify security threats in their information systems. As well as the threats, the electronic portal can hurt their information systems. In this study, the literature reviews the security threats in information systems, to be classified. And then the relationships between the threats and e-banking portals were studied. In this way, banks are able to understand the strengths and weaknesses of the portals that are against these threats. The present study is as objective and descriptive terms. Flexible classification model is dynamic and has multiple dimensions, and also provides a discussion of organizational behavior of threats. Organizations, especially banks can refer to the appropriate strategies and measures to avoid or reduce the impact of information security threats. According to the results obtained in this study and in most categories of threat, vulnerability significantly has Internet portal. The threat of domestic workers who can steal information from your organization is important. This problem is related to organizational behavior should design strategies for staff behavior management. Gateway also influence the types of threats that recognizes the threat is described by t = 9.28.

Key words: security threats, e-banking, e-banking portals

1. INTRODUCTION

With the development of information and communication technologies and increasing access to the Internet, organizations are vulnerable for various types of threats. The information is subject to attack the users of their services and the damage they cause, are located. Financial losses caused by security threats can usually be found explicitly. Because of significant losses due to the negligence of information system security risk occurs (geric and hutinski 2007). So managers need to identify the threats that affect their properties. The impacts of these threats are also known to stop numerous attacks, by an appropriate action.

When a system is vulnerable and not aware of the weaknesses can be exploited by attackers with a particularly intrusive techniques (Alhabeeb, Almuhaideb et al. 2010). Act XI of computer crimes, 74.3 percent of total losses by viruses are unauthorized entry and theft of personal information (gordon, loeb et al. 2006). A survey shows that 70% of the scams have been performed by internal staff. But 90 percent of security checks done for external threats (MCCUE 2008). To threats, have their origins as well as areas in which the system is affected, areas should be identified. The assets of the organization's information security safeguards are already in place (geric and hutinski 2007). Thus, the classification of security threats and effective action is necessary to understand the threats and their potential impact and are identified. Security threats can have different bases classified as a source of threat, threat factors and threat motivation. Identification and classification of threats help system to security threats and to prevent or reduce the impact of the threat of organized (tang, wang et al. 2012).

A number of categories of external and internal security threats exist in the literature. Many researchers have proposed classification based on regulation that have motivated attacker. This article is based on a combination of the above categories, if accepted, the result of this combination, the new classification that is presented to take appropriate action to reduce the risk of threats. In relation to the classification of threats by electronic devices such as a bank teller, sales terminals, card readers, kiosks, internet, landline and mobile phone will be examined took through questionnaires given to employees and experts of the Bank.

2. CLASSIFICATION OF SECURITY THREATS

In Review of the literature, we have done several attempts to classify the threats. In this section, an overview of the most common classifications has been provided.

A threat is the enemy of targets of the system and increases the ability of the enemy to attack a system (swiderski and snyder 2004). So a threat is made up of two parts: the first techniques that attackers exploit the potential vulnerability of the system they use and the effects that threaten the system's assets. The threats we can put in two main categories: (Jouini, Rabai et al. 2014)
- Ranking methods based on the techniques of attack
- Ranking methods based on the effects of the attack
- Classification methods based on the techniques of attack
A three-dimensional vertical model: (ruf, ag et al. 2010)
This model is used to improve the understanding of threats and loss of classification models. The threat of climate models is divided to three ordinate “motivation, localization and operating”.

- Threat, a threat to the operator of a particular property of the system that consists of three classes of people, technology, and the event is unpredictable.
- Motivated intimidation, threat displays that cause deliberate and accidental threats are divided into two classes.
- Localization of threats, showing the origin and source of internal and external threats are divided into two floors.

(B) Hybrid model for classifying threats ([geric, and hutinski 2007])

The model is known as C3 model and cube classification model. This model is available in the main three criteria:

- The frequency of threats: shows threats events frequency.
- Activity threat: a threat to the affected areas of the site. Such as physical security, personal security, operational security
- Source of the threat: Provides a variety of threats.

(C) Classification pyramid model of information security threats ([Alhabeeb, Almuhaideb et al. 2010])

This model is based on the following three factors that are classified as intentional threats:

- Attacker prior knowledge about the system shows the extent information that the attackers have about system components.
- Zone crisis: a crisis situation in different parts of the system that may be affected by the threats.
- Loss: all losses that occur in the system or organization.

• Impact on the classification of threats
  STRIDE model: (swiderski and snyder 2004)

This model focuses on identifying threats and attacks on targets. STRIDE has come from the first six letters of the word as follows:

- Spooﬁng identity (fraud), tampering with data (data corruption), repudiation (Disclaimer), information disclosure (disclosure of information), denial of service (denial of service), elevation of privilege (promotion advantages)

(B) ISO Model: (ISO 1989)

International Organization of Standardization has listed 5 impacts as follow:

- Destruction of data or other sources distort or change information, theft or destruction, or loss of information.
- Disclosure of information, service outages
- Mixed methods of techniques and effects of attack (jouini, rabai et al. 2014)

The basic idea of this model is incorporating the highest standards and demonstrating the threats and the impacts.

The classification criteria of the model are as follows:

1. Source of security threats: threats to internal and external sources. Internal threats occur when a person is permitted to access to the system in terms of hardware and software. Alien threats from outside of the organization are those works that people do not have permission to access the system, arises.

2. Security threats factors: Human threats include human actions, such as hackers or individuals within the organization. Attack the individual is informed of technical and non-technical vulnerabilities in security controls, information systems and networks in order to steal or sacrificing or compromising access to authorized users utilizing the network resources and information systems (2013). Environmental threats are caused by the inhuman factors such as earthquakes, floods and fires, lightning and animals. Computers are sensitive to dust and rough surface (Koshtegar2012). Technological threats include hardware and software technologies as well as providing energy. An information system or network may be under threat because of the accident, malfunction or human error (standard national organization of Iran 2013). Most applications such as WORD, EXCEL, and ACCESS can eliminate unwanted data files (Koshtegar2012).

3. Motivation security threat: bad or good intention. Powerful incentives to do in real life are a criminal offense against a person or organization. One of the main reason is revenge against the man who thinks he is a malicious damage or obtains money. Cyberspace for a group of people who are able to enter user accounts called subversive people, or as a pastime hurt other people. In other words, they leverage the user accounts, databases and network equipment as an honor for them. Vandals usually consider their activities as victimless crimes. Their argument is that when a user account or the database does not change and in ﬂuence is not stolen what will happen to the organization. (Sadosky et al. 2006) Bad intentional threats include attacks caused by internal staff or external parties for damage and disrupting the system. Attackers and destructive viruses are constantly changing, or deleting data (Gr died 2012). These threats occur because of poor security policies and errors of employees and external parties occur with the aim of not damaging the system errors. Neglect of important security features by programmers and designers create the security to be at a low priority for them. Users are normally not aware of the threats. Some users are aware of the security features, but do not take them seriously (Koshtegar2012).

4. The purpose of the security threat: intentional or accidental. Intentional threats of harm arise from a decision that someone deliberately planned to disrupt the system. Random Threats happens from the lack of prior knowledge.

5. The effects of threat: destruction of data, data manipulation, data theft, information disclosure, denial of service, promotion, beneﬁts, illegal use. Destruction of data includes the destruction of a system for stopping the operation of the system. Distorted information includes any unauthorized changes such as an increase or decrease in disk ﬁles, other ﬁles created by virus or other factors. Unauthorized disclosure of information disclosure includes the threats like Data theft, unauthorized use of a computer or network without loss of service for other users.).

3. ELECTRONIC BANKING

With the development of electronic commerce, the need of electronic financial services, e-banking and other financial services such as insurance branches was felt in order to buy and sell shares in electronic form as presented. The e-commerce is divided into ﬁnancial products and services, e-banking (Koshtegar 2012).

Electronic banking is a service that was ﬁrst used in 1995 in America and then spread rapidly among other countries (wan, luk et al. 2006). A wave of electronic banking to customers, comfort and savings for the authorities, new challenges, includes security, lack of access in case of violation of electronic networks, the cost of maintaining, updating databases, as well as the design and implementation of new economic policies (pikkarainen et al. 2004). Electronic banking, which means optimal integration of all banking activities, is in accordance with the organizational structure of banks that can provide the services required by our customers. Electronic banking needs information technology, in order to remove the shackles of
time and space of banking services. Two essential ingredients of electronic banking are electronic funds transfer and electronic resources (Haider Pur and Tahmasebi 2008).

Developments in the banking system can be divided into four stages (Amade and Jafarpour 2010):

First period: back office automation, the technology behind the counter was common in the 1960s and has been the starting point for computer applications in the banking system. The second course in front of the office automation, the course of the late 1970s is accessed and began to branch employees that are constantly checking accounts. And the possibility of continuous data was accomplished, through the use of telecommunication lines.

Third period: connecting customers to the accounts in the period that began in the mid 1980's customers access to their accounts via telephone, ATM, smart card, magnetic card and personal computers.

E-banking in Iran

The rapid advances in information and communication technologies are given as well as the 60's and 70's solar efforts in order to use the computer systems of the bank. In 1370 the first commercial bank debit cards issued. Following this action, Bank Sepah, also issued in 1371 the installation of seven ATM machine bank card. And thus the development of electronic banking began in the country (Amade and Jafarpour 2010).

In the following diagram, electronic funds transfer systems; electronic banking is shown in (Amade and Jafarpour 2010)

![Fig. 1. Electronic funds transfer systems in electronic banking](image)

The consumer banking, electronic banking, which is part of the bank, used by individuals and private clients. And users deal with it. The research is based on consumer banking.

- **E-banking devices**
  - Electronic devices electronic banking platform provide banking services and Positions which are defined for electronic banking. And other ad hoc ports services is defined as the ATM, POS, KIOSK BANK, PINPAD. Providing banking services without restriction in certain places multifunction devices is called sample internet banking, telephone banking, mobile banking (Koshtegar 2012), who described the following explanation of each of the ports.
  - (A)Teller machine (ATM): an ATM machine can act as a network of banking. Main tasks and a great part of banking transactions will be carried out with minimal human intervention. It can be said that the biggest investment banks in the world in the age of computer services has been distributed on ATMs and money. Withdrawal to the ceiling specified in the day. (Ebrahimifard 2004)
  - (B) Banking kiosk device: A device that after customer identification card withdrawals all services provided to customers in other bank ATM. Exchange, polls, buy tickets for buses, trains and planes safely connect to the Internet Banking can also be made from this device (Koshtegar 2012).
  - (C)Machines, point of sale (POS): means the electronic funds transfer at point of sale. Customer at any point of time and place can use a secure payment link from their account at a bank or financial institution and the product or service that is transferred to the seller (Ebrahimifard 2004). This device allows the seller to pay through credit card the cost of goods or provision of services (Koshtegar 2012).
  - ATM of (PINPAD) branch: A device that allows the Bank to provide banking services to customers based on their card (Koshtegar 2012).

Telephone banking: a balance of trade between banks and customers over the phone, called telephone banking. Methods used in telephone banking, include voice response, voice recognition and programmable phones. Telephone banking include facilities such as check account balance and circulation, pay bills, cash management, messaging services and cash transfers to other accounts (Hashemian 2004).

Mobile Banking: Banking services through mobile software at any place and time is available. The software-based technology and mobile operating systems, JAVA, ANDROID are more widely used by banks and customers. If necessary, make changes in response to the user database, and the operation is done (Koshtegar 2012). When mobile networks WAP, GPRS, UMTS, are equipped to offer next-generation multimedia services, mobile banking will enter the industry (Maleki and Akbari 2011).

Internet banking: the use of the Internet as a communication channel for remote banking services. With the help of internet banking the services are not limited to the time and geographical boundaries and it has many benefits for banks and customers (Karjaluoto, Mattila et al. 2002).

4. **ANALYSIS**

Based on a review of information in the field of electronic banking, and HP LaserJet devices, is defined as follows:
Based on the models listed and mixed model, combining the techniques of intimidation and threat effects, it is shown in diagram 3, following classifications provides the management threats to the organization. This classification leads to a better understanding of the threats and can cover all security risks that can threat all security risks.

In this study the aim is the relationship between the 7-electronic banking port that is shown in Figure 2 with a variety of security threats (figure 3).

To identify the major security threats, a questionnaire was designed and distributed among 15 experts of Mellat Bank of Abhar.

According to Figure 3, a total of 48 items in the questionnaire was design. For example, Question 1 of the questionnaire (the extent to which people outside the organization, as planned and ill intent, can destroy corporate information through the following ports).

Table 1. Frequency table related to the first question of questionnaire

<table>
<thead>
<tr>
<th>very much</th>
<th>much</th>
<th>average</th>
<th>little</th>
<th>Very little</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>8</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>5</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>7</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

The t-student test and the SPSS program were as follows:

$$ t = \frac{1 + 2 + 3 + 4 + 5}{5} = 3 $$

$$ H_0 = \mu = 3 $$

$$ H_1 = \mu > 3 $$

$$ s = \sqrt{\frac{\sum (x - \bar{x})^2}{n}} $$

$$ t = \frac{y - \bar{y}}{s} $$

$$ \sqrt{n} $$
Fig. 3. Classification of security threats

One-Sample Test

Table 2. Results obtained from spss software for port

<table>
<thead>
<tr>
<th>Test Value = 3</th>
<th>Test Value = 3</th>
<th>Test Value = 3</th>
<th>Test Value = 3</th>
<th>Test Value = 3</th>
<th>95% Confidence Interval of the Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Value</td>
<td>T</td>
<td>df</td>
<td>Sig. (2-tailed)</td>
<td>Mean Difference</td>
<td>lower</td>
</tr>
<tr>
<td>ATM</td>
<td>1.524</td>
<td>14</td>
<td>0.150</td>
<td>0.3333</td>
<td>-0.2175</td>
</tr>
</tbody>
</table>
ATM in the first question of questionnaire

Table 3. Results for the various ATM in the first question of the questionnaire

<table>
<thead>
<tr>
<th>Question</th>
<th>Jisdec</th>
<th>Accep</th>
<th>Mobile</th>
<th>Phone</th>
<th>Internet</th>
<th>PINPAD</th>
<th>Kiosk</th>
<th>POS</th>
<th>ATM</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.524</td>
<td>3.556</td>
<td>-2.749</td>
<td>-4.298</td>
<td>0.823</td>
<td>3.697</td>
<td>2.646</td>
<td>2.983</td>
<td>1.24</td>
</tr>
</tbody>
</table>

Similarly, the remaining 47 items were tested in the same manner. Ports unspecified security threats were impressed with obtained t that was identified as follows:

Table 4. Results of a variety of threats and types of ports

<table>
<thead>
<tr>
<th>No.</th>
<th>MOBILE</th>
<th>PHONE</th>
<th>INTERNET</th>
<th>Kiosk</th>
<th>POSPAD</th>
<th>PORT</th>
<th>ATM</th>
<th>r</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.587</td>
<td>2.086</td>
<td>9.38</td>
<td>-2.201</td>
<td>-6.874</td>
<td>0.619</td>
<td>2.129</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.128</td>
<td>-7.619</td>
<td>2.358</td>
<td>-1.341</td>
<td>-3.059</td>
<td>0.628</td>
<td>1.655</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.342</td>
<td>-1.268</td>
<td>2.352</td>
<td>-8.889</td>
<td>-11.225</td>
<td>-3.771</td>
<td>-0.211</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.254</td>
<td>-4.545</td>
<td>4.159</td>
<td>-2.795</td>
<td>-2.475</td>
<td>-3.933</td>
<td>-1.24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.254</td>
<td>-4.518</td>
<td>4.159</td>
<td>-2.795</td>
<td>-2.475</td>
<td>-3.933</td>
<td>-1.24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.254</td>
<td>-4.518</td>
<td>4.159</td>
<td>-2.795</td>
<td>-2.475</td>
<td>-3.933</td>
<td>-1.24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.254</td>
<td>-4.518</td>
<td>4.159</td>
<td>-2.795</td>
<td>-2.475</td>
<td>-3.933</td>
<td>-1.24</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. CONCLUSION

Information security is a crucial issue for individuals and organizations. Substantial financial losses caused by the inattention in this category. This is related to the problem of classification of threats in order to find a model that is flexible and public. This model has suitable strategies and measures to prevent or reduce the impact of threats on information security sectors. The classification model identified in the survey in Figure 3, it's flexible and dynamic and has multiple dimensions. And other behavioral issue in motivation is considered threatened. According to the results in Table 4, in most categories of threats, vulnerabilities Gateway is a substantial benefit. The gateways are structured in a way that all staffs that have bad intentions will be able to steal information of organization that is important. This issue is related to organizational behavior and should design strategies for behavior management of staffs. Gateway also influences the types of threats that recognizes the threat described by t = 9.28, in general threats that are associated with e-banking portals displayed in the table above and the bank can charge them by its decision.

REFERENCES

5. ISO (1989). "Information processing systems-open systems interconnection-basic reference model."
16. Sadoskay et al., 2006, translators MirDamadi m. et al., Information Technology Security, the Supreme Council of Information.