A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks

Rustu Yilmaz [1], Yildiray YALMAN [1]

[1] Turgut Ozal University, Computer Engineering Department, Ankara, Turkey

Abstract: **Universities are the leading institutions that are the sources of educated human population who both produce information and ensure to develop new products and new services by using information effectively, and who are needed in every area. Therefore, universities are expected to be institutions where information and information management are used efficiently. In the present study, the topics such as infrastructure, operation, application, information, policy and human-based information security at universities were examined within the scope of the information security standards which are highly required and intended to be available at each university today, and then a comparative analysis was conducted specific to Turkey. Within the present study, the Microsoft Security Assessment Tool developed by Microsoft was used as the risk analysis tool. The analyses aim to enable the universities to compare their information systems with the information systems of other universities within the scope of the information security awareness, and to make suggestions in this regard.**

Key words: **Information security, risk analysis, ISO/IEC 27001, university information systems, risk analysis tools, Microsoft security assessment tool.**

1. Introduction

People have battled and fought wars for the properties that they value, throughout the centuries. “Information” appears as the most valuable asset in this century. In lexical terms, information means the facts acquired through research, observation, or learning, or the whole cases, facts and principles that can be attained by people [1]. Each branch of science describes information depending on its field and studies. Notwithstanding, information is a concept that changes depending not only on the branches of science, but also on the time and the changes in conditions. Information is used both to form people and to ensure an exchange of news among people. Information has become a production factor along with the technological developments in recent years [2]. Ensuring information security where there exists information constitutes the most important issue in this regard.

With the development of technology, information which lent its name to our era makes its presence felt in all areas of life. Regardless of their sectors, the institutions which have and use information in a timely and effective way become able to get ahead of their rivals and attain their goals sooner. As a matter of its importance, information requires adoption of necessary measures for the purpose of its protection. The concept of information security has been brought into our lives for the protection of the information against ill-intentioned persons or institutions which threaten information.

The information security standards that the developed nations originally developed by designing several frames of rules in order to protect their own information properties have become the standards that are operated all over the world today. Institutions that care about information try to protect information in the direction of these standards, and they register their efforts with various certificates.

Ensuring information security requires addressing the whole institution and reinforcing the layers of infrastructure, management and application and security policies through measures to be taken or trainings starting from the persons in such institution first.

This study aims to examine the information system infrastructures of the leading state universities and foundation universities in Turkey, report the risk statuses of these universities by means of an information security risk analysis tool, interpret the outcomes obtained and contribute to the

DOI: 10.18421/TEM52-10
https://dx.doi.org/10.18421/TEM52-10

Corresponding author: Rustu Yilmaz - Turgut Ozal University, Computer Engineering Department, Ankara, Turkey
Email: rustu.ylmz@gmail.com

development of an information security awareness in universities.

2. Information Security

Computer networks and the Internet ensure the continuity of access to information. In the information era, when the access to information is continuous, the information security means the communication of information from sender to receiver by protecting its secrecy and preventing it from being changed or held by the others [3].

The increase in the use of information systems has not only eased the life for both institutions and people, but also increased the importance of information security, and thus, the information systems for which high level security precautions are taken in an effort to ensure information security has taken its place in the institutions. Taking into consideration that every point in the world has connected each other through the Internet and the computer networks, the significance of security levels and security investments would be better understood [3].

The security of institutional information systems to and from which more than one person connects and gets service is more important than that of personal information. Institutional services vary according to the sector in which the institution operates and they gain value depending on the degree of importance. For instance, information is vital for banking systems and generally no loss or change in the information of any customer is allowed. For such reasons, ensuring institutional information security appears as the only ladder to ensure personal information security [3].

2.1. Use of Information Technologies

The importance of information security increases day by day due to the increase in the use of information technologies. Besides helping people to have access to information, information technologies also make people open to threats. The results of the research on the use of information technologies at enterprises conducted by the Turkish Statistical Institute are presented in Figure 1 [5].

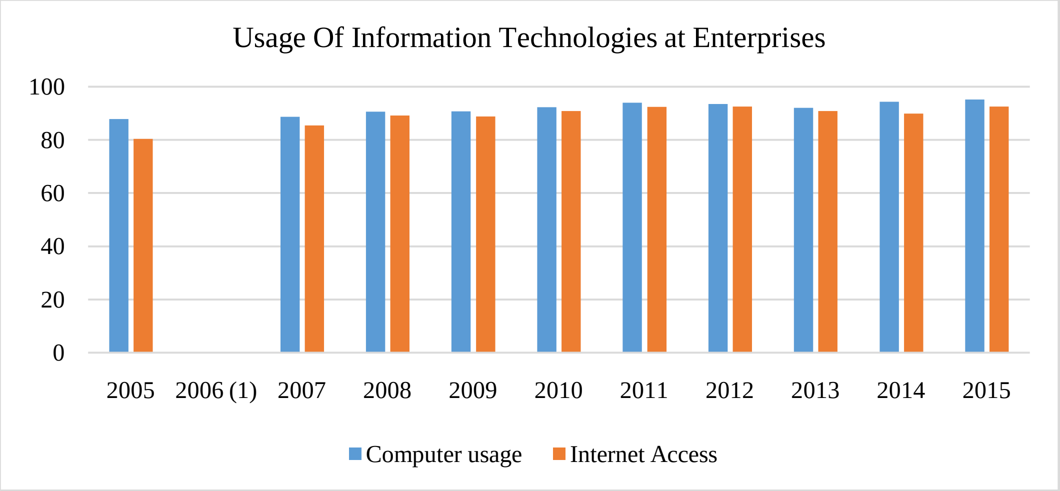

Figure 1. Use of Information Technologies at Enterprises
(1) No researches were conducted in 2006.

On examining the research data, it is seen that the rate of Internet use is above 90% in the institutions operating in Turkey. Considering that Turkey is not much ahead in terms of the use of Internet in the world, it can be concluded that access to information through online networks is much more common throughout the world. The high access rate proves the risks to which information is exposed and, therefore, information security gains more importance in this regard. The increase in use of Internet has also leaded to an increase in the attacks against information.

2.2. Identified Attacks

According to a report released by the Organization for Economic Co-operation and Development (OECD) in 2015, the biggest attacks against information security in the world by year are as follows [4]:

As a result of the cyber-attacks against Estonia in 2007, the parliament building, the prime ministry, banks, news agencies and publishers were adversely affected.

In 2010, as a result of an attack named “Stuxnet worm” against Iran, hundreds of centrifuges and nuclear equipment were destroyed [6].

As a result of an attack against the Sony Playstation networks in 2011, payment-related and personal information of 77 million users were stolen. It is estimated that the company had a loss of 250 million Dollar as a result of this attack.

As a result of the attacks against a petrol company, Saudi Aramco, lasted two weeks in 2012, all information kept on the internal network to which 30000 hard discs were connected was deleted [7].

An anti-spam producer, Spamhaus, experienced a denial of services (DoS) attack in 2013. This producer was exposed to a series of nine denial of services attacks including six moderate and three severe attacks. Some of these attacks were so unprecedentedly severe that could reach 300 Gigabits per second [8]. In the same year, a retail sales company operating in the United States, Target, was attacked on Christmas and information on 40 million credit cards and cash payment cards and the personal information of 100 million customers were stolen. This attack ended up with the resignation of a senior manager and costed billions of dollars [4].

As a result of the attack against a company named Home Depot in the United States in 2014, information on 56 million credit cards and cash cards was stolen. In Korea, a person stole the personal and credit card information of a total of 104 million customers of the three major banks in country. In the same year, the US Bank JPMorgan Chase was also attacked, and since the stolen information on 76 million home and seven million small-scale enterprises were in risk, the bank increased its security budget from 250 million Dollars to 500 million dollar. Sony Pictures Entertainment was also attacked the same year and both personnel data and e-mail information and information on non-released films were stolen. Finally, the attack against a steel company, Germany Led, caused a severe physical damage [4].

In December 2015, Turkey was exposed to a distributed denial of service attack (DDoS). This attack aimed to prevent the service of a total of six “.tr” domain name servers that were located at five different points. Some of these servers also had an Internet traffic of 200+ Gbps, which is very rare in history. An Internet organization in Europe, RIPE, which also involves one of the servers that provide domain name system (DNS) resolving abroad, turned off the server due to the intense attack [9].

The magnitude of and the damage caused by these attacks led to adoption of information security activities in various ways in every field.

3. Information Security Risk Analysis

Ensuring information security begins with identifying the risks. Various methods of risk analysis were developed in line with this aim. The risk analysis is divided into two basic categories: qualitative risk analysis and quantitative risk analysis. Some certain terms are used to conduct analysis in the qualitative methods [10]. For example, such terms as low-risk, moderate-risk, high-risk etc. may be used. The risk analysis method expressed by using mathematical and statistical expressions is, however, named as quantitative analysis method. The degrees of risks are presented using numerical expressions. In addition, there are also analysis tools that use both the quantitative and the qualitative analysis methods. While using these tools, one of the two analysis methods usually becomes prominent, therefore, these tools are regarded as more qualitative or more quantitative. Whether qualitative or quantitative, the risk analysis methods essentially aim to estimate the total value of risk in the environments where they are used [11].

3.1. Scope of the Analysis

In the present study, the information systems of universities were examined using a risk analysis method. Information systems are composed with a combination of six main systems. These systems are listed as follows: physical components, software components, data, persons, necessary rules and connections [12]. Within the scope of the present study, analyses were conducted at the leading State and Foundation universities in Turkey. The analysis conducted involves the evaluation of these mentioned systems. The information on the universities included in the analysis are presented in the following table [13].

A freeware-licensed tool, MSAT, developed by Microsoft® was used within the scope of the present study, and the results were analysed comparatively.

Table 1. Information on the Universities included in the Analysis

Universities*	Type	Number of Faculties	Number of Institutes	Number of Departments	ISO/IEC 27001	Number of Students
1st University	State	6	6	63	Yes	27222
2nd University	State	17	14	123	In the process of 27001	42438
3rd University	State	18	13	163	At planning phase	64469
4th University	Foundation	5	3	14	At planning phase	1002
5th University	Foundation	9	12	48	No	12577
6th University	Foundation	5	3	40	No	6402

* The real names of the related universities are not presented since these institutions' private data are shared.

3.2. MSAT (Microsoft Security Assessment Tool)

Microsoft Security Assessment Tool (MSAT), developed by Microsoft, is a high-level security assessment tool. This tool employs the qualitative analysis method. It was designed to provide the information technologies managers with information and recommendations about the security infrastructure of information technologies. It consists of two different layers; the first layer is for recognizing the existing organization and determining the risk status. The second layer, on the other hand, includes questions about the institution's infrastructure, application layer, operations and persons.

The questions were compiled from the suggestions of the employees at ISO/IEC 27001, NIST-800.x and Microsoft. In a way to embrace the whole institution, these questions assess the security status of the institution in terms of persons, operations, and technology [14, 15].

MSAT stages are as follows:

1. Basic information on the institution as well as information on infrastructure security, application security, operation safety, human security and environment are obtained from the person(s) that know about the institution to be analysed and have general information about the latter.
2. A new risk assessment is designed with regards to the security control.
3. Once all of the questions are responded, MSAT creates a report. This report presents a business risk profile and the security assessment result.

MSAT also calculates the security maturity status of the institution. Security maturity status means application development for a sustainable strong security. Multiple security defence systems are recommended for the institutions which are of low security maturity. In addition, the detailed report analyses the statuses of the institutions in a detailed way, and provides these institutions with recommendations depending on the security precautions taken by themselves. Created by Microsoft, these recommendations conform to the information security standards. One of its most important features is that it allows for a security comparison between similar institutions when required [15].

4. Analysis Assessment Results

In the present analysis study, the persons who have a knowledge of the system security and network infrastructure among the information systems of universities, generally with the redirection of the heads of the information processing departments, were visited and, then, MSAT application was run, and the report was obtained following the completion of required information with these persons. The study begins with the questions asked about the institution, and a business risk profile (BRP) is created depending on the activities performed. The risk profile varies by the applications planned to be sold or by worries of theft and spying of some of the universities. On the other hand, the questions in the second part are asked to compile a list of security precautions taken by universities. These questions ensure detecting the security measures taken, layers of defence, security risks and security vulnerabilities and preparing precautions to recommend for the security precautions for protection. A Defence in Depth Index (DiDI) is created in line with the responses. Then, an analysis is obtained by comparing the responses given within these two parts. The following reports are prepared for universities as a result of the analysis:

- **Security Maturity**: Security maturity is the measurement of a university's ability to create a sustainable security level by using the existing tools.
- **Business Risk Profile (BRP):** A business risk profile is the risk profile of universities for their business pattern.
- **Defence in Depth Index** (DiDI): A defence in depth index is the measurement of the precautions that have been taken to minimize the identified risks.

On examining the sustainable security maturity measurement of the universities within the analysis study. It is seen that the universities which bear a certification, in the process of a certification and are planning to get a certification have a sufficient maturity level in terms of infrastructure, application, operation and human; on the other hand, the other two universities are required to create a security awareness through trainings.

Table 2. Security Maturity Levels of Universities

	Scope of the Analysis			
Universities	Infrastructure	Application	Operation	Human
1st University	🟢	🟢	🟢	🟢
2nd University	🟢	🟢	🟢	🟢
3rd University	🟢	🟢	🟢	🟢
4th University	🟢	🟢	🟢	🟢
5th University	🟢	🟢	🟢	🔴
6th University	🟢	🟢	🟢	🔴

🟢Meets best practice 🟡Needs improvement 🔴Severely lacking

As can be seen in Table 2, the necessary investments were made in the universities analysed, and put into applications to some extent. New needs will certainly occur due to the advancing technologies. However, in order to ensure a better use of the current capabilities, first the persons who will use these capabilities are required to be addressed and a security awareness is required to be imposed to everyone from the management who use the informational assets.

The detailed outcomes of the business risk profile obtained on the infrastructure, application, operation and human resources and the defence in depth of the universities studied are as follows:

4.1. Security Infrastructure

In order to gain access to systems, the ill-intentioned or curious people generally use the remote access or sharing means that are used today as the network systems have become common and they can gain access to the information of the institutions. When ill-intended people gain access to systems, they take such steps that put the security and integrity of the institutions at risk as obtaining information to which they are not authorized or permitted to access, rendering systems out of order, making changes on such information, and sharing information with unauthorized third persons. There has been an increase in the violations of information security as the computer networks has become more common. Thus, the precautions required to prevent these violations and ensure information security have increased in number [16].

The communication between computers both through wired and wireless networks has created the need to ensure the security of these networks. Too many products have been developed for the security infrastructures of information systems. These products include the firewalls, attack detection systems, anti-virus programmes and physical security systems. These systems are the minimum infrastructure requirements that must be available in the information systems to ensure information security. According to the present analysis, the graph showing the precautions taken by the universities with regards to the infrastructure is as follows.

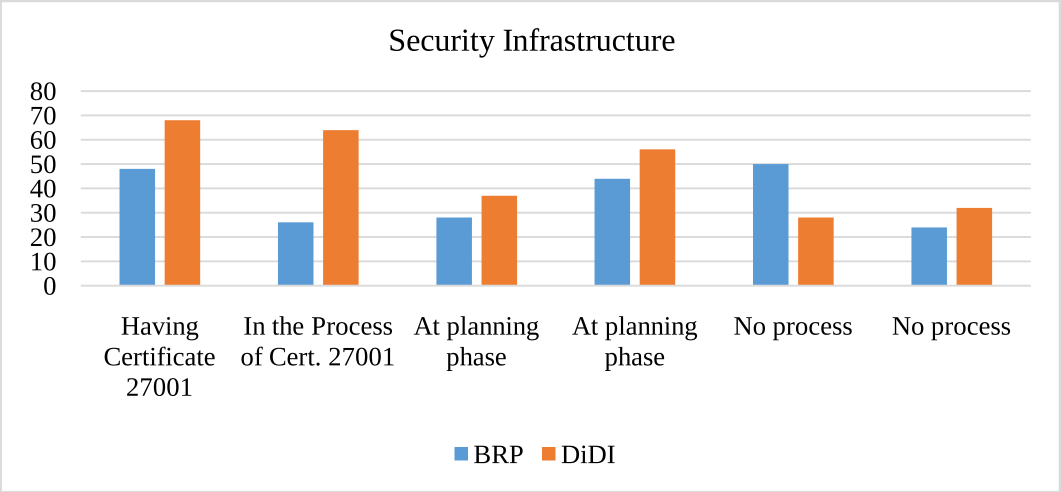

Figure 2. Comparison of the information security infrastructures between the universities

As seen in Figure 2, it can be clearly seen in the present analysis study that, in general, the universities take infrastructural precautions. Even if certain investments have been made almost at each institution to some extent, it can be stated that the universities that conduct studies or make planning for the purpose of obtaining ISO/IEC 27001 certificate are more successful than the others. On examining the infrastructural analysis study in depth, the outcomes obtained are as follows (Table 3):

Table 3. Comparative Analysis for the Infrastructural Security at the Universities

	1st	2nd	3rd	4th	5th	6th
Infrastructure	🟢	🟡	🟡	🟡	🟡	🟡
Primary Defence	🟢	🟢	🟡	🟢	🟡	🟢
Firewall and the rules	🟢	🟢	🟢	🟢	🟡	🟢
Anti-viruses	🟢	🟡	🟢	🟢	🟡	🟢
Anti-viruses - Desktops	🟢	🟢	🟢	🟢	🟢	🟢
Anti-viruses – Servers	🟢	🟢	🟢	🟢	🔴	🟢
Remote Access	🟢	🔴	🔴	🟡	🔴	🟡
Network Segments (VLAN)	🟢	🟢	🟡	🟢	🟢	🟢
Intrusion Detection Systems (IDS)	🟡	🟢	🔴	🟡	🔴	🟡
Wireless	🟡	🟡	🟡	🟡	🔴	🟡
Authentication	🟡	🟡	🟡	🔴	🟡	🔴
Administrative Users	🟡	🟡	🟡	🟡	🟡	🟡
Internal users	🟢	🟡	🟢	🟢	🟢	🟢
Remote Access users	🔴	🔴	🟢	🔴	🟢	🔴
Password policies	🟡	🟡	🟡	🟡	🟡	🟡
Password policies-Administrator Account	🟢	🟢	🟢	🟢	🟢	🟢
Password policies-User Account	🔴	🔴	🔴	🔴	🔴	🔴
Password policies-Remote users	🔴	🔴	🔴	🔴	🔴	🔴
Inactive Accounts	🟢	🟢	🟢	🟢	🔴	🟢
Administration and Monitoring	🟢	🟢	🟡	🟡	🟡	🟡
Event reports &Response	🟢	🟢	🟡	🟡	🟢	🟡
Secure Build	🟢	🟢	🟡	🔴	🔴	🔴
Physical security	🟢	🟡	🟡	🟢	🟡	🟢

🟢Meets best practice 🟡Needs improvement 🔴Severely lacking

Since MSAT, the analysis software used in the present study, regarded the use of a remote desktop as a security vulnerability in the analysis, it is seen as a factor of danger at the most of the institutions. The universities that use remote desktops generally use virtual private networks (VPNs). This is a method of secure connection provided by the firewalls. According to the results of the analysis, each university has firewalls, intrusion detection systems, anti-virus software and physical security all of which are of great importance to ensure security. The only prominent university is the 1st University which has an ISO/IEC 27001-certified information security system. The reason for its prominence is that it supports these security tools with policies and rules. On the other hand, the fact that its users have awareness about information security constitutes the main advantage of the 1st University.

4.2. Security and Application

When the analysed universities are evaluated, it is observed that they generally have the standard applications for application security such as clustering and load distribution. However, only the universities that have or are in the process of a certification are observed to have the non-standard applications such as encryption algorithm. It is obvious in the following graph that the universities that have obtained, are trying to obtain or are planning to obtain an information security certification take more precautions than the other universities (Figure 3).

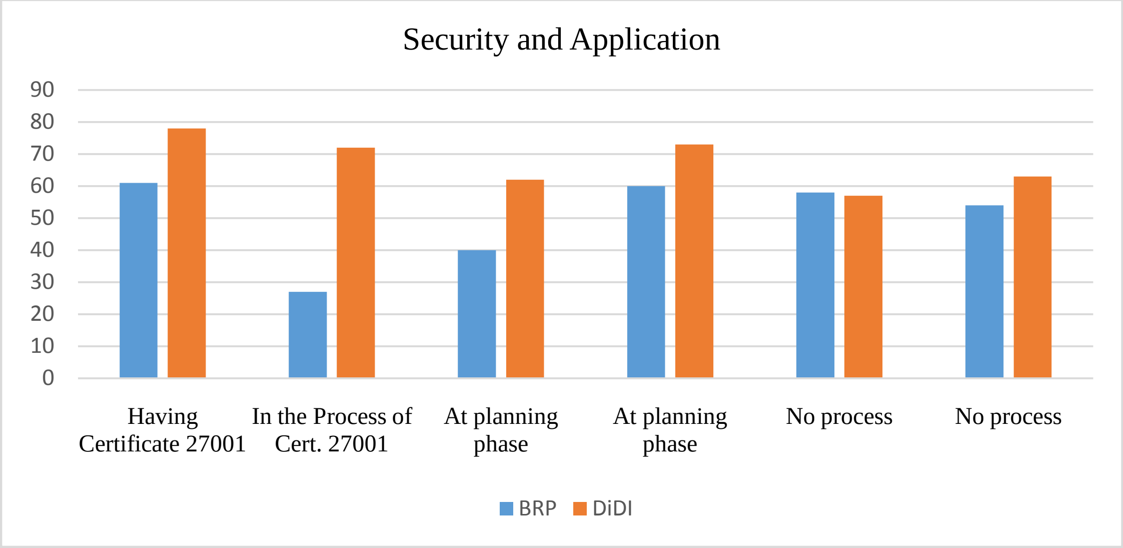

Figure 3. Application Security at Universities

The detailed results of the analysis study, obtained for the application security, are presented below in further detail (Table 4). It can be clearly understood from the table that each university applies successfully the identity validation policy and password policy. Moreover, it can be seen that each university has a load distribution device that is generally supplied as a hardware and each of them performs the clustering installations that are vital for the business continuum.

Although each university interviewed stated that they had a software team and they were developing applications, it is clear that they make no investment or impose no sanctions for secure software development. No application was observed for input supervision in none of the universities other than the one which bears an ISO/IEC 27001 certificate.

Table 4. Results of the Application Security Analysis

	1st	2nd	3rd	4th	5th	6th
Application	🟡	🟡	🔴	🔴	🔴	🔴
Development and Use	🔴	🟡	🔴	🔴	🔴	🔴
Load Balancing	🟢	🟢	🟢	🔴	🟢	🔴
Clustering	🟢	🟢	🟢	🟢	🟢	🟢
Application & Data Recovery	🟢	🟢	🟢	🟢	🟢	🟢
Third-party independent software Vendor(ISV)	🔴	🟡	🔴	🔴	🔴	🔴
Inside development	🔴	🔴	🔴	🟢	🔴	🟢
Weaknesses	🔴	🔴	🔴	🔴	🔴	🔴
Application Design	🟢	🟡	🔴	🔴	🔴	🔴
Authentication	🟢	🟢	🟢	🟢	🟢	🟢
Password Policies	🟢	🟢	🟢	🟢	🟢	🟢
Access Control	🟢	🟢	🟢	🟢	🔴	🟢
Logging	🟢	🟢	🟡	🟡	🟢	🟡
Input Validation	🟢	🔴	🟡	🔴	🔴	🔴
Software Security Development methodologies	🟡	🔴	🔴	🔴	🔴	🔴
Data Storage & Communications	🟡	🟡	🔴	🔴	🔴	🔴
Encryption	🟡	🟡	🔴	🔴	🔴	🔴
Encryption Algorithm	🟡	🟡	🔴	🔴	🔴	🔴

🟢Meets best practice 🟡Needs improvement 🔴Severely lacking

The efficiency of the information security certification programme ISO/IEC 27001 for the encryption of vulnerable data can be seen in the detailed analysis.

As far as observed, the universities either do not have a systemic weakness or gap or they do not know whether they have one. In the interview made at the university that has ISO/IEC 27001 certificate, they stated that they were aware of a weakness and they were trying to take precautions against it.

4.3. Security and Operation

The information systems may need to be changed or get informed about the risks due to the development of new risks or presence of already-existing risks. Operational evaluations include the operational functions, threats, security vulnerabilities, work processes, facilities, the practice of the changes in the policies and regulations, the changes in the technical skills and the methods of the ill-intended people who attack the system and the decrease in the current sources within the institution [17]. The rapid development in technology and people's confidence both generally in the Internet and in doing their transactions on the Internet have brought along the information security problems. According to the data obtained from the Organization for Economic Co-operation and Development, attacks also increase rapidly with the evolving technology. The increase in the attacks and the damage to the companies and countries around the world require establishment of national information security policies [18].

According to the present analysis, the results obtained with regards to the operational departments at the universities are as follows:

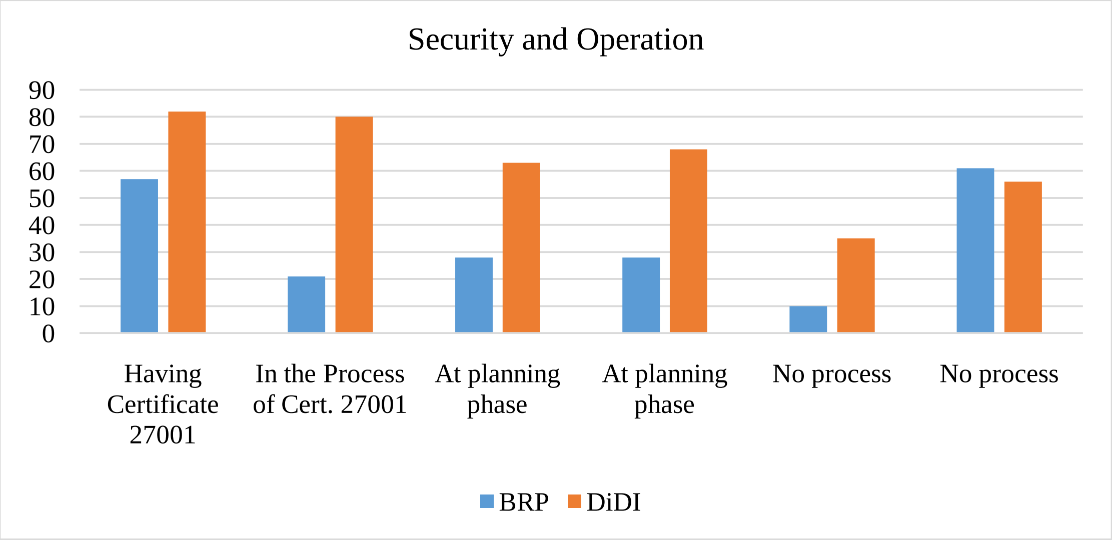

Figure 4. Results of the Operational Security Analysis at the Universities

The universities that are in the process of or already have an information security certificate were seen to have completed almost all of the procedures required in terms of the operational management (Table 5). It was also observed that the universities which are planning to obtain an information security certificate were applying information security, even if not so successfully as the first two universities, and the universities that had no effort for information security had more risks than the precautions they have taken or were applying little information security, even if they tried to implement the necessary procedures.

Table 5. Operation and Security at the Universities

	1st	2nd	3rd	4th	5th	6th
Operation	🟢	🟢	🟡	🟡	🔴	🟡
Environment	🔴	🟢	🟢	🔴	🔴	🔴
Management Host	🔴	🟢	🟢	🔴	🔴	🔴
Management Host–Servers	🔴	🟢	🟢	🔴	🔴	🔴
Management Host-Network Devices	🔴	🟢	🟢	🔴	🔴	🔴
Security Policy	🟢	🟡	🔴	🟡	🔴	🟡
Data Classification	🟢	🟡	🔴	🔴	🟡	🔴
Data Disposal	🟡	🟡	🔴	🔴	🔴	🔴
Protocols & services	🟢	🔴	🟢	🔴	🔴	🔴
Acceptable use	🟢	🟢	🔴	🟢	🔴	🟢
User Account Management	🟢	🟢	🔴	🟢	🟡	🟢
Administration Policies	🟢	🟢	🔴	🟢	🟢	🟢
Security Policies	🟢	🟢	🔴	🟢	🔴	🟢
Patch & Update	🟢	🟢	🟢	🟡	🔴	🟡
Network Documentation	🟢	🟢	🟢	🔴	🔴	🔴
Application Data Flow	🟢	🟡	🟡	🔴	🔴	🔴
Patch Management	🟡	🟢	🟢	🟢	🟡	🟢
Change Management and configuration	🟢	🟢	🟡	🟡	🔴	🟡
Back-up and Rescue	🟢	🟡	🟢	🟡	🟡	🟡
Log Files	🟢	🟢	🟢	🟢	🟢	🟢

Disaster Recovery & Business Resumption Planning	🟢	🔴	🟢	🔴	🔴	🔴
Backup	🟢	🟢	🟢	🟢	🟢	🟢
Backup Media	🟡	🟢	🟢	🟡	🟢	🟡
Backup &Restore	🟢	🟢	🔴	🔴	🟡	🔴

🟢Meets best practice 🟡Needs improvement 🔴Severely lacking

According to the detailed table, it is clear that the ISO/IEC 27001 certification positively affects the information security of the universities. With the help of this certification, the universities better create and apply especially the security policies. All of the universities were observed to have security policies to some extent. The universities have efforts especially for physical security, encryption security and Internet security. Looking from the point of view of the information system employees, the universities were observed to have information security awareness to some extent, but not sufficient for the standardized levels due to lack of support by the management and other similar reasons. It is seen that the universities which have even not a planning level for information security had no information security training activities for employees including the information processing personnel. The information processing personnel, therefore, established and applied certain policies as far as they knew and searched and with their own efforts. However, they were not regarded as sufficient when evaluated within the scope of the certification of 27001. In addition, all of the procedures for patching and updating were observed to be applied by the universities that had or were in the process of a certification. Due to the fact that back-up is essential to prevent loss of information, no problem was generally observed about back-up and rescue procedures. Having perfect security policies after making the necessary hardware investments is not enough for security. These investments are useless unless there is a resource of conscious humans.

4.4. Security and Human

Kevin Mitnick says "If a hacker contacts a reliable employee at a company, gains his trust and breaks into the company, then the money spent for security so far is wasted." [19] This quote illustrates the importance of the humans for security.

The most critical factor with regards the information security is the human factor [20]. Despite using developed technologies and providing quality training, it is impossible to say that a system is under protection unless people have information security awareness. Information security is a process that renovates itself and that is always open to innovations. There are different dangers for tomorrow even in a system that is of the best standards and is equipped with the best technology. It is never possible to say that a system provides success 100%. It is necessary to act in a continuously developing process to meet the needs of tomorrow. A reached point is always one-step behind tomorrow [2].

According to the results of this analysis study, it is seen that especially the institutions that have no certification of information security or currently do not apply any information security rules have the most important weakness due to the human factor.

Another significant factor observed during this analysis is that the universities that have or are in the process of a certification have authorized employees for information security, and an information security department under its roof. Having an information security department demonstrates that the university management cares about information security and proves the presence of information security awareness. According to the following graph, two universities become prominent thanks to this awareness.

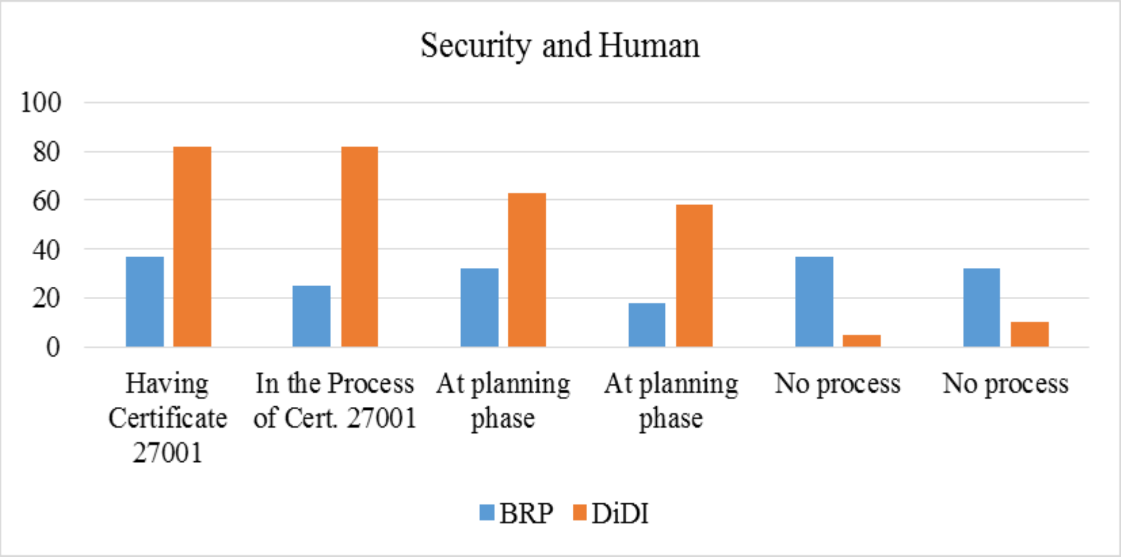

Figure 5. Results of the human resources security analysis at the universities

The present analysis study is designed according to the security knowledge and responses of people. The detailed results of the analysis obtained through the data on the people are as follows (Table 6):

Table 6. Results of the analysis conducted on the people at the universities.

	1st	2nd	3rd	4th	5th	6th
People	🟢	🟢	🟡	🟡	🔴	🔴
Requirements & Assessments	🟢	🟢	🟢	🟢	🔴	🔴
Security Requirements	🟢	🟢	🟢	🟢	🔴	🔴
Security Assessments	🟢	🟢	🟡	🟡	🔴	🔴
Policies & Procedures	🟡	🔴	🔴	🟢	🔴	🔴
Background Checks	🔴	🔴	🔴	🟢	🔴	🔴
Human Resources Policy	🟢	🟡	🟡	🟢	🟢	🟢
Third-Party Relationships	🟡	🟡	🔴	🟡	🔴	🔴
Training & Awareness	🟢	🟢	🟡	🟡	🔴	🔴
Security awareness	🟢	🟢	🟢	🟡	🔴	🔴
Security trainings	🟢	🟢	🔴	🟢	🔴	🟡

🟢Meets best practice 🟡Needs improvement 🔴Severely lacking

When the table is examined, it is seen that the employees at the university that has achieved the processes of ISO/IEC 27001 are at a sufficient level for security, get regular trainings and have security awareness. on the other hand, it is observed that the employees at the universities that are planning to obtain one, have a knowledge of security to some extent, but their knowledge needs to be improved. Every point except for human resources at the universities that have no effort for information security needs to be improved and poses danger.

5. Conclusion

The results of the study reveal that it is possible to increase information security at universities by taking several precautions.

Observations show that each of the analysed universities has an application development team, but they need to take precautions and provide training for their employees for secure application development procedures. Moreover, it is observed that the universities do not take enough care for data categorization and encryption of vulnerable data.

Since human is the primary factor about operation, from management and planning to application, it was found that the human factor directly affected every stage of the analysis. In addition, it was seen that documenting and keeping documents updated are the common problems of universities and these problems could be overcome by increasing information security awareness among people.

It is clear that institutional information security management systems are crucial for the protection of information properties; therefore, the universities that are planning or making no effort to obtain an ISO/IEC 27001 will diminish the information security risks by applying the ISO/IEC 27001 procedures in case that they attempt to use institutional information security management systems.

Evaluating generally the universities visited during the analysis, it can be seen that the universities that have or are in the process of a certification have rules and principles on every component from the entry to the people to interview, which shows the great importance of the certification process for the protection of information properties.

All in all, it is revealed that universities need to conduct a risk assessment by identifying the information properties, threats, weaknesses and security vulnerabilities of their systems by using comprehensive analysis programmes and to make attempts to diminish the risks for their informational assets by determining risk acceptance values in the direction of this risk assessment.

6. References

[1]. Güncel Türkçe Sözlük, http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.568f6ce848c209.12198361, Access Date:08January 2016.

[2].Ismayil Gokhan Akay, (2014), *Information Security Management Systems: Information Security Application Reviews*, Master of Science Thesis, Şeyh Edebali University.

[3].Bhatt, Ganesh D. (2001). *Knowledge management in organizations: examining the interaction between technologies, techniques, and people. Journal of knowledge management*, 5(1), 68-75.

[4]. OECD Recommendation and Companion Document, "Digital Security Risk Management For Economic and Social Prosperity" http://www.oecd.org/publications/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm, Access Date: 4 January 2016

[5].Information Society Statistics (2015), ICT Usage Survey in Enterprises (In Turkish), Turkish Statistical Institute.

[6].Karnouskos, S. (2011, November). *Stuxnet worm impact on industrial cyber-physical system security*. In IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society (pp. 4490-4494). IEEE.

[7]. Bronk, C., & Tikk-Ringas, E. (2013). *The cyber-attack on Saudi Aramco*. Survival, 55(2), 81-96.

[8]. Genge, B., &Siaterlis, C. (2013). *Analysis of the effects of distributed denial-of-service attacks on MPLS networks*. International Journal of Critical Infrastructure Protection, 6(2), 87-95.

[9]. DDoS attacks (2015), Public announcement, Middle East Technical University.

[10]. Peltier, T. R. (2005). *Information security risk analysis*. CRC press.

[11].Fatma Ozden Aktas, (2009), *Choosing The Most Proper and Objective Method in Information Security Risk Management*, Master of Science Thesis, GebzeTechnical University

[12].Whitman, Michael, and Herbert Mattord. (2011) *Principles of information security.* Cengage Learning,

[13].Statistics of Turkish Universities, https://istatistik.yok.gov.tr/, Access Date: 21 November 2015

[14].Microsoft Security Tools MBSA and MSAT Explained, http://www.computerweekly.com/tip/Microsoft-security-tools-MBSA-and-MSAT-explained, Access Date: 9 November 2015

[15].Ionita, Dan. (2013), *Current Established Risk Assessment Methodologies and Tools*

[16].Yılmaz Vural, (2007), *Enterprise Information Security and Penetration Testing*, Master of Science Thesis, GaziUniversity

[17].The Government of the Hong Kong Special Administrative Region: Patch Management http://www.infosec.gov.hk/english/technical/files/patch.pdf, Access Date: 4 January 2016

[18].OECD (2012), *"Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy"*

[19].Whitman, M., & Mattord, H. (2013). *Management of information security*. Cengage Learning.

[20]. Alnatheer, M. A. (2015, April). *Information Security Culture Critical Success Factors.* In Information Technology-New Generations (ITNG), 2015 12th International Conference on (pp. 731-735). IEEE.