Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 122 (2019) 32-43 EISSN 2392-2192

Information security management in an individual documentomat project

Tomasz Chajduga

Faculty of Management, Czestochowa University of Technology,
69 Dabrowskiego Str., 42-200 Czestochowa, Poland

E-mail address: tchajduga@gmail.com

ABSTRACT

This publication discusses the concept of information security management based on a documentomat machine. In addition, the device has been described itself, its place in the information flow system and its impact on improving the competitiveness of the reference company using this device.

***Keywords*:** information security management, documentomat, parcel locker, information security, secret of correspondence

1. INTRODUCTION

Information in modern world has a particularly high value. Through the general wide access to technology, it can be processed and transmitted extremely quickly, which makes the data of various entities particularly sensitive to leaks and unauthorized access [1]. On the other hand, users of information, recipients to whom data is addressed, are becoming more and more used to comfortable and easy access using more and more flexible solutions [2], with implemented standards and procedures ensuring a high level of security [3].

Information security means protection of information against various threats in such a way as to ensure business continuity, minimize losses, maximize return on investments and business activities [4]. The issue of information security management and the construction of

(Received 04 February 2019; Accepted 20 February 2019; Date of Publication 21 February 2019)

information security management systems is regulated by the ISO / IEC 27000 family standards. These are primarily:

• PN-EN ISO / IEC 27001;
• PN-EN ISO / IEC 27002.

The first of the above standards, PN-EN ISO / IEC 27001, is also called Information Technology - Security Techniques - Information Security Management Systems - Requirements. It defines the requirements for the establishment, implementation, maintenance and continuous improvement of the information security management system in the organization, taking into account the circumstances the organization operates. In addition, it also provides tailor-made requirements for estimating and dealing with risks in information security. This standard is the canon of information security and is used not only in Poland but throughout the world. The standard with the number PN-EN ISO / IEC 27002 is called Information Technology - Security Techniques - Practical Information Security Principles. It provides recommendations on information security standards in organizations and information security management practices, including the selection, implementation and management of collateral. According to the Polish Standardization Committee, the more stringent information security standards developed by ISO and IEC are considered to be the basis for safe management of sensitive data.

In this publication, the documentomat is a term for a machine used to issue documentation in an organized, supervised and targeted manner, ensuring security to the documents issued with its help. This device could be called a parcel machine, because you can also store documents in parcels, moreover, the document file can be perceived as a parcel, but the polish name "paczkomat" has been reserved, patented by one of the service providers made using such devices. In general, a documentomat from a parcel locker can be distinguished through the boxes. In case of the first one they should be narrower in order to simultaneously serve a larger number of recipients, i.e. in particular to increase the possibility of simultaneous storage of documents addressed to a larger number of interested persons.

The practice indicates that providing large spaces for the purpose of disposing of larger amounts of documents with use of the device is generally unnecessary [5] - parties are interested in receiving relatively often fewer documents rather than rarely receiving large amounts of data (documents) [6]. On the Polish market at least several solutions are available in the field of devices that can be used to automate the issuing (withdrawal) of documents or parcels.

The solutions that can be quoted are:

- InPost parcel lockers;
- ZPAS Lab3 depository;
- Parcel Technik4 secretaries;
- other.

It should be noted that in the case of each of the above companies, the details of the solutions used are the secret of the entities that produce them, and the level of security used is largely independent of the recipient of the device. He has no influence on this level. The use of an individually developed solution allows you to have full control over the security level, allows you to perform separate tests of each of the device components.

We should also mention the possibility of further expansion or implementation of future modifications, limiting costs to a minimum, i.e. in the purchase price of components. In the longer term, it could also allow the company to expand its offer to sell such or similar machines. The above features seem to be particularly encouraging to implement and develop their own device concept.

The reference X undertaking, for which the issues discussed in this publication are significant, deals with the processing of their clients' data - mainly correspondence, including a wide range of diverse documentation. This documentation, despite its processing, often has a source value and some customers recognize and report the need to have original documents in their archives. The purpose of the device, here referred to as the documentomat, would be to enable automated and secure delivery of such documentation to the clients of enterprise X, also after or before the operating hours of the office. This would let the clients of enterprise X utilize human resources [7].

The main objective of the study is to indicate ways to manage information security in an individual documentomat project. This publication introduces issues related to the need to ensure permanent and secure access to documents processed [9] by a reference company managed by the author of this publication, which are reported by the company's clients. The publication describes the process of making decisions regarding the arrangement, development and implementation of the original design of the described device – documentomat, what is able to improve the performance of the company X [10].

Such machine would reflect the information processing as an integrating concept in organizational design [8]. A SWOT analysis was carried out to implement the assessment of the possibility and legitimacy of the creation of a parcel machine.

2. THE SITUATION ON THE MARKET OF DEVICES FOR THE AUTOMATED WITHDRAWAL OF PARCELS AND DOCUMENTS - A DESCRIPTION OF THE FEATURES OF AVAILABLE MACHINES

During the analysis of solutions available on the domestic market that can be used for the automated issuing of documents, the following have been distinguished:

- InPost1 parcel machines;
- ZPAS Lab2 deposit machines;
- Parcel Technik3 secretaries.

InPost parcel lockers are the most common available solution. They are characterized by strong integration with the Internet and GSM networks. This means that the recipient receives automated e-mails as well as sms about sending the parcel, waiting for it to be picked up at the destination and its release. Currently, the use of this solution is integrated with the courier service and the details of the solution, as well as the name "Paczkomat" are legally protected by means of patent protection. Authentication of the package recipient is carried out using codes sent by e-mail or text message.

ZPAS Lab deposits are similar, but have a popular solution. The manufacturer delivers them without a courier service. These devices are characterized by a modular design, consisting of a set of columns with storage boxes, allowing a large configuration of the number and size of deposit boxes and various methods of authentication and identification of persons using a

deposit machine. These machines are characterized by the use of the Internet for correct operation and diagnostics - on-line control of the depository resources enables remote monitoring and central supervision through a dedicated IT system, as generally described in literature [15].

The manufacturer ensures the possibility of installing a ventilation, heating or cooling system for stored deposits (depending on the needs). Parcel Technik is a solution currently under construction. The main market for Parcel Technik is Poland, where the device manufacturer focuses on the preparation of a network of automatic boxes for the distribution of domestic and foreign parcels. The company's specialists also work on the construction of their own network of automatic boxes on the territory of Germany and Israel, where they sell similar devices, such as kiosks, night time slots, multi-divisions. According to press releases, Parcel Technik machines ensure issuing and receiving parcels by means of a coded lock system without having to connect the machine to a power source or GSM network.

3. DESCRIPTION OF THE SUBJECT OF RESEARCH

Enterprise X is a company existing on the Polish market since April 2015. The offer of the X includes customized information processing, in accordance with the recommendations of customers, generally gathered according to parameters specified by X. Data processing is most often carried out immediately after receiving them, it usually takes up to 24 hours and ends with the transfer of electronic information in the form of an attachment (or attachments) to the authorized e-mail address specified in the contract. It is necessary to emphasize the special role of the channels indicated by the clients as authorized so the information processed by X is largely sensitive data according to the so-called RODO. Even those data processed by X, which are not directly subject to the above mentioned act, are often presenting the key value from the point of view of clients' interests.

Internal procedures of company X enable its employees to suspend or limit the processing of customer-company data if during processing it turns out that the nature of the data being processed questions the sense of their digitization, conversion and introduction to the network [18]. The customer may then decide to continue processing data or, for example, to personally collect critical and extremely confidential data for him or her. This is most often the case of multi-page draft contracts with contractors or lawsuits with a large number of attachments, i.e. documents in which persons responsible for managing the company personally want to eliminate any risk of leakage of even rudimentary information that may affect, for example, the price of shares listed publicly on stock exchange or the amount of credit lines provided by contractors.

The company's customers also report the need to receive unprocessed original documents directly from the office. A significant facilitation for many of them would be the ability to receive such materials outside the official business hours. The above-mentioned aspects have been indicated as a context for the company to look for solutions in the field of automated and secure way of issuing documentation. Next point, a SWOT analysis will be presented, in which particular factors influencing the direction of the implementation of the individual documentomat project will be considered in relation to the issues of information security management.

4. SWOT ANALYSIS OF THE LEGITIMACY OF IMPLEMENTING A DOCUMENTOMAT MASCHINE DEVELOPMENT PROJECT IN THE CONTEXT OF INFORMATION SECURITY MANAGEMENT OF X'S CLIENTS

The purpose of the SWOT analysis is to enable and facilitate the decision on whether it is worth to launch an individual project for the development of a documentomat - a device to be used for storing and automatically issuing documents.

3. 1. Presentation of the procedure of analysis to participants

Participants of the SWOT analysis (being employees of the X enterprise) were presented the procedure for its implementation, in order to ensure a unitary approach to the observed aspects that should be included in the analysis.

3. 2. Development of individual lists of strengths and weaknesses as well as opportunities and threats

As a result of the SWOT analysis, the following **strengths** were distinguished resulting from the development of an individual documentomat project:

- full control over security issues regarding to the machine to withdrawal of documents, as a part of the model of the process[11];
- the possibility of further developing, enriching the project - adding additional functions as needed, as well as adding more boxes to store documents for more clients (as a development of automation infrastructure [13] and supporting the unifying framework and flexibility [14]);
- high level of control over the performance and functioning of the device;
- high level of security resulting from the fact that 100% know-how about the manner of project implementation has been preserved in enterprise X;
- any further changes to the device can be made at the cost of materials;
- all possible repairs can be made at the cost of components;
- independent construction of the device will be significantly cheaper than the purchase of a ready solution;
- an individually implemented project means that the future use of the device will work at 100% of its capabilities - the machine will perfectly match the needs of enterprise X.

As a result of SWOT analysis, the following **weaknesses** resulting from the development of an individual documentomat project were distinguished:

- significant use of time resources - the implementation of the project to create a documentomat will be relatively time-consuming when compared to the purchase of a ready solution;

As a result of the SWOT analysis, the following **opportunities** resulting from the development of an individual documentomat project were distinguished:

- a company realizing such a project on its own will gain know-how and experience, which will enable its development of the product offer with such and similar devices;
- knowledge acquired during the project implementation may be sold to another company;

- the possibility of supporting the company's expansion by building a second similar device;
- project development gives the opportunity to enrich the company X with knowledge and technology from related fields, the recognition of which may result in further development.

As a result of the SWOT analysis, the following **threats** were distinguished resulting from the development of an individual documentomat project:

- the implementation of the project in order to create a documentomat can mean incurring (as it may be later) additional, excessive expenses, without which it would not be able to test all the solutions properly in the device;
- independent development and execution of the device will unfortunately also mean the lack of a guarantee given by external entity and need for a possible self-repair;
- there is a risk resulting from the complexity of the project (including the purchase of various elements, software, electronics, settings and assembly) that the project, despite the costs incurred, will never be completed.

3. 3. Discussion and dialogue of all participants involved in the study

As a result of the discussion involved in the research participants, the following conclusions were made:

Strong sides neutralize and outweigh the identified threats. Above all, strengths such as: full control over security issues (aspects), the possibility of further development, enrichment of the project and adding additional functions outweigh the threat resulting from the lack of guarantees and the existing threat due to the complexity of the project (including the purchase of various elements, software, electronics, settings and assembly) that the project, despite the costs incurred, will never be completed. Strengths in the form of: a high level of control over the performance and functioning of the device; high level of security resulting from the fact that 100% know-how about the manner of project implementation has been preserved in company X and any further changes to the device can be made at the purchase costs of materials outweigh the threat, which is the implementation of the project document creation that could mean the incurrence of additional, redundant expenses without which you will not be able to test all the solutions on your device properly. Then strong sides: all possible repairs can be made after the cost of components, independent construction of the device will be significantly cheaper than the purchase of a ready solution, individually implemented design will make future use of the device will take place in 100% of its capabilities - the machine will perfectly match the demand enterprises X will outweigh the threat resulting from the complexity of the project (including the purchase of various components, software, electronics, settings and assembly) that the project, despite the costs incurred, will never be completed (despite the incentive to eliminate waste [16].

It was recognized that the possibilities resulting from the implementation of the project neutralize the negative impact of these aspects of its implementation, which were identified as weakness. The following possibilities: the company realizing the project itself will gain know-how and new experience, which will enable development of its offer neutralizes or even prevails

the identified threat in the form of significant use of time resources - the implementation of the project will be relatively time-consuming compared to purchase of a ready solution.

4. TECHNICAL SOLUTIONS IN THE FIELD OF DOCUMENTOMAT INFORMATION SECURITY MANAGEMENT

The technical aspect of information security management in terms of the device used for automated document issuing is much more complex. In other words, level of security depends on the complexity of the systems used, their susceptibility to unauthorized outside interference, mutual separation, sensitivity to possible anomalies (mainly voltage spikes) occurring in the power grid, proper selection of input / output devices, applied software and access to the web.

A special level of security is to be ensured by additional separation of energy and logic (function) systems. Separation at the energy level will be achieved through several elements. First of all, the entire documentomat will be powered by a surge protector equipped with an additional energy meter, which will allow to make an additional check-up in case of increased power consumption. Secondly, it will be reasonable to include an additional PowerBank device between the power supply on the surge protector with adapter and the control module. The battery will remain charged at all times, ready to provide power to the controller in the event of voltage surges or decay, which will prevent the occurrence of any incorrect signal on the GPIO connectors that control the locks. The battery parameters are:

- 5200 mAh capacity (18.72 Wh);
- DCIN 5.0V / 1.0A;
- DCOUT 5,1V / 1,5A.

The detailed parameters of the adapter of the main controller are:

- Brand: Akyga;
- ACIN 100-240V, 0.5A 50 / 60 Hz;
- DCOUT 5V, 2500 mA.

Detailed parameters of the executive circuit adapter power supply (power supply locks):

- ACIN 100-240V, 0.6A, 50 / 60 Hz;
- DCOUT 12V, 2A;
- Compliance with the IP20 standard.

It should be mentioned that the power supply of the secondary circuit of the static relay unit will be implemented by alternating current from the power network (exit from the surge protector). Separation at the logical level will be accomplished by dividing into a number of controllers:

- Raspberry Pi 3 Model B - a de facto small computer, programmable, architecture-based microcontroller controlling GPIO connectors under Raspbian operating system, which can be powered by a small USB charger;
- Solid State Relay - a set of static (semiconductor) relays, working as a function of the electric lock controller, executing the command of the main controller;

- electric locks controlled by 12V and 2A, by impulse shorter than 1 second;
- the input device will be a computer wireless numeric keypad;
- an output device in the operating mode will be a sound card and a connected loudspeaker enabling the sound to be played, so-called beep;
- the output device in the operating mode will also be the locks themselves, opening of which will signal the correct operation of the device;
- the device entering into the diagnostic mode will be a full-sized computer keyboard;
- the input device in diagnostic mode will be a computer mouse;
- the output device in the diagnostic mode will be a computer monitor.

The diagnostic mode will be used in the development phase only. In order to store the software together with the database, as a driver, the "brain" of the device will be used the Raspberry Pi 3 Model B controller, characterized by the following parameters (Fig. 1):

- Broadcom BCM2837 quad-core processor 64-bit ARM-8 Cortex-A53 1.2 GHz;
- 1 GB of RAM;
- built-in WiFi and Bluetooth 4 module;
- four USB ports;
- 40 GPIO connectors;
- microSD card connectors;
- Ethernet port.

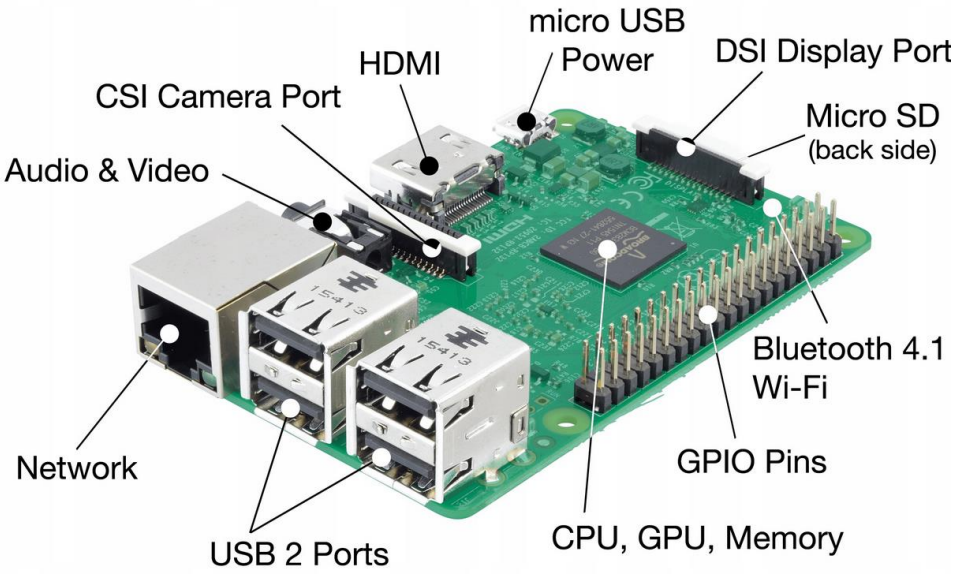

Fig. 1. Raspberry Pi 3 Model B

Installing the Raspbian system on the SD card allows to operate the Raspberry Pi 3 Model B as a regular PC. This system allows to run programs written in the Python programming language, which enables the operation of the SQLlite database. For this reason, it was decided

to use above mentioned database for storing information about the status of shipments stored in the device. The program (obtained as a software engineering process [12]) allows the device to work in one of two modes:

- service mode;
- standby mode.

The service mode is intended for employees of enterprise X and designed to leave documents in the machine. The standby mode allows secure receipt of documents at any time of the day or night. By default, the device will always be in standby mode. A person authorized to receive documents will have to provide a series of codes in order to do this:

- box code (boxes);
- customer code;
- one-time access code.

The example of the correct sequence that opens box number 5 is:

5 [ENTER] **2365** [ENTER] **6394** [ENTER]

After pressing button 5 and confirming it with Enter key, the machine will emit a single beep (single sound signal). It will mean that it recognizes the mailbox of this number as it is busy (stores the documents). Subsequent entering of the code 2365 and confirmation by pressing the Enter key will verify the client code, which will also be confirmed by a single audio signal.

Providing the next code will verify it (in the context of previously entered information), generate another single sound signal and open a mailbox number 5 containing information important for a specific client. In case of entering wrong code, the system (machine) will generate two shorter signals, which will mean come back to the basic standby state. It is worth noting that such system of coding system allows you to obtain over 100 million combinations. Considering that the client will not be provided with any diagnostic connector, no USB port or any possibility of connecting any automated device that allows quick code entry, the above presented code system is considered to be safe. In order to program the device, you will have to enter it into the service status.

This will be done by entering the service code. This code will contain special characters available only on the full keyboard of an employee of Enterprise X (clients - persons receiving documents will only have a numeric keypad, wired wirelessly to the device). Further programs, i.e. after entering the service mode, will be done analogously to the standby mode. You will need to enter the number of the box to which the employee X will want to put in the documents, the customer code and a random one-time code. From the point of view of security, it should be noted that the client code will be sent once, along with signing the contract with the customer and will never be forwarded via e-mail. On the other hand, one-off codes will be transmitted to the medium selected by the client (by e-mail or by phone) each time after expressing the desire to receive the documentation.

Important elements from the point of view of safety are:

- no touch screen in the device;
- only a numeric PC keyboard available to customers.

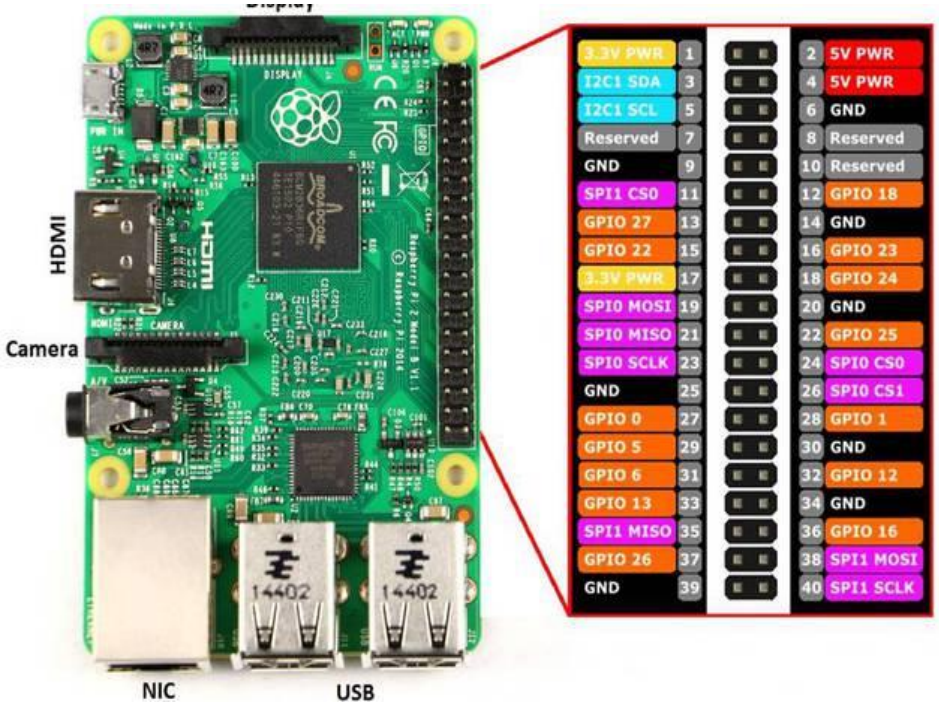

Fig. 2. Raspberry Pi GPIOs description,

Fig. 3. Solid State Relays 8-channel Module

The above elements significantly increase the level of security, because any possibility of deliberately or accidentally entering a service code or programming code, which is always

alphanumeric, is eliminated. In addition, there is no need for the client to have access to such keys as TAB, ALT, CTRL or SHIFT, which keys are absolutely necessary when conducting a hacker attack or regarding the information overload attack on the system [17].

In addition, in order to eliminate the risk of hacking the device by remote means, eg using network tools, it was decided to disable the wifi and bluetooth modules.

From the point of view of the logic of the machine, the application of the correct sequence of codes gives the generation of a signal to open the appropriate box. This Raspberry signal can be generated on a specific GPIO pin (connector) (see Figures 2 and 3).

Information from this pin (connector) is directed to the next module, which will be Solid State Relay - a set of static (semiconductor) relays, working as a function of the controller of electric locks, executing the commands of the main controller.

5. CONCLUSIONS

Conducted SWOT analysis led to the conclusion that it is strategically reasonable to perform the project of development the machine to issue the documents in automatic way – the documentomat. Additional technical analysis were presented in order to describe the more specific way of obtaining high security level for the operations of the machine.

References

[1] Earl, Michael. Knowledge management strategies: Toward a taxonomy. *Journal of management information systems* 18.1 (2001) 215-233

[2] Anand, Vikas, Charles C. Manz, and William H. Glick. An organizational memory approach to information management. *Academy of management review* 23.4 (1998) 796-809

[3] Schwenk, Charles H. Information, cognitive biases, and commitment to a course of action. *Academy of Management Review* 11.2 (1986) 298-310

[4] Buhalis, Dimitrios, and Rob Law. Progress in information technology and tourism management: 20 years on and 10 years after the Internet - The state of eTourism research. *Tourism management* 29.4 (2008) 609-623

[5] Benbya, Hind, Giuseppina Passiante, and Nassim Aissa Belbaly. Corporate portal: a tool for knowledge management synchronization. *International Journal of Information Management* 24.3 (2004): 201-220

[6] Wang, Richard Y. et al. Manage your information as a product. *MIT Sloan Management Review* 39.4 (1998) 95

[7] Hersey, Paul, and Kenneth H. Blanchard. Management of organizational behavior: Utilizing human resources. (1969) 526-526

[8] Tushman, Michael L. and David A. Nadler. Information processing as an integrating concept in organizational design. *Academy of management review* 3.3 (1978) 613-624

[9] Van Der Aalst, Wil MP, Arthur HM Ter Hofstede, and Mathias Weske. Business process management: A survey. *International conference on business process management*. Springer, Berlin, Heidelberg, 2003.

[10] Daugherty, Patricia J., et al. Reverse logistics: superior performance through focused resource commitments to information technology. *Transportation Research Part E: Logistics and Transportation Review* 41.2 (2005) 77-92

[11] Miller, Vernon D. and Fredric M. Jablin. Information seeking during organizational entry: Influences, tactics, and a model of the process. *Academy of Management Review* 16.1 (1991) 92-120

[12] Brereton, Pearl, et al. Lessons from applying the systematic literature review process within the software engineering domain. *Journal of systems and software* 80.4 (2007) 571-583

[13] Georgakopoulos, Diimitrios, Mark Hornick, and Amit Sheth. An overview of workflow management: From process modeling to workflow automation infrastructure. *Distributed and parallel Databases* 3.2 (1995): 119-153

[14] Wright, Patrick M., and Scott A. Snell. Toward a unifying framework for exploring fit and flexibility in strategic human resource management. *Academy of management review* 23.4 (1998) 756-772

[15] Alavi, Maryam, and Dorothy E. Leidner. Knowledge management systems: issues, challenges, and benefits. *Communications of the AIS* 1.2es (1999) 1

[16] Hicks, Ben J. Lean information management: Understanding and eliminating waste." *International journal of information management* 27.4 (2007) 233-249

[17] Edmunds, Angela, and Anne Morris. The problem of information overload in business organisations: a review of the literature. *International journal of information management* 20.1 (2000) 17-28

[18] Teo, Thompson SH, and Bee Lian Too. Information systems orientation and business use of the Internet: An empirical study. *International Journal of Electronic Commerce* 4.4 (2000) 105-130