Influence of IT on Accounting Practice and Exposure to Cyber Attacks

Marija Boban
University of Split
Faculty of Law
Split, Croatia
marija.boban@pravst.hr

Valentina Vinšalek Stipić
Polytechnic "Marko Marulić" Knin
Knin, Croatia
valentinavinsalek@net.hr

Josipa Grabić
Geoprodukt d.o.o. Split
Split, Croatia
geoprodukt1@gmail.com

***Abstract*—The accelerated development of information technology requires additional investment in education and training for advanced technologies. In the unfavorable position there were numerous other occupations that were not technical or informational. Hence, many years ago, there are many obstacles to accounting practice for tracking technology advancement. Many accountants skilled in their work can not cope with the fast-paced IT developments and cybercrime exposure. There are a large number of accounting information systems that are of different quality to accountants. The market for accounting information systems has progressed significantly, enabling a business organization to meet legal obligations faster. However, the rapid progress of IT technology does not keep pace with the rapid progress of accounting personnel, leading to greater risk for cyber attacks. This research aims to confirm a greater exposure to cyber attacks in cases where management structures are not convinced of the rapid advances in IT technology that the accounting profession can not track. Business management's possible savings do not engage IT professionals, ultimately leading to greater exposure to cyber attacks and causing large financial losses.**

Keywords—accounting information system; accounting practice; cyber attacks,; information technologies.

I. INTRODUCTION

Today, the business world is rapidly changing, and this extremely turbulent business environment drives business organizations to re-examine business decisions and adjust business risks to which they are exposed, including increased exposure to cyber threats and hacker attacks. The rapid pace of change in information technology requires greater investment and additional employment in R & D, leading to higher business expenditures as a result of globalization [1]. Business management responds differently to a wide range of IT technologies of different quality. The relationship between IT technology and accounting practice needs to be complemented with quality to make the company competitive on the global market. The decision to establish an IT structure must be related to business strategy decisions that are consistent with the accounting department of the company [2]. IT basically changes the nature of accounting operations. The advantage of using information technology in accounting is unquestionable, but management of companies must be aware of the rapid advancement of IT technology compared to the accounting profession. If the accounting profession is unable to track IT, the assumption is the possibility of more frequent hacking attacks on the company's financial and accounting system. In practice, the problem arises in the fact that the IT profession does not carry out accounting activities in the company or accountants are experts in information technology. So it comes to the assumption that the necessity of IT professionals in the enterprise is necessary for the purpose of protecting accountancy from possible hacker attacks. The management of a company must be aware that accountants are not experts in preventing hacking attacks and are unable to cope with such a crime. Therefore, the purpose of this paper is to determine the frequency of hacker attacks on the accounting system of an enterprise depending on the size of the enterprise, the type of accounting information system and the age structure of employees in accounting.

II. ACCOUNTING INFORMATION SYSTEM

The basic purpose and task of accounting firm of an enterprise and accounting information system is to provide timely and accurate information required by regulatory bodies, and management and management of companies at all levels. Accounting information from an accounting information system (AIS here and after) helps managers at all levels in the enterprise to manage business processes to achieve company goals. Data from the accounting information system helps management in all stages of decision-making and problem solving: problem identification, alternative solution identification, alternative solution assessment, and ultimately decision-making for problem solving [3]. Here is a clear fact that without a good accounting information system management company it is not possible to make good quality and correct decisions. It is indisputable that hacking attacks in key moments for making business decisions increase business risk and cause losses.

The goals of AIS differ depending on characteristics of organization which implements them. When speaking of companies, efficient usage of information through AIS can have various goals. However, in the end, entire set of goals converge to the fundamental goal every company has – profit

maximization for the owners. One of the most important functions of AIS is to support decision-making at all organizational levels within a local government unit. In addition to the function of providing periodical information to the external users through formalized financial statements, AIS also has function of providing relevant information at all organizational levels within an organization, especially to the highest management levels in process of decision-making. AIS handles both financial and non -financial transactions that directly affect the processing of financial transactions. Besides traditional financial information (the amount of cash available, cost structure etc.), non-financial information is also needed for the more efficient decision-making process because certain information that can be very significant aren't contained in financial statements and attention should be paid to them. When changes are made to customers' data, for instance change in next of kin and/or address, these changes provide vital information for processing of future data to such users/customers. [4]

Accounting records the financial transactions and the effects of these transactions. Accounting also distributes transaction information to operating personnel to perform day-to-day key tasks. In addition to employee, administration and management, the business of an enterprise through an accounting information system is significant for customers, suppliers, financial institutions and other regulatory bodies. Each of the business process participants (which take place in the enterprise or from the company) has certain areas of interest in the business of the enterprise and all use the information obtained from the accounting information system of the enterprise. The company's accounting information system records and manages business information for internal and external stakeholders. Therefore, all business participants (both internal and external) require full business relationship security. However, in frequent hackers attacks, business confidence is lost in management and only in the enterprise. Business confidence builds long but is easily lost. If business partners feel insecure in the business environment, there is a great possibility of withdrawal and business relationship in order to preserve their own identity and security.

A. Types of Accounting Computing Systems

A modern accounting information system is a combination of a standard accounting system and a management information system to track and track financial and non-financial information. Financial accounting information for the use of external users is defined by regulations and guidelines in order to avoid ambiguity.

The accounting information system includes three main subsystems: [5]

• a transaction processing system that supports business operations on a daily basis with numerous documents and messages for users throughout the organization;

• a financial reporting system that reports traditional financial statements, such as an income statement, balance sheet, statement of cash flows, tax returns and other reports prescribed by law;

• business Reporting Management System that enables internal management of financial statements of special purpose and information for the purposes of planning and making business decisions.

There are usually two ways to build an accounting and information system in a company:

• develop from the beginning customized systems of development activities within the enterprise or

• purchase pre-programmed commercial systems from software vendors.

In most cases large companies prefer independent self-development of accounting information system due to the complexity of programs and business activities. Smaller companies and companies with standardized information needs are primarily commercial software. [6]

B. Role of the Accountant in AIS

The common fact of all accounting computing systems consists of the basic structure of the system where the company builds its business excellence. The primary data processing in the accounting program is the logic pre-programmed, and the program provider then designs the user interfaces according to the individual needs of the client. The backbone system is a compromise between a custom system and a standard system. This approach can produce very satisfactory results, but customization of the system is expensive.

Systems supported by vendors are tailored to the systems that customer organizations purchase commercially and do not develop them independently in their own businesses. Under this approach, the software vendor designs, implements and maintains a system for its customers. This is a popular choice in health and social care organizations and small business organizations, while commercial enterprises (primarily large) have their own staff to develop and track accounting systems within the enterprise. In both cases, the key is the fact that it is protecting the accounting information systems from hacking attacks.

The accountants are legally responsible for the management, operation and control of the accounting information system in the company. Accountants should have a major role in choosing AIS as users and system auditors. When choosing the appropriate AIS, ethical and legal requirements must be taken into account. Due to the significance of information available to AIS, each company should pay particular attention to AIS protection in accordance with appropriate internal control procedures and security measures. Especially from hacking attacks and the theft of personal and financial data contained in the accounting information system. However, big problems arise when the management of the company is unaware of the dangers of the exposure of the accounting system to hacker attacks. Due to possible savings in operating costs, IT professionals are not hired to protect the accounting information system from hacking attacks. Then the accountants are left alone and they have to know the computer language despite being not an IT professional. Despite the expertise in his work, he faces a host of obstacles and computer threats, and then the accountants are not able to carry out daily tasks independently.

C. Internal control of Accounting Computing System

Internal control implies procedures „performed by management, executives and employees to ensure the provision of moderate guarantees with regard to the achievement of objectives that can be grouped in the following categories:

- Efficiency and effectiveness of business,
- Reliability of financial statements,
- Compliance with applicable laws and other regulations“ [7]

Control procedures imply methods for „recognition, prevention and elimination of irregularities that impede the fulfilment of the objectives of the enterprise”, and the classification is as follows: [7]

- Preventive controls – they have the function of preventing irregularities,
- Detective controls – they are carried out with the purpose of analyzing deviations,
- Corrective controls – they are conducted after the irregularity has already emerged, with the aim of its removal and improving system functioning.

Control procedures are useful in all phases of accounting process: [8]

- Input – preventive control application when entering data,
- Processing – the control of the data and compliance with the relevant regulations,
- Output – checking the information through financial reporting.

III. Connection of IT and Accounting System

The biggest impact IT has made on accounting is the ability of companies to develop and use computerized systems for tracking and recording financial transactions. Computer networks and computer systems shortened the time the accountants needed to prepare and present financial information. Companies have been given quicker and easier creation of management reporting reports. Other features of computer accounting systems include: increased functionality, improved accuracy, faster processing, and better external reporting. Accounting is a system that companies use to measure financial performance by recognizing and classifying all transactions in sales, purchases, assets and liabilities in a manner that complies with certain accepted standards. Computers, servers, the Internet, wireless and personal digital devices have forever transformed the way they do business in enterprises. Program packages have also improved traditional operations and production processes. Accounting has undergone tremendous advances thanks to the growth of information technology. The accounting informatics program automates traditional bookkeeping and accounting books. Businesses usually choose accounting programs based on the size of their business and the number of users accessing the system. Large companies can choose software packages from the system. Information technology has created significant benefits for accounting departments [9]. IT networks and computer systems have shortened the time needed for accountants to prepare and present financial information to the manager and stakeholders. Not only did IT shorten the time it took to display financial information, but also improved overall efficiency and accuracy of information.

IV. Hacker Attacks Unknown to Accounting Profession

Accidents such as hacker attacks on the accounting information system can cause huge damage to operations and business customers. Businesses, accountants, IT and regulators agree that these incidents may also endanger the stability of the financial system. Hacker attacks are deliberate efforts to hinder, steal or destroy data stored in the accounting information system. Tactics of hackers include finding weaknesses in the software to enter the computer system itself, or a computer network, pointing to e-mail accounts to steal passwords, directing websites to infect users with malicious software and software that erase users from their own systems [10]. The Internet provides several ways for attackers to enter an enterprises internal computer network. Detailed information on incidence, tactics and results of hacker attacks and incidents is weak. Data is scarce partly because financial companies and business organizations avoid reporting incidents due to concerns about reputation. Evidence of growing concern about hacker attacks is seen in industry surveys, service provider reports, regulatory submissions, and responses to major incidents [11]. Attacks are often motivated by gain. Criminals can sell stolen credit card information and buy software and other black market tools to trigger new infiltrations. Hackers may also have other goals, including goals related to foreign policy or espionage. Threats and hacker attacks impose direct costs on companies. These costs include loss of funds or customer records, additional expense on IT technology and software protection, reimbursement costs, cost of reputations and legal costs. These incidents may also pose a wider risk to financial stability. Most companies work in complex networks and rely on electronic transactions because of the speed of financial data transfer. However, all of the above is mostly unknown to accountants who work directly in accounting information systems. Hence, exposure to hacker attacks is extremely high and the risk to the business system is significant. Although skilled at work, accountants who completed their education in the twenties of the last century and have not been further upgraded and educated for advanced technologies fall into extremely risky groups and as an excellent basis for hacking attacks. Therefore, the management and management of companies must be aware of the risk exposure to hacking attacks and the risk of theft of business and personal data stored in enterprise accounting systems. It is important that financial accounting experts are

not computing and IT professionals need to be hired to protect themselves against hacker attacks and prevent them from operating on the accounting information system.

V. Literature of Previous Research

The role of new IT technologies in accounting systems is very clear. An integrated system such as the planning system as well as the increasing use of the Internet in carrying out accounting operations is striving to keep pace with the progress of IT technology progress. Although IT has an important role in the field of accounting, little research has been carried out on the relationship between them. Based on the literature review of previous research and studies, it was concluded that little is known about the effectiveness of advancing the latest world technology in the field of accounting and exposure of accounting information systems to hacking attacks. Although IT apparently plays an important role in accounting and control and control [12], this relationship is not sufficiently studied. Current research focuses on the relationship between investment in IT and enterprise performance [13]. Several discoveries were made on the basis of a study [14]:

• There is a significant relationship between information technology and accounting systems.
• There is a significant relationship between challenges and the use of information technology.
• There is a significant relationship between information technology and organizational performance.

Specifically, such studies have attempted to measure the amount of investment in IT and enterprise productivity [15] or even materialized IT investment [16].

The aim of this paper is to focus on the efficiency of IT technology in order to improve and secure the operating conditions of accounting information systems, to reduce hacker attacks on local corporate IT networks and data theft from accounting systems. It tries to wake the awareness of the company's administration about the importance of IT and employment of IT professionals in order to better protect the local networks and accounting information systems of the enterprise, rather than relying on informational jobs for which they are not trained.

VI. Goals and Hypotheses of the Research

The aforementioned topics emphasized the importance of IT technology and its benefits for accounting information systems. This research has highlighted the importance of IT technology to improve company performance. Due to the increasing exposure to hacking attacks, this paper focused on highlighting the importance of IT in protecting accounting information systems from hackers since accounting officers responsible for the neat and secure operation of accounting systems are not trained to fight hackers and hackers. Therefore, this paper seeks to investigate the correlation between the frequency of hacker attacks in relation to the size of the enterprise, the type of accounting information system and the age structure of employee accounting employees in the enterprise.

The following hypotheses form the basis of this research:

H1 = There is a statistical significance of linking hacking attacks to enterprise size

H2 = There is a statistical significance of hacking attacks being associated with the type of accounting information system

H3 = There is statistically significant correlation between hacking attacks with the age structure of employees in the accounting department.

VII. Method of the Research

The research described in this paper is based on empirical testing on a sample of 56 business organizations (in the Sibenik, Croatia) of the private and public sector. The information for this research was obtained from the surveys conducted on the company's sample. Finally, the answers to the questions were rated 1 to 3 for each individual company and for each individually observed dependent variables. The research carried out was to demonstrate the correlation of the frequency of cyber attacks on the accounting information system due to the size of the enterprise, the quality of the accounting program and the age structure of employees in the accounting department, and an analysis by correlation and regression in the statistical program SPSS Statistics 17.0., And the obtained results are shown in the tables below.

The following variables have been defined in this research:

a) Predictors (Constatnt) VAR X – Frequency of cyber attacks => this feature is determined by the following responses offered:

1. There were no cyber attacks in a year
2. One to two times a year
3. Three and several times

b) Dependent Variable:

- VAR Y1 – enterprise size => this feature is determined by the following offered responses:
  1.Small Enterprises
  2.Medium Enterprises
  3.Large Enterprises
- VAR Y2 – type of accounting program => this feature is determined by the following offered responses:
  1.A self-developed accounting program
  2.Purchased program developed abroad
  3.Purchased program developed in Croatia
- VAR Y3 – age structure of accounting employees => this characteristic is determined by the following responses offered:
  1.Average age of employees from 18 to 35
  2.Average age of employees from 36 to 50
  3.Average age of employees from 51 to 65

The next part of the paper presents the results of research and data processing.

VIII. Results of the Research

Table I. presents the results of the statistical significance of the coefficient of correlation and regression of the frequency of cyber attacks (VAR X) and enterprise size (VAR Y1).

TABLE I. Statistical View of the Correlation and Regression Cyber Attacks with Enterprises Size

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	,575[a]	,330	,318	,762	,330	26,622	1	54	,000	2,176

a. Predictors: (Constant), VAR_X

b. Dependent Variable: VAR_Y1

In Table I. the correlation coefficient (0.575) shows the correlation between the frequency of cyber attacks and the size of the enterprise. When we look at the F ratio, we see that the empirical F ratio is considerably higher than the theoretical value, which is consistent with the fact that the samples (surveyed companies) are not from the same population but from different activities, so the variability among the groups is significantly higher than that within the group, there is variation that is the result of the treatment effect, which results in differences between the groups. The F ratio is greater than 1. However, with a given level of significance of 0.05 and with the number of degrees of freedom (1.54), while Durbin-Watson has a value of about 2 that tells about the existence of no correlation error autocorrelation. We can talk about how statistical connectivity exists, meaning that hacker attacks are more common in larger companies.

In the Table II. presents the results of the statistical significance of the coefficient of correlation and regression of the frequency of cyber attacks (VAR X) and type of accounting program (VAR Y2).

TABLE II. Statistical View of the Correlation and Regression Cyber Attacks with Type of Accounting Program

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	,431[a]	,185	,170	,366	,185	12,288	1	54	,001	2,002

a. Predictors: (Constant), VAR_X

b. Dependent Variable: VAR_Y2

From the coefficient of correlation R in Table II. we can see that there is a link between variables, the determination coefficient R2 is closer to zero than the unit, so we can not speak of a good linearity of the model. F ratio is higher than the theoretical value because the samples are not of the same economic activity, according to a given level of significance of 0.05 and the number of degrees of freedom (1.54), we come to the conclusion that the frequency of cyber attacks is partially but not significantly related to the type of accounting program. Durbin-Watson has a value of 2 indicating that there is no auto correlation of relationship.

Table III. presents the results of the statistical significance of the coefficient of correlation and regression of the frequency of cyber attacks (VAR X) and age structure of accounting employees (VAR Y3).

TABLE III. Statistical View of the Correlation and Regression Cyber Attacks with Age Accounting Employees

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	,301[a]	,090	,074	,597	,090	5,367	1	54	,024	2,051

a. Predictors: (Constant), VAR_X

b. Dependent Variable: VAR_Y3

In Table III. from the coefficient of correlation R we can see that the correlation between the variables exists and is important. F ratio is higher than the theoretical value because the samples are not of the same economic activity, on the basis of that, with a given level of significance of 0.05 and the number of degrees of freedom (1.54) we come to the conclusion that the incidence of cyber attacks and the greater exposure of companies is quite related to the age structure of accounting employees in company. Accounting employees who are no longer trained or trained hardly carry the fast-paced IT technology and hacking threats.

IX. Conclusion

Accounting information systems basically IT changes and improves. The advantage of using information technology in accounting is unquestionable, but management of companies must be aware of the rapid advancement of IT technology compared to the accounting profession. If the accounting profession is unable to track IT, there is a possibility of more hacking attacks on the company's financial and accounting system. Our research has led to the following results that there is a cyber attack connection with enterprise size and partial correlation with the type of accounting information systems that companies are using. However, it is indisputable that accounting officers enter data and manage accounting programs, and this research has shown that there is an undesirable connectivity (0.601) between cyber attacks and the age structure of employees, which has a causal effect on the first two hypotheses of this research. It is important to note that accountants are not IT professionals and because accounting legislation is constantly changing, accountants can not overlook IT technology progress. Therefore, Business management must be aware of the importance of IT profession in business organizations of any size.

References

[1] S. Amiri and N. Amiri, "Information Technology (IT) and its Role in Accounting Practice", International Journal of Economy, Management and Social Sciences, 3(1) January 2014, pp. 28-32.

[2] J. Efending, E. Muling and L. Smith, "Information technology and systems research published in major accounting academic and professional journals", Journal of emerging technologies in accounting, 2006.

[3] V. Roska and J. Bubic, "Accounting Information Systems for Management Decisions: Empirical research in Croatia", Business & Economics Society International Conference , 2008.

[4] Muhrtala, T. O., Ogundej, M., Computerized Accounting Information Systems and Perceived Security Threats in Developing Economies: The

Nigerian Case, Universal Journal of Accounting and Finance 1(1): 9 - 18, 2013.

[5] A.J. Hall, "Accounting Information Systems", South – Western Collage Publishing, 2008.

[6] Boban, M., Šušak, T., Accounting information systems and their use in regional and local governments sector: Quality, efficiency, security and control procedures as (present) challenges // 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija: IEEE, 2015. pp 1546-1551

[7] Mamić Sačer, I., Žager, K. „Računovodstveni informacijski sustavi, Rif, Zagreb, 2007.

[8] Ramljak, B., Interne računovodstvene kontrole u javnom sektoru, 15. Savjetovanje Interna kontrola i revizija, Zagreb, Hrvatska zajednica računovođa i financijskih djelatika, 2012., pp 141. – 153

[9] M. Ghasemi, V. Shafeiepour, M. aslani, and E. Barvayeh, "The impact of Information Technology (IT) on modern accounting", Procedia - Social and Behavioral Sciences (28) 2011, pp. 112-116.

[10] Office of Financial Research - Viewpoint, "Cyber security and Financial Stability: Risk and Resilience", 17-01, February 15, 2017., pp. 01-12.

[11] Symantec Corp., "Internet Security Threat Report", Herndon, Volume 21, April, 2016, Page 7.

[12] N. Dechow, M. Granlund and J. Mauristen, "Management control of the complex organization: relationship between management accounting and information technology", Handbook of management accounting research, Elsevier, 2007.

[13] N. Melville, K. Kraemer and V. Review, "Information technology and organizational performance: an integrative method ot IT business value", MIS Quartly, 2004.

[14] J.N. Taiwo and M.E. Agwu, " Effect of ICT on Accounting information System and Organizational Performance", European Journal of Business and Social Sciences, Vol. 5, No. 02, May 2016., pp. 01-15.

[15] J.K. Dedrick, V. Gurbaxani and K. Kraemer, "Information technology and economic performance: a critical review of the empirical evidence", ACM Community Management, 2003., page 34.

[16] B. Dehning and V. Richardson, "Return on investments in information technology: A research synthesis", Journal of information systems, 2002, page 16.