Audit financiar, XVI, Nr. 1(149)/**2018**, *131-139*
ISSN: 1583-5812; ISSN on-line: 1844-8801

Information security challenges - vulnerabilities brought by ERP applications and cloud platforms

Sînziana-Maria RÎNDAŞU,
Bucharest University of Economic Studies,
E-mail: sinziana_rindasu@yahoo.com

Abstract

The accounting profession is in a continuous process of change as ERP applications and emerging technologies such as cloud computing continue to bring improvements into the accounting and financial areas. Nevertheless, beside the variety of benefits, these technologies carry specific risks that can affect the fundamental characteristics and security aspects of data.

This paper aims to highlight the most common vulnerabilities of ERP applications and cloud computing platforms in the context of digital accounting. At the same time, in addition to the technical aspects and good practices used to prevent and correct these vulnerabilities, the study focuses on a critical component of data security: the human factor. Moreover, the empirical research conducted has highlighted the fact that young professionals understand the need for sensitive data protection, but they do not always display the best behavior to prevent security incidents.

This article aims to provide an overview of ERP applications and cloud computing platforms that are currently used in the financial and accounting field, focusing on the main technical vulnerabilities and the human factor, which is one of the most important aspects of data security.

***Keywords**: information security, ERP, cloud computing, human factor*

***JEL Classification:** M15, M41, M42*

To cite this article:
Rîndaşu, S.M. (2018), Information security challenges – vulnerabilities brought by ERP applications and cloud platforms, *Audit Financiar*, vol. XVI, no. 1(149)/2018, pp. 131-139, DOI: 10.20869/AUDITF/2018/149/005

To link to this article:
http://dx.doi.org/10.20869/AUDITF/2018/149/005
Received: 27.06.2017
Revised: 02.08.2017
Accepted: 08.11.2017

Introduction

The constant evolution of IT has contributed to the development of most industries and professions by automating and digitalizing certain elementary activities, to enable professionals to focus more on complex activities that add value to companies. Digitalized and automated processes are not intended to replace the human resource, but rather to support the progress of professionals.

Information is the essence of any organization or individual, as it is what creates a competitive advantage. Ronald Reagan stated that it is "the oxygen of the modern age." In the financial and accounting field, almost everything is limited to information (ACCA, 2013) and in this current digital era, information has become one of the vital resources in the process of value creation. Protecting sensitive data, whether we refer to data stored on a physical or electronic basis, by implementing an effective IT security incident management system, must be an essential concern for any organization, regardless of its size or field of activity. Accidental or deliberate disclosure of confidential information can irremediably damage the companies' operations, by affecting its financial situations and reputation.

Currently, security incidents are one of the most significant concerns in the Internet of Everything era, as technological developments have introduced new concepts in the financial and accounting field such as ERP, cloud computing and mobile technologies that, besides the variety of advantages, carry specific vulnerabilities that can affect the security of sensitive information. In recent years, there has been an increase in security incidents, at both national and global level. According to the latest CERT report, over 110 million cyber security alerts were recorded in Romania in 2016, the increase being more than 60%, compared with the previous year. At international level, according to Breach Level Index, more than 1.3 billion IT security incidents occurred, increasing by over 85%, compared to 2015.

In the accounting field, most of the activities have been digitalized due to the need to have continuous access to relevant information in real time. Whether we are talking about mobile technologies, ERP systems or cloud computing platforms, almost all sensitive information has moved into the electronic environment.

This paper aims to analyze the main challenges of information security in the context of digital accounting and to assess which are the vulnerabilities of the technologies currently used. Moreover, this study investigates the perception and awareness of the impact of security incidents from the perspective of future professional accountants.

1. Literature review – ERP applications and cloud platforms vulnerabilities

The development of ERP (Enterprise Resource Planning) systems had as a starting point the need to automate the core data processing and data input activities, which did not require an increased level of professional judgment. Although the digitalization and automation of certain processes such as inventory and production management began in the 1950s, it was only in the early 1990s that we could identify the first ERP system (Møller, 2005) that incorporated various modules: accounting, human resources, project management and distribution. Currently, the existing applications include the same essential functions, but they are configured according to the needs of each organization. Most recent applications include also financial planning modules, supply chain management and customer relationship management (CRM).

According to the relevant research conducted in this field, the impact of ERP systems was positive, as these applications were built on the idea of aggregating most of the key processes in a company into a single IT system (Klaus, 2000) by using a shared database to eliminate redundant processes (Davenport, 1998). In the financial and accounting fields the main advantages are the following: cost reduction, elimination or automation of simple processes, increased quality of the financial reporting, improved flexibility and competitiveness (Kanellou and Spathis, 2013; Stanciu and Tinca, 2013; Ponorica et al. 2014; Voulgaris et al., 2014).

Lately, ERP systems have begun to adapt to the current needs of the users. Therefore, we can discuss the use of ERP applications in cloud computing platforms, which allow data to be accessed also from mobile devices. It can be observed that the general trend of migrating to cloud to benefit from continuous access to data, without taking into account technological or geographic barriers.

ERP applications are a target of cyber-attacks because they store confidential information, such as organizational secrets, financial data, data about the organizations' customers and suppliers. Nevertheless, ERPs are also targeted to commit various acts of fraud, such as master data modification.

To analyze the vulnerabilities of ERP applications, regarding data stored by systems, we need to understand the architecture and functionalities of ERP applications. Most ERPs share the three levels structure, starting with the base of any ERP: a database where the information is stored and most applications use Microsoft or Oracle databases that use SQL query language. The next component is the application layer where are the implementation, logic and system rules. The last level of ERPs is the user interface (Surjit et al., 2016; Bahssas, 2015). At the same time, besides the simplified architecture of an ERP application, the environment in which this application is implemented is also important: locally or on a cloud computing platform.

Taking into consideration the structure presented, the first vulnerability of an ERP system is due to the existence of the databases used. At the database level there may be inconsistencies that can endanger the fundamental characteristics of the data: privacy, integrity and availability, if the database has not been properly implemented (Bertino, 2005; Swart et al., 2007).

Among the potential vulnerabilities, there are excessive or unauthorized privileges, operating system vulnerabilities, SQL injection, malware, inappropriate passwords or incorrect implementation of the database (Ali and Afzal, 2017; Malik and Patel, 2016; Lodha and Dhande, 2014). All of these vulnerabilities occur both in local ERP applications and cloud platforms. Comparing the level of security between local ERP and cloud ERP, we cannot say that security will be improved or not, because it all depends on the implementation mode and the controls created.

Analyzing the next level of ERP applications, the logic level, as in the case of the database behind the ERP application, if the deployment was not correctly performed, the issue of data security occurs through brute force or SQL injection attacks. At this level, most of the issues arise because of the poor implementation of the database security measures.

ERP users also represent a vulnerability for sensitive data (Evans et al., 2016) because organizations do not always create a culture that is efficient enough to make them aware of the possible theft or exposure of confidential information. The human factor is one of the most important components of data security, whether or not we are talking about an ERP application. It is essential that organizations instruct their employees about the impact of security incidents.

In 2014, some of Sony Pictures Entertainment directors received an email, apparently from Apple, for an email verification. The email they received was a phishing that allowed the attackers to get the password from their Apple accounts, being used to authenticate to the Sony network and stole confidential financial information and Sony service passwords, which were later posted on the Internet. According to the company statements, IT system recovery cost 35 million dollars. This incident is a classic example demonstrating that the human factor is still one of the most important vulnerabilities. At the same time, the fact that the executives who were attacked had the same passwords for corporate and personal accounts indicate that there was not a well-developed culture of risk prevention associated with unauthorized exposure of sensitive data.

As it can be seen from the example presented above, the prevention of loss of sensitive information is essential, especially for ERP systems, which, according to statistics, are used by over 83% of Forbes 500 companies. To prevent security incidents, the risks must be first identified and the potential impact assessed.

Given the fact that each company has its particularities, each ERP application will have differences, depending on the needs of the specific organizations and activities. Therefore, we cannot propose a universal ERP security model, but we can only highlight the best practices that can prevent security incidents.

As previous mentioned, one of the main security concerns is the excessive privileges granted to application users (Horwath, 2012). Database administrators allocate differentiated rights to users, either by using the existing roles in the application or by creating new roles that suit the needs of users in the application (Bruchez, 2012). These customized rules could prevent unauthorized access to data, but only if properly implemented.

Incorrect configuration of the database is also a significant vulnerability. By storing access passwords in the ERP application database, without encrypting data,

gives potential attackers the ability to obtain the users credentials. In the case of SQL Server databases, the user authentication data can be stored encrypted in another database, not even visible to the database administrator. Also, an implementation that does not take account of the vulnerabilities of such application may allow attackers to steal data using SQL injection (Gicev et al., 2013; Bhatia, 2017), which are still one of the most significant databases weaknesses.

Malware infections increase the risk of losing sensitive information. In the last period, it can be observed that more and more types of viruses are created and can remain undetected or their impact is observed only after a significant period. More recently, we can see applications like ransomware whose purpose is to encrypt all user data, and decryption will only be done after the attackers are paid for the information. Programs that can prevent such incidents are currently being developed (Kolodenke et al., 2017), but the progression of malware is more fierce than the development of prevention programs.

Most databases incorporate database audit modules that can prevent confidential information from being exposed, if effective controls that target the applications risk areas are implemented. Database auditing has the role of prevention in determining vulnerabilities, but also a function of detection. For databases, the most efficient audit controls are:

- Analysis of back-up or database restoration activities - to determine which users have performed such activities. As described above, one of the biggest vulnerabilities in an ERP application is the excessive privileges granted to users and if the results of the control indicate that such activities were performed by individuals who should not have the rights to perform these tasks, this must be an alarm signal for the organization.
- Analyzing the actions conducted on the database or its objects - as with the previous control, this control has the role of monitoring and detecting illegal activities. However, given that in an ERP application there are many users that make changes to the database, the amount of information is too vast to be analyzed manually. In this case, it is recommended to use data mining techniques to identify possible inconsistencies.
- System logging analysis - this control is important because it monitors both user access to the application, but also checks unsuccessful login activities. This control can prevent a brute-force attack, but also highlights logins into the system by former employees of the organization, whose credentials have not yet been annulled.

ERP systems are vital components of any organization because they incorporate the companies' most important processes and therefore the proper implementation, in line with good practices, is necessary to prevent potential security incidents. Due to the complexity of ERP systems, we cannot talk about a common security framework that meets the needs of all companies. Therefore the most efficient way to protect sensitive data in ERP applications is to identify risks by using best practices correctly.

The current economic context has created the need for continuous access to information. This new necessity, in the financial field, is what it is called real-time reporting, a process that creates a competitive advantage for organizations (ACCA, 2013b), by improving the agility and transparency of activities. To meet the need of users and businesses, most accounting and financial processes have migrated to cloud computing platforms (Trigo et al., 2014). In this way, the users of a particular application can view or manipulate data regardless of location or devices used as long as they have an Internet connection.

As in the case of ERP applications, to understand the main security vulnerabilities of data stored in cloud computing platforms, we need to have a clear picture of the functionality and architecture of the platforms.

The concept of cloud computing was based on the idea of unlimited access to technology (hardware) to information, according to Giordanelli and Mastroianni (2010). Currently, the cloud computing concept is represented by server networks and data warehouses (Kim, 2013), whose purpose is to provide a broad range of web services (storing and manipulating data, performing queries on the database, etc.).

By analyzing the delivery model, three types of platforms can be differentiated: IaaS - Infrastructure as a Service, PaaS – Platform as a Service and SaaS - Software as a service, according to NIST standard 800-145.

A second classification can be done by following the implementation model used: public, private, community or hybrid. From a security point of view, the lowest level of security is found in the public model, followed by the community, hybrid and private model.

IaaS incorporates all the functions of a cloud, as users have the right to modify the functionalities and security aspects of applications. At the same time, this type of platform allows organizations to have the highest level of IT infrastructure control compared with the other two platform models. Due to these considerations, in the case of IaaS, the security of operating systems and applications rests with the organization, while the cloud provider is only responsible for the safety of the network and servers.

According to the Symantec study from 2015, the most common vulnerabilities in IaaS are the following: loss or disclosure of confidential information, unauthorized access - mostly due to theft of user credentials and inadequate security configurations. However, in the case of IaaS, security issues may also occur due to other cloud users (tenants) when the server is not dedicated - multi-tenancy issues.

To prevent security incidents for this type of platform, it is essential to choose the appropriate model (public, private, community or hybrid) to match the organizations' objectives and to ensure that implementation is properly done, by respecting the best data security practices. Moreover, systems monitoring and auditing are vital processes for preventing cyber-attacks or unintended exposure of confidential information. Furthermore, to improve credentials' security, two or more authentication factors are recommended (Jaiswal and Rohankar, 2014).

The PaaS model does not give organizations the same freedom as the IaaS model, because it is designed to allow organizations to deploy applications. In this model, the company that leased the platform cannot make changes to the network, servers or operating systems. In PaaS, the cloud provider is responsible for the database and network security, while the tenant is in charge of the safety of the applications developed on this platform.

From a security point of view, most PaaS platforms provide tools such as integrity checking, data encryption, access management and firewalls (CSCC, 2015). However, at this level vulnerabilities, that may affect the characteristics of the data fundamentals, can be found, if the application development is not done by using the best practices to maintain data security. Also, effective controls must be implemented for this type of platform to prevent potential security incidents.

The third platform model is SaaS, which is the most common type of cloud, because it has the lowest cost compared to the last two models. Most accounting applications, mainly ERP applications, are embedded in this model. In SaaS users can access some applications, but cannot deploy others. Also, within this model, most data security issues are the responsibility of the cloud provider.

Potential vulnerabilities in the SaaS model identified by the relevant literature are: excessive privileges, unauthorized access, inappropriate configuration of applications that may affect the fundamental characteristics of the data and aspects of the security of virtual machines (Hussein and Khalid, 2016; Ahmed et al., 2017; Sharma et al., 2017).

Because this model is more restrictive regarding the client application implementation and since the needs of each organization have specific particularities, most data security controls are the responsibility of the cloud provider, which must offer an acceptable level of assurance for the security of sensitive information. At the same time, given the fact that the cloud platforms store various information that is subject to special treatments regulated by national and international bodies, it is essential to provide for each type of information the appropriate level of security.

In conclusion, cloud platforms have specific vulnerabilities, depending on each model. As with ERP applications, we cannot talk about an absolute security model that would have the ability to prevent any incident, but we need to understand how the data stored in cloud computing platforms can generate risks that might have the potential to cause a security incident.

Because of the wide range of benefits of cloud computing, more and more companies are considering migrating to a cloud platform to improve performance and become more competitive. Given that this technology is emerging, new types of vulnerabilities are expected to develop, mainly due to the increased use of other technologies, along with cloud platforms, such as mobile technologies, which have begun to be increasingly used, in particular in the financial and accounting fields. These issues can contribute to the

development of new risks, but it is important to understand that cloud migration does not automatically mean a lower security level, but in many cases can improve security compared with local applications.

2. Research methodology

In the first part of the paper, the human factor was presented as being an essential component in ensuring data security, as that the accounting field is vulnerable to security incidents because it stores and generates high-confidential information.

Lately, professional bodies have begun an international dissemination of the impact of information security in the accounting field, with the aim of attracting practitioners' attention to the risks associated with handling confidential data, especially when used along with computer applications. At the same time, ACCA reports from 2014 and 2016 draw attention to the need that the professionals in this field have to improve and develop their capabilities to protect sensitive information, especially if data is associated with emerging technologies such as cloud computing, Big Data and mobile technologies. ACCA studies have further demonstrated that over time, at international level, there has been an increase in the level of awareness of the members.

Considering the ACCA reports as a reference point, an empirical research based on a questionnaire was conducted. This survey has been addressed to students of the Master of Accounting, Audit and Management Information Systems program at the Bucharest University of Economic Studies, in the last year of study. This survey aimed to analyze the perception of the participants regarding the security of data in the financial and accounting fields. The purpose of this research was to find out whether future accountants have acquired sufficient knowledge to understand the impact of security incidents and if they have a sufficiently well-developed culture in the field of sensitive data protection.

The survey was sent to 80 potential respondents, 49 of whom decided to participate, the response rate being of 61.25%. The survey contained 16 different enquiries: questions with one or more possible answers, for situations where an in-depth analysis was not required we used response matrix, evaluation scales, but also open questions for subjects requiring a more thorough review.

All students work in the financial and accounting field and have in average two years of experience, the average age of the respondents being 24 years.

3. Findings and discussions

To analyze the level of familiarity of the respondents with information security concepts, they were asked if they had received enough information on data security during their study programs. At this question, only 17 participants considered that the level of information received was sufficient, while 27 people, representing 55.10% of the total sample, assessed that they had received indeed training on the importance of data security, but considered that the level of information received was not sufficient. The remaining 5 participants said they did not receive such information during their study programs.

The variations of the responses can be justified by the fact that the students might have participated in different bachelor programs. However, given the current need to create a well-defined culture for the financial and accounting professionals in the field of sensitive data protection and prevention of security incidents, it is necessary, in our opinion, for universities to introduce courses in the curriculum that focus on this area in order to make it easier for graduates to integrate into the profession and comply with the needs of the organizations.

The next question of the survey was a 5 point Likert scale question and the participants assessed on a scale of 1 to 5 (1 - total disagreement, 5 - complete agreement) the need for professional accountants to be aware of the impact that security incidents can have on the financial information and operational activities. 43 students stated that they fully agree with this assertion and the rest of the participants were partly in agreement with this statement. The answers are consistent with the results presented by ACCA, which indicates that young professionals possess a significant increase level of awareness of the potential impact of security incidents. However, the sharp rise in security alerts at national level, according to the report released by CERT, highlights the lack of sufficiently developed knowledge that might underpins future cyber incidents.

To analyze whether there is a culture of information security implemented in the companies where the students work, they have been asked if they attended

any course on the maintaining and protecting sensitive data. 79.59% of participants responded affirmative to this question, while the rest of the interviewees stated that they did not attend such training programs. This result is a positive factor, but taking into account the fact that currently the academic environment from Romania does not fully cover the necessary curricula in the field of information security, as prior research has shown (Stanciu and Rîndaşu, 2017), the remaining 20% of the companies for which the participants work, must give a greater importance to information security aspects.

Because the actions of the employees can directly affect the security of data, the participants were asked if their work passwords are safe, depending on the minimum complexity required by the system and the shelf life. Although 95.91% of students answered affirmative to this question, 31 of them confirmed that they keep their password written at the work place. Even if the systems used by the companies in which respondents work involves the use of strong passwords, keeping the written passwords at the workplace is a practice that can lead to malicious exposure of sensitive data, as related literature confirms (Evans et al., 2016; Symantec, 2015).

To analyze whether the organizations for which the respondents work have implemented security controls, such as anti-virus programs, only 75.51% of the interviewees responded affirmatively. This outcome raises a question mark over the prioritization of information protection at the organizational level, mostly because malware infections are among the most significant vulnerabilities of ERP applications (Ali and Afzal, 2017).

Another question of the study focused on scanning attachments received by email. Analyzing the answers provided, only two people confirmed that they always scan email attachments, 20 respondents said they are scanning the attachments only when the sender is unknown and the other 27 reported that they never scan attachments, although most participants stated that they have an anti-virus installed. This practice draws attention to the fact that employees are responsible for increasing the risk of data exposure, although they have almost all of the necessary tools to secure their work.

The responses provided by the participants demonstrate that they are aware of the impact that security incidents could have, but also indicate that the respondents are not always behave appropriately, fact that should be a wake-up call for organizations. Behaviors such as keeping access passwords written at the workplace and opening attachments in emails, without scanning them first, are ways to unintentional expose sensitive data.

Although 80% of participants were trained on information security aspects, most of them still perform actions that are inconsistent with an efficient privacy prevention policy. We believe that this result can be explained in two ways: the training sessions that the employees attended may not have been clear enough or the participants do not understand the significant role they are playing in protecting information.

Conclusions

Currently, security incidents are one of the most significant concerns in the Internet of Everything era, as technological developments have introduced new concepts in the financial and accounting fields such as ERP, cloud computing and mobile technologies that, besides the variety of advantages, bring specific vulnerabilities that threaten the security of sensitive information. In recent years, there has been an increase in security incidents both at national and global level. According to the latest CERT report, over 110 million cyber security alerts were recorded in Romania in 2016, up to 60% more compared with the previous year. At international level, according to Breach Level Index, more than 1.3 billion IT security incidents occurred, the number increasing by over 85% compared to 2015.

In the financial and accounting fields, most of the activities have been digitalized due to the need to have continuous access to relevant information in real time. Whether we are talking about mobile technologies, ERP systems or cloud computing platforms, almost all sensitive information has moved into the digital environment. This paper aimed to analyze the main challenges of information security in the context of digital accounting. This is done by highlighting the main vulnerabilities of the currently used technologies. We have also conducted a survey to determine the perception and awareness level of the impact of security incidents from the perspective of future professional accountants.

Analyzing the data presented, we can say that there are a variety of vulnerabilities, which have an increased potential to affect the security of financial information,

operational activities and the reputation of the organizations as well.

Because both ERP and cloud computing platforms are still under development, new types of vulnerabilities are expected to occur along with the technological progress. The best solution for preventing security incidents is to apply the best practices by using secure systems and applications and implementing effective controls to monitor potential exposures of sensitive information regularly.

Another important conclusion of this study is the need to create a stable culture of risk management and prevention, especially for confidential information exposures. The empirical research has shown that young professionals understand the importance of data protection, but they do not always demonstrate the best behavior to prevent security incidents. Due to these results, we consider the involvement of the academic environment as being important and should provide sufficient support regarding information security in the accounting study programs.

REFERENCES

1. Ahmed, H.A.S., Ali, M.H., Kadhum, L.M., Zolkipli, M.F. and Alsariera, Y.A. (2017), A review of challenges and security risks of cloud computing, *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, no. 1-2, pp. 87-89.
2. Ali, A. and Afzal, M.M. (2017), Database security: Threats and solutions, *Database*, vol. 6, no. 2, pp. 25-27.
3. Bahssas, D.M., AlBar, A.M. and Hoque, M.R. (2015), Enterprise Resource Planning (ERP) Systems: Design, trends and deployment, *The International Technology Management Review*, vol. 5, no. 2 pp. 72-81, DOI 10.2991/itmr.2015.5.2.2.
4. Bertino, E. and Sandhu, R. (2005), Database security-concepts, approaches, and challenges, *IEEE Transactions on Dependable and secure computing*, vol. 2, no. 1, pp. 2-19, DOI 10.1109/tdsc.2005.9.
5. Bhatia, T. and Verma, A.K. (2017), Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues, *The Journal of Supercomputing*, vol. 73, pp. 2558–2631, DOI 10.1007/s11227-016-1945-y .
6. Bruchez, R. (2012), *Microsoft SQL Server 2012 Security Cookbook*, Packt Publishing Ltd.
7. CERT (2016), *Raport cu privire la alertele de securitate cibernetică procesate de CERT-RO în anul 2016*, available on-line la https://cert.ro/vezi/document/raport-alerte-cert-ro-2016 (accessed 15 April 2017).
8. Cloud Standards Customer Council (2015), *Practical Guide to Platform-as-a-Service*, available on-line la http://www.cloud-council.org/CSCC-Practical-Guide-to-PaaS.pdf (accessed 15 April 2017).
9. Davenport, T.H. (1998), Putting the enterprise into the enterprise system, *Harvard Business Review*, vol. 4, pp. 121-31.
10. Evans, M., Maglaras, L.A., He, Y. and Janicke, H. (2016), Human behaviour as an aspect of cybersecurity assurance, *Security and Communication Networks*, vol. 9, no. 17, pp. 4667-4679, DOI 10.1002/sec.1657.
11. Giordanelli, R. and Mastroianni C. (2010), The cloud computing paradigm: Characteristics, opportunities and research issues, *Istituto di Calcolo e Reti ad Alte Prestazioni* (ICAR) .
12. Horwath, J. (2012), *Setting Up a Database Security Logging and Monitoring Program*, available on-line la http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.394.3370&rep=rep1&type=pdf (accessed 30 April 2017).
13. Hussein, N.H. and Khalid, A. (2016), A survey of Cloud Computing Security challenges and solutions, *International Journal of Computer Science and Information Security*, vol. 14, no. 1, pp. 52-56.
14. Jaiswal, P.R. and Rohankar, A.W. (2014), Infrastructure as a service: security issues in cloud computing, *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 3, pp. 707-711.
15. Kanellou, A. and Spathis, C. (2013), Accounting benefits and satisfaction in an ERP environment,

International Journal of Accounting Information Systems, vol. 14, no. 3, pp. 209-234, DOI 10.1016/j.accinf.2012.12.002 .

16. Kim, W. (2013), Cloud computing architecture*, International Journal of Web and Grid Services*, vol. 9, no. 3, pp. 287-303.
17. Klaus, H., Rosemann, M. and Gable, G.G. (2000), What is ERP?, *Information Systems Frontiers*, vol. 2 no. 2, pp. 141-162.
18. Kolodenker, E., Koch, W., Stringhini, G. and Egele, M. (2017), PayBreak: Defense against cryptographic ransomware, *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pp. 599-611.
19. Lodha, S. R. and Dhande, S. (2014), Web Database Security Techniques, *International Journal*, vol. 2, no. 3, pp. 293-299.
20. Malik, M. and Patel, T. (2016), Database security-attacks and control methods, *International Journal of Information*, vol. 6, no. 1/2, pp. 175-183, DOI 10.5121/ijist.2016.6218.
21. Møller, C. (2005), ERP II: a conceptual framework for next-generation enterprise systems?, *Journal of Enterprise Information Management*, vol. 18, no. 4, pp. 483-497, DOI 10.1108/17410390510609626.
22. Ponorîcă, A., Al-Saedi A. and Sadik H. (2014), The impact of enterprise resource planning systems on management accounting, *Challenges of the Knowledge Society*, vol. 4, no. 1, pp. 682-690.
23. Sharma, M.M., Husain, S. and Ali, M.S. (2017), Cloud computing risks and recommendations for security, *International Journal of Latest Research in Science and Technology*, vol. 6, no. 1, pp. 52-56.
24. Stanciu, V. and Rîndaşu, S. (2017) Emerging information technologies in accounting – are the aspiring professional accountants prepared to face the challenges? A case study of Romanian universities, *Proceedings of the 29th International Business Information Management Association Conference*, pp. 2455-2467.
25. Stanciu, V. and Tinca, A. (2013), ERP solutions between success and failure, *Accounting and Management Information Systems*, vol. 12, no. 4, pp. 698-612.
26. Surjit, R., Rathinamoorthy R. and Vishnu Vardhini, K. J. (2016), *ERP for Textiles and Apparel Industry*, WPI Publishing.
27. Swart, R., Marshall, B., Olsen, D. and Erbacher, R. (2007), ERPII System Vulnerabilities and Threats: An Exploratory Study, *Managing Worldwide Operations & Communications with Information Technolgy*, pp. 925-928.
28. Symantech, (2015) *Mistakes in the IaaS cloud could put your data at risk*, available on-line la http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/mistakes-in-the-iaas-cloud-could-put-your-data-at-risk.pdf (accessed 18 April 2017).
29. The Association of Chartered Certified Accountants (2013a), *Big data: its power and perils*, available on- line at http://www.accaglobal.com/bigdata (accessed 24 April 2017).
30. The Association of Chartered Certified Accountants (2013b), *Understanding investors: the road to real-time reporting,* available on-line la http://www.accaglobal.com/content/dam/acca/global/PDF-technical/financial-reporting/pol-afb-ui03.pdf (accessed 20 April 2017).
31. The Association of Chartered Certified Accountants (2014), *Digital Darwinism: thriving in the face of technology change*, available on-line la http://www.accaglobal.com/content/dam/acca/global/PDF-technical/futures/pol-afa-tt2.pdf (accessed 20 April 2017).
32. The Association of Chartered Certified Accountants (2016), *Cybersecurity - Fighting Crime's Enfant Terrible*, available on-line la http://www.futuretoday.com/technology/digital/cybersecurity.html (accessed 20 April 2017).
33. Trigo, A., Belfo, F. and Estébanez, R. P. (2014), Accounting information systems: The challenge of the real-time reporting, *Procedia Technology*, vol. 16, pp. 118-127, DOI 10.1016/j.protcy.2014.10.075.
34. Voulgaris, F., Lemonakis, C. and Papoutsakis, M. (2014), The impact of ERP systems on firm performance: the case of Greek enterprises, *Global Business and Economics Review*, vol. 17, no. 1, 112-129, DOI 10.1504/gber.2015.066536.