The Security of Accounting Information – A Perception-Based Analysis of the Practitioners from Romania

Sînziana-Maria RÎNDAŞU, Ph. D. Student,
Bucharest University of Economic Studies,
e-mail: sinziana_rindasu@yahoo.com

Abstract

The associated risks of the technologies currently used in the accounting field, relating to the difficulty of maintain the security of data, are still significant due to the complexity of the systems used which, in addition to the benefits they bring in accounting processes, generate a number of challenges in maintaining the fundamental characteristics of data. To address the current lack of well-trained practitioners for them to be able to reduce these risks, the international professional bodies support the need of developing a sufficient set of skills for accountants, by raising the awareness level of the impact that security incidents may have. At the same time, there is a gap between the skills that students acquire and the requirements of the business environment, an aspect that favors the increase and the impact of cyber-attacks. The purpose of this paper is to investigate the perception of data security of the practitioners in the field of accounting and auditing and the extent to which they believe that the information they receive is sufficient while examining the different types of actions of the professionals that may affect the security of accounting information. The results of the research show that the professionals are aware of the good practices of maintaining the fundamental characteristics of the data and understand the impact of incorrect information management, but a significant part of the study participants believes that does not receive enough information on data security from companies and professional organizations.

Keywords*: information security, perception of the practitioners, phishing, risks, accountability*

JEL Classification*: M14, M15, M41, M42*

To cite this article:
Rîndaşu, S-M. (2019), The Security of Accounting Information – A Perception-Based Analysis of the Practitioners from Romania, *Audit Financiar*, vol. XVII, no. 2(154)/2019, pp. 298-305,
DOI: 10.20869/AUDITF/2019/154/012

To link this article:
http://dx.doi.org/10.20869/AUDITF/2019/154/012
Received: 22.02.2019
Revised: 24.02.2019
Accepted: 11.03.2019

1. Introduction

The security of information has become one of the main challenges of organizations, as a result of the increased digitalization and process automation. Continuous access to information and real-time reporting of accounting data have become over the years the main objectives of companies to prove transparency and increase the level of confidence of investors.

To remain competitive and maintain the normal performance in optimal conditions, in the current context in which the information flow is continuous and grows exponentially, most companies are choosing to use technological solutions for process automation and time reduction, needed by the practitioners to manage information, which has led to an increased risk of exposing confidential and sensitive data, that may result in financial losses.

At the international level, professional bodies have been pursuing in recent years to increase the awareness level of the exposure risks of data by introducing concepts and control methods in the curricula of future practitioners (ACCA, 2018).

In the relevant literature there are studies that deal with the issue of the security of accounting information in terms of IT applications and solutions, but less attention has been paid to the level of understanding the need to secure information and how practitioners contribute to the decrease or increase of the risks generated by the digitalization of the processes. The objective of this paper is to investigate the extent to which accountants and auditors from Romania understand and protect the data and understand the expectations of the companies and professional bodies.

2. Literature review

The changes in the role of practitioners along with the evolution of IT systems and applications used to manage the activities requires a realignment of the practitioner's working skills to efficiently manage the volume of data, both in terms of the content of the financial data and maintaining and improving the characteristics of the data: confidentiality, integrity and availability. The changes in financial reporting and processes have generated different needs of investors and management and ensuring optimal security of systems and working procedures used is not optional (No and Vasarhelyi, 2017).

The relevant literature in the field of accounting information security proposes methods which can be used by practitioners to maintain data confidentiality (Hawker, 2005; Seetharaman et al., 2017; Bawaneh, 2018) by reviewing the user access rights to applications, using cryptographic solutions, implementing effective internal controls to reduce vulnerabilities and creating a set of procedures to maintain the security, but due to the complexity of current and emerging technologies that can be adopted in accounting, these methods do not fully cover the variety of risks.

Due to the fact that future and current professionals develop the skills needed to practice this profession through two sources, training from the professional bodies and the academic environment, one must consider how they both contribute to the continuous development and training of accountants and financial auditors. To prepare future and current practitioners to respond properly to the needs of the business environment, the international professional bodies have begun in the last years to draw attention both to the need to acquire a sufficient set of working skills with current and future technologies and to protect data, by avoiding incorrect manipulation or exposure and creating controls that are sufficient to reduce the information security risks (ACCA, 2016). However, in the ACCA report, we only find little information about how practitioners can cover these risks, so the sphere of knowledge that needs to be developed is not fully defined. In the author's opinion, professional bodies should provide a clear set of tasks that accounting practitioners need to develop in order to reduce the impact of existing vulnerabilities.

ICAEW (2015) urges practitioners to develop their digital skills to understand and use new technologies to manage the increasing amount of information and raise a flag to highlight the risks associated with the incorrect manipulation of data that may end up jeopardizing the confidentiality of it. At the same time, the ICAEW proposes a new representation where the role of the accountant distances from traditional image to a new role based more on financial analysis activities and management forecasts.

Long-term expectations are that more and more emerging technologies will be integrated and used in the accounting departments to respond to the market competition. Thus, the set of IT skills that current and future accountants need to develop is in a continuous change, but according to the relevant literature, there is currently a gap between the requirements of the business environment and the study programs offered by the universities, due to the lack of an active communication (Blount, 2016). As academic education is the foundation of professional training, it is vital to review the curricula so that universities keep students active and improve their ability to integrate into the workplace. Accounting faculties must therefore respond urgently to changes resulting from the increasing adoption of emerging technologies, otherwise, there is a risk that more and more potential students may choose other study programs that will provide them with a sufficient knowledge base.

In Romania, as per the study conducted by Stanciu and Rîndaşu (2017), the majority of public accounting faculties offers a double specialization, both in the accounting and management information systems fields, but the authors conclude after analyzing the plans studies in master and undergraduate programs, that only in a few cases were included in the syllabus subjects such as management information systems, data security, IT audit and emerging technologies, which are currently among the most demanded competencies by the business environment. This result confirms the gap between the skills that practitioners develop within the academic environment and the expectations of the companies and the non-alignment of the university training to the new requirements will determine in the medium and long term the failure to meet the skills needed by the employers as a result of the review employment requirements and an increase in the number of security incidents due to the diversity and importance of information. However, according to the study by Stanciu and Tinca (2018), the lack of well-trained staff is only a part of the causes of the incidents, the other part being the lack of budgets and the complexity of implementing effective controls.

3. Research methodology

The aim of this paper is to analyze the perception of accountants in the field of information security and to find out whether they consider themselves well prepared enough to cope with the challenges of maintaining the fundamental characteristics of the accounting information. At the same time, the research includes elements to determine whether practitioners are behaving correctly in order to reduce data security risks and whether they have sufficient information to act appropriately in the event of a cyber-attack. To accomplish this goal, we have made a qualitative empirical research in the form of a survey of 20 questions with one or more variants and Likert scale questions.

The questionnaire was addressed solely to accounting practitioners, particularly those in financial accounting and auditing and was sent to potential respondents through professional social networks and online practitioners' groups. The responses were collected between January and February 2019 and 137 responses were received, one response being disregarded as the participant was not part of the target group, therefore having 136 valid answers.

Analyzing the years of experience in the field, the average is of 10 years and this result is one of the first conclusions of this research: the fact that there is a maturity of the participants, who should have sufficient knowledge about the information security and demonstrate correct data protection behaviors. Analyzing participants' responses to affiliation with professional bodies, 73 practitioners, representing 53.67% of the total of respondents to the questionnaire, are members of at least one professional organization.

The big companies adopt new technologies much easier because they have higher budgets for investment, which is why we considered it appropriate to take into account the size of the companies, having in mind the idea that companies with more than 250 employees have more knowledge about data security. Analyzing the results, the majority of respondents (44.8%) works in large companies, 39% in medium-sized companies with less than 250 employees and 16.2% work in organizations with less than 10 employees.

4. Results and discussions

The questionnaire consists of four sections, the first investigating the experience in the field and the affiliation with professional bodies. In the second part of the research, the study focused on analyzing the quality and quantity of knowledge regarding the security of information that the participants receive both from the companies for which they work and from the professional bodies. The majority of practitioners (88.2%) who responded to the survey believe that organizations should provide training programs to improve data security, but only 63.2% confirmed that they had attended such courses. As a result, organizations may need to pay more attention to this issue, as IT vulnerabilities are not universal, with every IT infrastructure having its own characteristics and challenges.

Due to the fact that the human factor continues to represent a significant element that can diminish or accentuate the risks of exposure or loss of information, companies need to realize the importance that training programs can have in reducing risks that can generate financial losses and a decrease in the investors' level of confidence (Colwill, 2009). Over time, social engineering methods have improved and generated more attacks due to a lack of staff well-trained to recognize them and the most effective solution to combat is through effective training sessions (Greitzer et al., 2014).

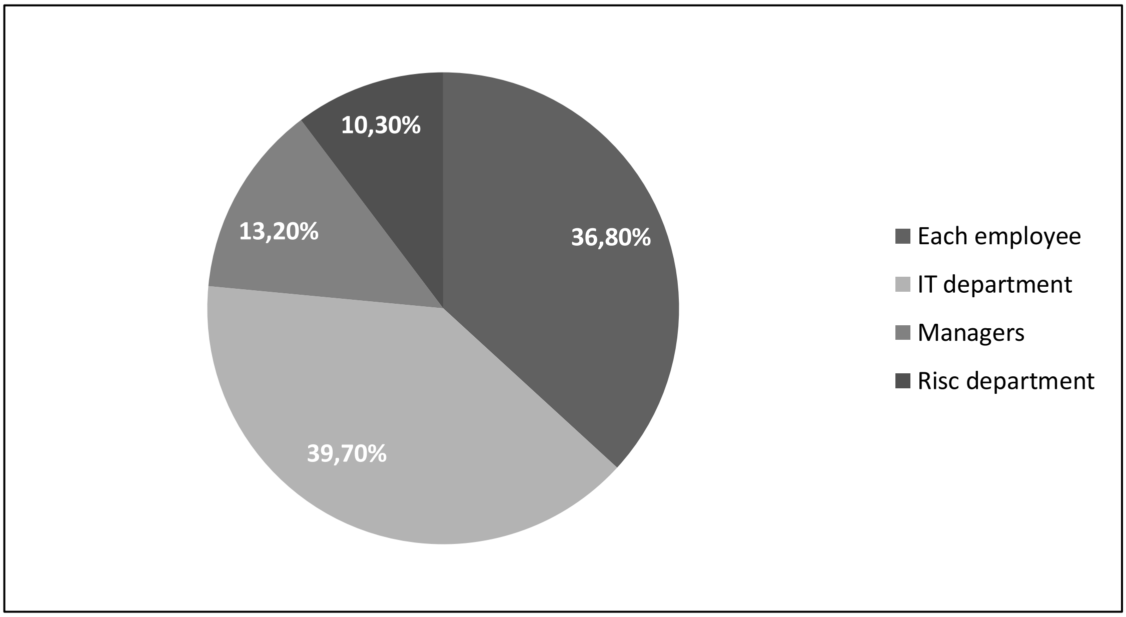
From those 53.7% participants who are members of national and international professional organizations, 54.79% consider that they have enough information on data security, 31.50% says they receive some information, but consider that it is not enough and the rest the participants responded that did not receive any information in this respect. This result indicates a gap between the long-term professional training plans and the business environment expectations. Information security is indeed a complex subject, which requires continuous learning, but in the absence of a sufficient level of skills to protect sensitive and confidential data, the impact and frequency of cyber-attacks will increase significantly.

Since May 25, 2018, across all the countries of the European Union, the General Data Protection Regulation (GDPR) has entered into force and concerns the protection of personal data. Given that a significant part of the data in the accounting field is referring to individuals, this regulation should have led companies to provide training to employees in order not to disregard the principles of the regulation. A study conducted by Stanciu and Rindaşu (2018), two months before the GDPR came into force, made it clear that at that time only a relatively small percentage of practitioners in the Romanian accounting field received training on this matter. To analyze whether changes really took place one year after the regulation started to be applied, the participants from this current study were asked whether they were using personal data and if they had received training sessions from the companies. Analyzing the answers received, 77.9% of respondents use personal data, but only 66.03% of the 103 participants confirm that they have been trained. By comparing this result with that of the above-mentioned study, no significant changes are identified, a fact that should raise a flag, mainly due to the fact that if the companies are not complying with the GDPR can incur significant sanctions fees.

The questions from the third part of the survey aimed to investigate the actions of the practitioners that could affect data security. Thus, the respondents received a set of questions about the responsibility of data security, account management and passwords. After analyzing the answers received, there were identified some actions that increase the risk of incorrect data management: 4.4% of participants said they use the same passwords for accessing personal and professional accounts and 14% confirmed that in the teams they are working, account and application passwords are not individual, which may lead to fraud, if there are no unique means of identifying users. At the same time, after being asked if they shared the credentials within the team, 11% of the respondents answered in the affirmative and 3.7% confirmed that they had been asked for their passwords, but did not offer them. Such actions can have multiple and major consequences, even financial losses and should be addressed urgently by the companies.

In terms of the accountability to maintain the security of data, most respondents believe the IT department is responsible, followed by each employee, managers and risk department (**Figure no. 1**).

Figure no. 1. The perceptions of respondents about the responsibility of maintaining the security of the information



Source: Own processing, based on responses received from the participants

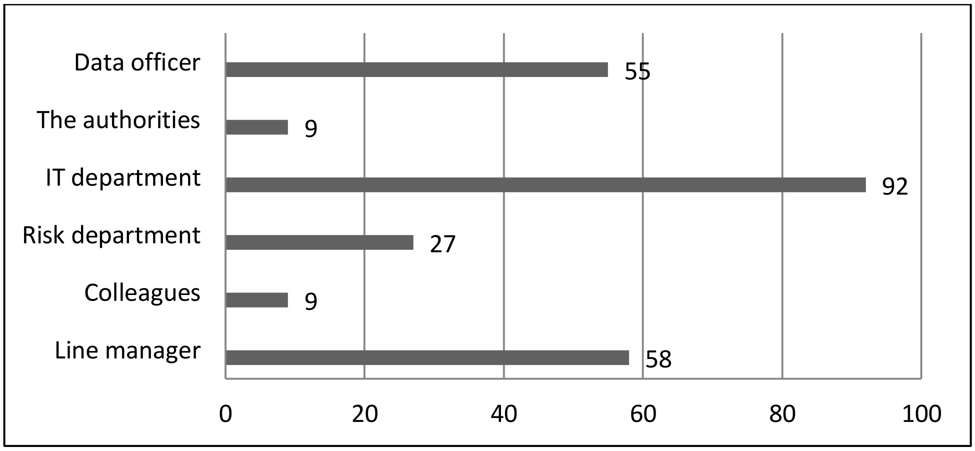
The answers provided show that over 60% of practitioners believe they are not responsible for the data security, aspect which raises concerns about how sensitive and confidential data is managed. IT departments may impose some preventive controls to avoid unauthorized access and data exposure, but these solutions fail to completely avoid such risks, especially when the staff in charge of handling the data does not have enough knowledge and adopts actions that are not following the best practices to avoid data loss.

In the last part of the questionnaire, the goal was to study participants' perceptions about their knowledge of data security. Considering that social engineering techniques continue to be one of the most important vulnerabilities, participants were asked if they had knowledge about phishing attacks and the majority (68.4%) responded affirmatively. This result should not be regarded as positive because of the fact that there is a significant population that does not have enough knowledge to avoid becoming a victim of such an attack. To reduce these risks, companies should initiate training campaigns to draw employees' attention to such dangers, but even in such cases, the relevant literature shows that the avoidance rate is not absolute due to the fact that this kind of attack is improving continuously and manages to pass undetected even by the trained employees (Alsharnouby et al., 2015).

The participants were asked if they thought they had enough knowledge to detect whether the laptop or computer they were using has been the target of a cyber-attack and 39.7% answered affirmatively, 19.1% said they could not detect it and 41.2% have no certainty that they could identify such a situation because they believe to have insufficient knowledge. According to the report by the Ponemon Institute (2018), on average, the existence of an attack is identified in 196 days, enough time for confidential data to be exposed.

Asked who they are addressing when detected that they have been the victim of a cyber-attack, most responded that they will alert the IT department, followed by the hierarchical superior and the data protection department (**Figure no. 2**). Even if employees have enough knowledge to detect a cyber-attack, it's important to know to who they can report to minimize possible losses. Therefore, companies must issue procedures that give clear indications, so that they can act as quickly as possible.

Figure no. 2. Points of contacts addressed by accountants when they suspect they have been the target of a cyber-attack



Source: Own processing, based on responses received from the participants

In the last question of the questionnaire, the participants self-evaluated on a 5-point Likert scale (0 - total disagreement, 5 - total agreement) the degree of awareness of the impact of data security, the level of knowledge, the importance of the data it manages and the impact they have in the risk reduction, the statistical analysis of the answers received from the respondents being detailed in **Table no. 1**.

Table no. 1. Statistical analysis of received responses

	Changes in the awareness level regarding the impact of data security	Having sufficient knowledge to ensure data security	There are activities performed by the practitioners that could affect data security	The managed information does not pose any risk
Average	3.94	3.57	2.85	2.72
Standard deviation	1.24	1.14	1.32	1.33
Minimum	1	1	1	1
No. min.	12	9	31	36
Frequency min.	8.82%	6.62%	22.79%	26.47%
Maximum	5	5	5	5
No. max.	59	30	16	13
Frequency max.	43.38%	22.06%	11.76%	9.56%
Median	4	4	3	3
SKEW	-1.15	-0.63	-0.02	0.09

Source: Own processing, based on responses received from the participants

According to the statistical analysis, most participants consider that they have lately changed their awareness of the impact that incorrect data security may have on organizations and believe they have an average level of knowledge to ensure the maintain of the fundamental features of the data. These results are consistent with the respondents' answers from the previous questions and it can be noted that most practitioners show relatively reasonable behavior, even in the absence of training sessions. Also, regarding the existence of activities that could affect the security of the managed data, most consider that they do not contribute to the existing risks and are aware of the impact of inappropriate data manipulation, but in the same time it should be taken into account that this output has been achieved as a result of a self-evaluation of the participants on their own skills, the purpose of the work not being to test the real level of knowledge.

Conclusions

In this paper it has been studied the perception of the practitioners from the accounting field regarding data security by focusing on the following aspects: the quantity and quality of the information received from the companies and professional bodies, the responsibility for the preservation of the data quality and the perception of the associated risks.

Although the professional bodies emphasize the importance of information security, a significant percentage of members believe that the information received is not enough or in some cases is completely missing and the companies they are working for do not provide adequate training to create a sufficient knowledge base to address security issues. In order to overcome this gap, both professional organizations and companies need to pay more attention to effectively manage the vulnerabilities of the accounting data and systems used.

In terms of data protection accountability, most practitioners show relatively reasonable behavior, but due to the fact that they do not receive enough information, they do not believe they can fully manage the risks generated by the data used. The practice of shared accounts and access codes is an aspect that significantly increases the risk of data integrity and companies should review their procedures to avoid maintaining these vulnerabilities.

The practitioners consider that they have enough knowledge to manage the data correctly and believe that over the years their awareness level over the impact has increased, result that it is also reflected in their behavior. These opinions should be seen with some skepticism, being merely subjective opinions of the respondents, who are not subject to an assessment of the level of knowledge on data security. There is a significant number of respondents who consider that their activities don’t pose any risk, although they manage personal data without the proper training.

The human factor continues to be a significant element in maintaining information security, but in the absence of the adequate support and procedures that can provide sufficient knowledge to effectively manage vulnerabilities, the risks associated with accounting data continue to pose a challenge. After analyzing all of the respondents' answers, it is highlighted the existence of a gap between the needs of companies and the support they provide to practitioners, in order to be able to respond to current needs and act as caretakers of sensitive and confidential data.

REFERENCES

1. Alsharnouby, M., Alaca, F., & Chiasson, S. (2015), Why phishing still works: User strategies for combating phishing attacks, *International Journal of Human-Computer Studies*, 82, pp. 69-82.
2. Bawaneh S. (2018), Securing Information Technology for Banks and Accounting Information Systems, *International Journal of Applied Engineering Research*, Vol.13, 6 (2018), pp. 3291-3300
3. Blount, Y., Abedin, B., Vatanasakdakul, S., & Erfani, S. (2016), Integrating enterprise resource planning (SAP) in the accounting curriculum: a systematic literature review and case study, *Accounting Education*, 25(2), pp. 185-202
4. Colwill, C. (2009), Human factors in information security: The insider threat–Who can you trust these days?, *Information security technical report*, 14(4), pp. 186-196.
5. Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014), Analysis of unintentional insider threats deriving from social engineering exploits, *IEEE Security and Privacy Workshops*, pp. 236-250
6. Hawker, A. (2005), *Security and control in information systems: A guide for business and accounting*, Routledge
7. ICAEW (2015), *Providing leadership in a digital world*, available at https://www.icaew.com/-

/media/corporate/files/technical/information-technology/technol ogy/providing-leadership-digital-full-report.ashx (accessed on February 17, 2019)

8. No, W. G., & Vasarhelyi, M. A. (2017), Cyber-security and continuous assurance, *Journal of Emerging Technologies in Accounting*, 14(1), 1-12.
9. Ponemon Institute (2018), *2018 Cost of Data Breach Study: Global Overview*, available at https://www.ibm.com/downloads/cas/861MNWN2 (accessed on February 17, 2019)
10. Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which repeals Directive 95/46/EC
11. Seetharaman, A., Patwa, N., & Niranjan, I. (2017), Role of Accountants and Auditors in Mitigating Digital Crimes, *Journal of Applied Economics & Business Research*, 7(1).
12. Stanciu V. & 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*, 2455-2467
13. Stanciu, V. & Rîndaşu, S., (2018), The Impact of General Data Protection Regulation in The Accounting Profession – Evidences from Romania, *Journal of Information Assurance & Cyber security*, Vol. 2018
14. Stanciu, V., & Tinca, A. (2017), Exploring cybercrime–realities and challenges, *Accounting and Management Information Systems*, 16(4), 610-632
15. The Association of Chartered Certified Accountants (2018), *Strategic Business Leader (SBL) Syllabus and study guide*, available at https://www.accaglobal.com /conte nt/dam/acca/global/PDF-students/acca/SBL/Strategic-Business-Leader-syllabus-and-study-guide-D17.pdf (accessed on February 17, 2019)
16. The Association of Chartered Certified Accountants (2018), *Market change is faster than ever – is your finance function in the race?*, available at https://www.accaglobal.com /content/dam/ACCA_Global/Technical/fin/PI-Market-change-is-faster-than-ever%20-is-your-finance-function-in%20-the-race.pdf (accessed on February 17, 2019)