Stanciu, Victoria; Gheorghe, Mirela

Article

Facing the Mobile Revolution: A Romanian Insight

Journal of Accounting and Management Information Systems (JAMIS)

Provided in Cooperation with:
The Bucharest University of Economic Studies

Suggested Citation: Stanciu, Victoria; Gheorghe, Mirela (2019) : Facing the Mobile Revolution: A Romanian Insight, Journal of Accounting and Management Information Systems (JAMIS), ISSN 2559-6004, Bucharest University of Economic Studies, Bucharest, Vol. 18, Iss. 1, pp. 101-118, https://doi.org/10.24818/jamis.2019.01005

This Version is available at:
https://hdl.handle.net/10419/310737

Accounting and Management Information Systems
Vol. 18, No. 1, pp. 101-118, 2019
DOI: http://dx.doi.org/10.24818/jamis.2019.01005

Facing the mobile revolution: A Romanian insight

Victoria Stanciu[a1] and Mirela Gheorghe[a]

[a] *The Bucharest University of Economic Studies, Romania*

Abstract

Research question: Are the accounting graduates prepared to deal with mobile devices' security issues? ***Motivation:*** Nowadays, mobile computing is a part of the younger generation, the entering workforce in coming years, and from this point of view the BYOD (Bring Your Own Device) approach will continue its increasing trend. The authors investigated the accounting bachelors' knowledge in regard with mobile devices' use aiming at signaling the existing gap on mobile devices' security awareness. IT security specialists consider that both, academia and industry should focus their security awareness campaigns aiming at combat the false sense of security that mobile devices' users have. ***Idea:*** The authors aimed at providing an in-depth understanding of the accounting students' profile as mobile devices' users and their knowledge and awareness in regard with mobile security threats. ***Data:*** The analyzed sample includes 180 subjects, out of which 81% are bachelors in accounting (38% 1st year; 43% 3rd year) and 19% master students in accounting and banking. ***Tools:*** The literature review helped us in structuring our research objectives and design a multiple-choice questionnaire used in the empirical study. ***Findings:*** The study reflects the students' insufficient information in regard with mobile devices features and security issues. This is the result of the limited IT lectures and seminars in the curriculum and the insufficient focus on mobile devices' use in the accounting profession. Students should understand the mobile devices as complex devices providing diverse features, not limited to communication with friends and Internet information searching. ***Contribution:*** The study contributes towards closing the existing gap in the Romanian research and literature in regard with young generation insufficient knowledge on mobile devices' security and the potential threat brought by BYOD on the companies' IT environment.

[1] *Corresponding author*: Department of Management Information Systems, The Bucharest University of Economic Studies; 6 Piata Romana, Bucharest; tel. (+40) 0213191901; email address: victoria.stanciu@cig.ase.ro

Keywords: Mobile devices, threat, mobile security, BYOD

JEL Codes: A2, I25, M15

1. Introduction

Gadgets such smartphones and tablets brought a new lifestyle across generations. "Mobile devices are paying a larger role, not only in business but social media" and people's personal life (Grant Thornton, 2013). The Y generation is the one that embraces natively the mobile devices' use and this new lifestyle. On the other hand, companies are looking for business increase, higher efficiency, more visibility in the virtual space and improved relationship with clients and partners. The solution stays in mobile devices that bring lots of advantages together with business transformation and the new cultural challenge of mobile culture, altogether reshaping the business processes and rules. But let's look at the second facet of the coin: mobile devices' use is accompanied by a diverse and concerning set of security risks. The companies are aware that it is a high likelihood that sensitive information or data will be sent or received via mobile devices (Grant Thornton, 2013). "Securing organizational data and protecting personally identifiable information is not possible unless mobile devices are secured" (Gearns, 2016: 36). In this new complex IT environment, the companies face the security risks from a new perspective. This risk approach emphasizes the need for a threat intelligent program and imposes integrated solutions, protecting the companies' network, applications and the diverse mobile devices' infrastructure.

The companies understood that they have to align their operating model to the digital world, to manage their complex and continuously evolving IT environment embedding in it all the new gadgets that are now part of employees' lifestyle. Specialists consider that companies demonstrating lack of "confidence in their ability to implement emerging technologies should see this as a concern" (Kluver, 2013: 10). Nowadays, the mobile culture is deepened rooted in the companies' business processes. Companies worldwide are now opened to the mobile devices usage, being aware of mobile computing advantages. The BYOD (Bring Your Own Device) wave overflows the companies' IT environment. A survey performed in 2014 emphasized that 63% of the respondents declared that their employees are using, on daily bases, smartphones and tablets, 46% declared that the employees are using just smartphones and 29% of the employees are using tablets. The same survey revealed that 90% of the respondents allow in their companies some mix of personal and business own mobile devices (ISMG, 2015). As a result, we can conclude that BYOD concept has already reshaped the way employees perform the job requirements and the companies' culture. It shouldn't be forgotten that "mobile

computing is a part of the younger generation entering in the workforce in coming years" (Madan et al., 2013:4) and from this point of view the BYOD will continue its increasing trend. Even if the young generation is so opened to the mobile devices' use it is observed a lack of mobile security knowledge reflected in the users' behavior and security practices. A survey issued in 2014 emphasized the IT security specialists' opinion that "employees behavior is a significant factor for information security" (Dimensional Research, 2014: 2).

IT security specialists consider that since the mobile users "do not actively follow most of the security best practice, academia and industry should focus their security awareness campaigns and efforts in order to combat the false sense of security that users have" (Androulidakis, 2016:9). The authors totally agree with the above mentioned opinion and conducted their research on the young generation use of mobile devices aiming at emphasize their mobile users' profile and security knowledge. The research investigated the students' mobile devices' security awareness and personal practice behavior, the gaps in the students' training on the topic and the universities' role in preparing the young generation of accountants to face the mobile devices' culture and security challenges. The research revealed significant gaps regarding the mobile security knowledge and awareness in the context of an extended use of mobile devices by accounting students. The complexity of the software, complicated settings and difficulties in performing updates are the causes for no security measures' use declared by the respondents. The authors consider that bachelor students need more theoretical training and specific mobile devices' security skills. There is still room for more focus, in the computing classes, on detailed approaches in regard with accounting automated processing flows and their security issues.

The present study is part of a wider research started two years ago focusing on the mobile computing impact of the accounting profession and the accounting students' options for mobile devices use. The present study contributes towards closing the existing gap in the Romanian research and literature in regard with young generation insufficient knowledge on mobile devices' security and the potential threat brought by BYOD on the companies' IT environment.

The paper is structured as follows: the following section, Section 2, reports on the literature review on mobile devices' increased use and mobile devices' specific security issues. Section 3, discusses the research methodology, objectives and methods. Section 4 retains the main findings and conclusions of the empirical study. The research conclusions are synthetized in the final section, Section 5, emphasizing the insufficient knowledge of the mobile devices' users on security threats affecting the companies' information security in the context of the BYOD trend.

2. Literature insights on mobile device use and security

Global sales of smartphones registered, according Gartner's analysis, an important increase in the first quarter of 2017, 9.1% comparing with the Q1 of 2016, meaning 380 million units. The operating systems for those worldwide sales reflect the domination of Android OS (86.1%) and iOS, 13.7% (Gartner, 2017). This market share consolidates the previous years of dominance of Android and iOS. Taking into consideration the market share, it is not surprising that IT specialists view these mobile platforms as the greatest risks for their companies (Dimensional research, 2014). The cybercriminals will always focus on most numerous targets presenting same week points. The sales increase reveals the users' preference for the above mentioned mobile platforms and users' trend of spending more to get a better smartphone.

The number of global tablet users registers a continuous increase from 840 million in 2014 at 1.32 billion in 2017 being expected 1.46 billion users in 2020 (Statista, 2017). The global tablets' market registered ups and downs, the increase being less dynamic during the years, Apple and Samsung continuing their domination.

ISACA specialists consider that mobile computing devices' vulnerabilities exist in: the device itself, the wireless connection, the user's personal practices, the organization's infrastructure and wireless peripherals (e.g. printers, keyboard, mouse etc.).

NIST emphasizes seven aspects that define a model for all threats of mobile device (NIST, 2013):

1. **Lack of physical security controls:** compared to other devices, the mobility of smartphones and tablets exposes them at the risk of being stolen or lost, fact that affects data confidentiality. This statement is confirmed by all the international surveys analyzed by the authors, surveys that indicate stolen and lost mobile devices as one of the most significant treat in regard with mobile devices.
2. **Use of untrusted mobile devices:** in the current way of manufacturing the mobile devices and also in the OSs there are not implemented suitable security restrictions comparing to those available on a PC or laptop this being explained by the mobile devices initial usage destination.
3. **Use of Untrusted Networks:** the mobile devices can use non-organizational network for Internet connection. The data communication is based on technology such as Wi-Fi or cellular networks. Wireless capability poses a number of specific security risks.
4. **Use of Untrusted Applications:** the facility of searching and installing apps specifically designed for those devices (games, WhatsApp, Snapchat etc.) is a

characteristic that provides a high level of satisfaction to the users but poses obvious security risks.

5. **Interaction with Other Systems:** mobile devices may interact with other systems in terms of data exchange and storage and, as a result, this interaction raises important security issues.
6. **Use of Untrusted Content.**
7. **Use of Location Services:** mobile devices with GPS capabilities typically run as location services.

The critical question in regard with mobile use is why these devices raise significant security issues? It should be mention that mobile devices began as a consumer technology, and as a result, "*many of these devices lack the security and administrative functions that IT and security teams use to manage traditional endpoints such as laptops and desktops*" (McEnaney, 2016). Nowadays, cyber criminals focus a significant part of their attacks on mobile devices, being aware of the existing security weak points. Security specialists and more informed users understood that no one is immune to cyber-attacks and day by day it is more difficult to secure mobile devices. But it is a large segment of mobile devices' users being not informed or insufficient informed in regard with mobile devices' communications and apps issues this fact being reflected in their behavior. "Excessive confidence could lead to "relaxation" of security practices while excessive fear certainly hinders technology adoption and especially mobile downloading" (Androulidakis, 2016: 9). As a conclusion, aiming at benefit from the mobile devices advantages there is a stringent need to inform the mobile users in regard with the important mobile security issues and make them aware with the existing threats. Improving the mobile users' behavior as a result of their increased security awareness will be beneficial for the individuals as well as the companies that adopted BYOD.

As it is already mentioned, compared to personal computers, mobile devices (including smartphones and tablets) are threatened by a larger variety of factors determined by technical characteristics such as: data communication via Wi-Fi or other Internet connections, video camera, microphone, data storage systems, GPS connectivity etc. ISACA specialists believe that the most common risk factors that apply to using mobile devices are: device-specific malware; theft of sensitive data; exposure of critical information through wireless sniffers; wireless intruders capturing emails, email addresses and attached data; loss, theft or damage of the device (ISACA, 2016).

The first virus, a Trojan, affecting Palm devices was identified in 2000. Cabir, "the first malicious code that can spread itself exploiting the network technologies on mobile devices" (Bluetooth) to infect other device was identified in 2004 (La Polla

et al., 2013: 449). Not long ago, two malware, Gooligan and HummingBad, affected millions of phones. Gooligan has taken hold of about 10 million Android phones. The Google accounts were breached being obtained personal and sensitive data (Hautala, 2016; Check Point Research Team, 2016). Two families of mobile banking Trojans, Faketoken and Marcher, were created to steal payment details from Android devices. In the Facktoken case it should be mentioned the resourcefulness of the attack: when the user visits its online banking account, the Trojan modifies the page and asks the user to download an Android application to secure the transaction. As a result, the cybercriminal gains access to the user's banking account (Kaspersky, 2015). These are some examples of cyber-attacks on mobile phones demonstrating the virulence and increasing sophistication of the mobile attacks methods. The continuous growing of mobile malware is expecting to continue due to the widespread of mobile devices. The 2017 survey of Dimensional Research signals that malware (58% of the respondents) and phishing using text messages (54% of the respondents) were the most frequent types of attacks on mobile phones registered by the companies. In 2015, in Romania, the mobiles using Android OS experienced ransomware attacks; the source of attacks was represented by spam e-mail having as attachments infected files or archives.

The 2017 PWC survey emphasized that 28% of the respondents "*reported security compromises of mobile devices, and securing smartphones and tablets is clearly top of mind*" for the IT security specialists (PWC, 2017: 9). The IT security professionals fight against mobile devices' attacks issued by cybercriminals is extremely difficult. They deal with many products, from multiple vendors, determining significant costs to configure and manage all these mobile devices and having insufficient budgets so that many companies do not use advanced mobile cyber-attack protection solutions (Dimensional Research, 2017).

In this context, it is obvious that security professionals consider as the top three inhibitors for the full deployment of mobile workforce: privacy, device security and content security (Information Security Media Group, 2015).

The mobile devices' security must be accompanied by a secure mobile communication. Aiming at ensuring confidentiality and data integrity the security specialists should identify the most adequate security mechanisms (as for example mobile token or a link-layer) and promote authentication so that the receiver to trust the source of the message.

Mobile devices' security implies a set of controls as for example (ISMG, 2015; PWC, 2017):

- Devices' management (enforcing passcodes, malware prevention etc.);

- Controlling users' login time, patterns of access and type of device;
- Applications' security, implying vulnerabilities testing and permanent updates;
- Enterprise data encryption;
- Screen locks;
- A risk based mobile access decision in regard with the companies' resources;
- Transactions' security (end-to-end encryption, transaction risk scoring etc.);
- Restricted sharing of the company content with non-company approved applications etc.

A centralized and coherent BYOD policy is for now compulsory for any company. Adopting this policy is not an easy task, IT professionals having to take into consideration and balance several factors:

- the need to understand the company's mobile computing pattern and the entire set of potential security risks induced by the mobile devices' use;
- it is difficult to decide how to drown the line on enforcing security and usage policy as long as the device is not own by the company;
- the personal and company's data and applications are on the same devices;
- the policy should be articulated with the entire set of IT policies and reflect the integrated information security defined for the company;
- there is a new paradigm that impacts the company's culture and employees' behavior that should reflect an increased awareness on mobile threats.

The companies are aware that they should integrate the new technologies in their digital ecosystem this being a very demanding and challenging objective. There is an increasing dynamic of the innovation in the IT industry and the companies should be prepared to understand and assimilate all these technological changes integrating them in the business and management models. The effort continues on the IT maintenance layer and monitor of the mobile device.

Facing so diverse and challenging information security threats, IT specialists became aware of the need to have a threat intelligent program.

Starting from the security professionals' conclusion that employees are a great threat to security, greater than cybercriminals and their behavior could make the "difference in preventing high-profile security breaches" (Dimensional Research, 2014) the authors investigated The Bucharest University of Economic Studies' students' knowledge and awareness on mobile security issues. The study's results are synthetized in the section 4.

3. Methodology

The authors' research had two coordinates: a qualitative one aiming to identify the security issues, characteristics and trends in mobile devices' use and, a second one, aiming at performing and empirical study in regard with the accounting students' use of mobile devices and their knowledge and practices in regard with mobile devices' security.

The authors performed a systematic literature review on mobile devices' use and security. The literature review helped us in structuring our research objectives and design the questionnaire used in the empirical study. The authors focused on researches performed worldwide in regard with the mobile devices' use in business processes and specific issues raised in the IT risk management, synthetizing the main problems emphasized by the researches and analysing the surveys issued by prestigious international organizations.

The empirical study is based on a survey aiming to reveal the users' practices and awareness in regard with mobile devices. The students in The Bucharest University of Economic Studies (the last year of bachelor degree and master students) represent the target group. The criteria used to establish the target group are [i] the students' age – the Y generation is more receptive to new technologies and [ii] the graduate students are the new entries in the accounting profession and, from this point of view, it is revealing for the study to investigate their mobile devices' practices and security awareness.

In the study was used a multiple-choice questionnaire containing 21 questions structured in two parts: in the first part were included demographic questions aiming to retain the students' gender, field and level of study. The second part included questions focusing on the nature, characteristics, practices and security perception of the users' in regard with mobile devices.

We collected 180 questionnaires, none of them being rejected. The respondents' sample is representative for the analyzed population. The subjects are accounting bachelors and students from accounting and finance and banking master programs. The data collection was performed between October 2017 and January 2018. The present survey extends the previous one performed during October 2016 and December 2017 aiming at enlarging our research on the mobile devices' use and security impact in the accounting profession and consolidates the previous research conclusions.

4. Results and discussion

The authors conducted the data analysis starting from the following questions:

1. Which is the students' behaviour as mobile devices' users?
2. What are the aspects influencing the students in mobile device purchase?
3. Which is the students' perception on the education/training in mobile security field?
4. Which are the security measures implemented by the students on their mobile devices?
5. Which are the reasons of not using security measures?
6. Which are the security incidents experienced by the students in the past 2 years?

The structure of the analyzed sample includes: 180 subjects, out of which 81% are bachelor's in accounting (38% 1st year; 43% 3rd year) and 19% master students in accounting and banking. From the entire sample 14% respondents are males and 86% females.
The study reveals that all the students questioned use at least one mobile device and among them a major part owns a smartphone (99%) and a laptop (86%).

Table 1. Types of mobile devices used by students

Type	Frequency
Smartphone	99%
Laptop	86%
Tablet	28%
MP3 Player	6%
Cell phone	1%

Within the questionnaire a number of questions tried to investigate the students' views upon the mobile devices technical features. In this regard, one of the questions analyzed the elements that can influence the buyer (on a scale of 1 to 7) while choosing a device. The results highlighted that the most important factor is the producer, followed by the price and the operating system. The last places were occupied by the connectivity and the service systems.

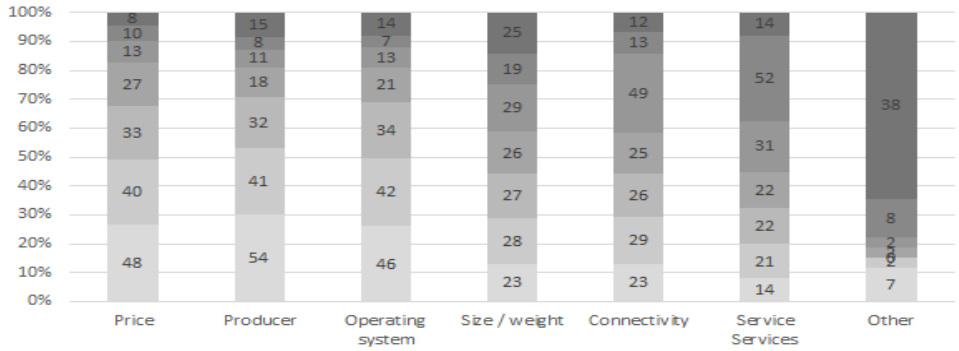

Figure 2. Factors influencing the decision to acquire a mobile device

The authors proceeded to another analysis aiming at create a scale for the technical features of the mobile devices. The analysis emphasizes that battery autonomy, operating system, storage capacity and RAM size are the main preferences of the students. Last places are taken by interoperability, screen size, keyboard and weight. The security is somewhere in between, fact that represents a healthy reasoning that proves a certain awareness.

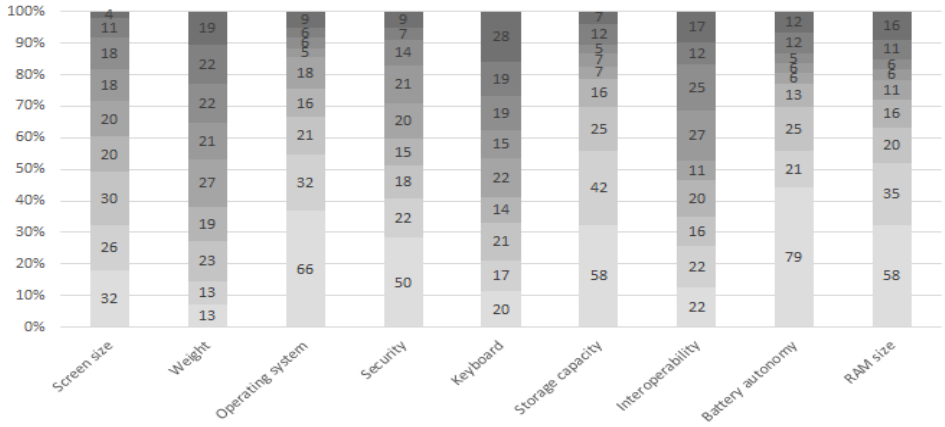

Figure 3. Technical features priorities

The following questions focused on the security of the mobile devices. On this purpose, we asked the subjects: How important is the security for them? At which level do they estimate their mobile devices' security? How did their behaviour evolve towards information security in the past year? The students' answers reveal interest for the topic in discussion, 63% consider that they implemented good security solutions, 26% are not sure and 11% think they are not using enough

security measures. The great majority of the respondents consider they are more aware on security need then in the previous years. This is in line with the respondents' opinion in our 2017 survey. Other issues refer to the level of education/training in information security field. We can observe that a great majority (40%) learned about this subject online, 20% from the university lectures and 11% claimed that nobody taught them.

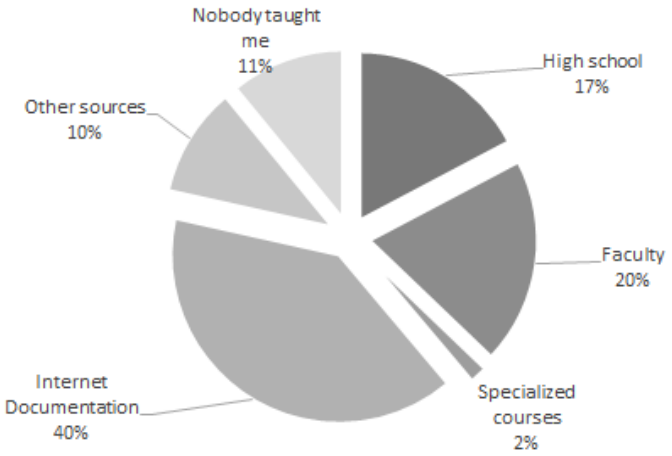

Figure 4. Where did you learn about information security?

The subjects' point of view regarding information security education is that every person should receive this sort of information (132 students) or search about it on their own (60 students). Again, as the 2017 survey revealed, the mobile security information is collected individually, the Internet being the main source. The academic curricula did not significantly improve the students' knowledge and behaviour in regard with mobile devices' security. There is still room for security training in the university's curriculum.

Table 2 The respondents' point of view in regard with information security education

Assertions about education	Frequency
Everyone should receive information on information security	49%
Employees of companies need to have knowledge of information security	14%
Information security must be taught in schools	12%
Everyone should be documented about the security of information	22%
Education in the field is not required if the security software is used	1%
Education in the field is only needed by IT specialists	2%

Regarding the measures of security used by the subjects and also the reasons why they wouldn't use them we obtained the following results: 69% claim that they are using anti-virus software, 12% firewall, 8% software anti-spam and only 6% are not using any security methods.

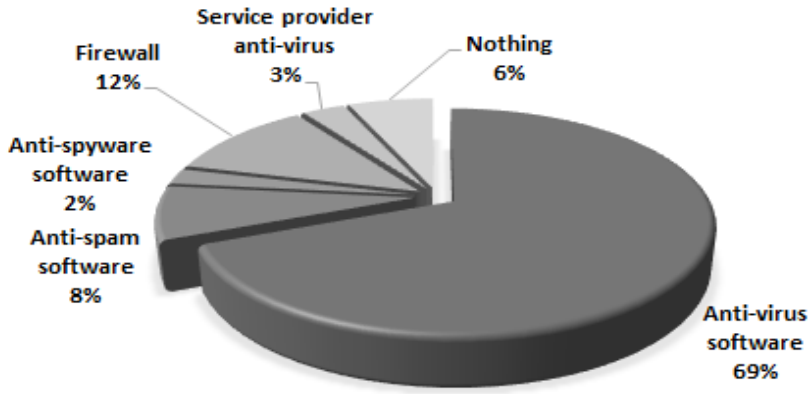

Figure 5. Security measures implemented on the computer/telephone

Considering the data and information security coverage the respondents indicated as the most used protection measures - backup files (52%), periodically change of the passwords (30%) and encryption of important files (12%). The respondents' answers focus more on laptops than smartphones that reflecting the connection they make between laptops (computers) and IT threats being less aware on mobile security issues. The students' answers did not indicate specific smartphones' security measures.

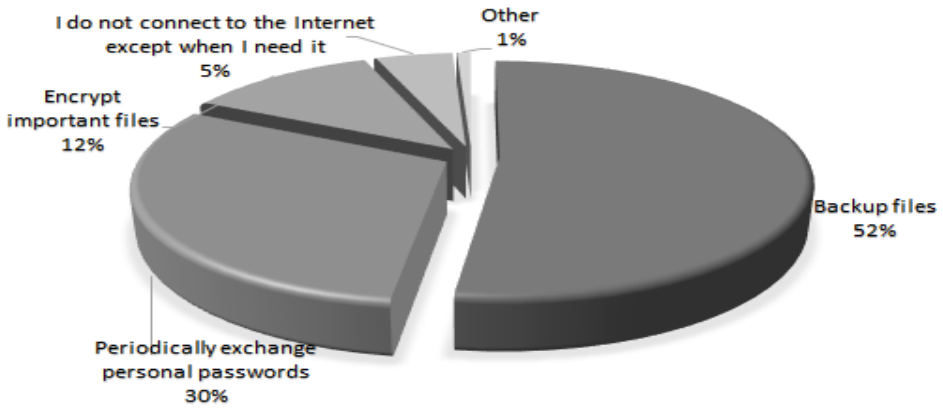

Figure 6. Security measures to protect data

The respondents indicated their reasons for not using security measures: 33% believe that setting the security system is too complicated, 32% consider that the updates and backups imply complex software knowledge, 22% think it's too expensive, 13% don't feel the need. Even if we expected the costs to be reported as the top obstacle it can be seen that the situation is quite alarming, the respondents' answers indicated insufficient knowledge and skills.

Table 3 Why did you not use security measures?

Reasons for security measures	No. of respondents	%
It costs money	40	22%
Their setting is complex	60	33%
Update, back-up settings involve complex software	57	32%
I do not feel the need for security measures	23	13%

The students' opinion is that the most important disadvantages of the security measures are: the need of special technical installation knowledge (37%) and the cost (36%).

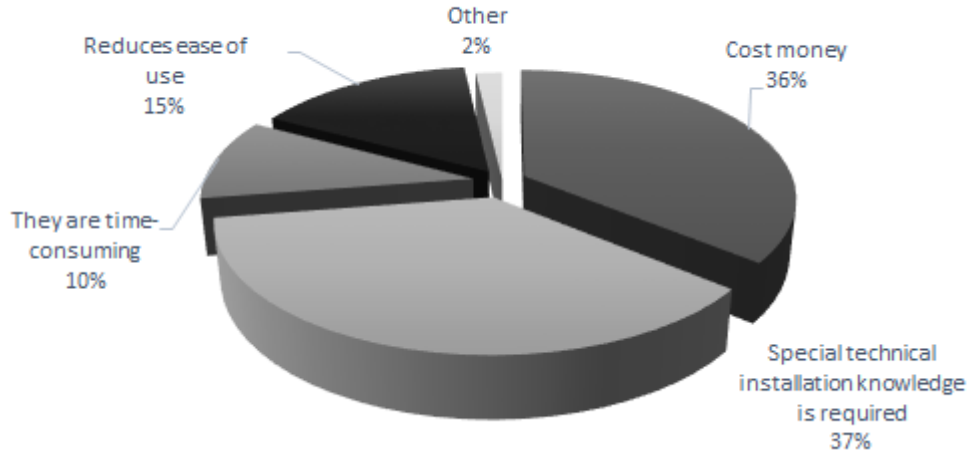

Figure 7. Disadvantages of security measures

Questioning about web surfing students placed socializing on the first place (93%), the e-mail coming up next 87%. Also, many subjects search on the Internet for professional information 73%, the online shopping was voted by 71%, lifestyle and hobbies covered 69% of the responses, news only 62%. It is not surprising that socialization and e-mail are the first two preferences being in line with the international surveys on the same topic, indicating them as the main preference of young people. The same preferences were revealed the authors' survey in 2017.

Table 4. Areas of Internet usage

Internet usage	No. of respondents	%
Socialization	168	93%
E-mail	157	87%
Get professional information	132	73%
Shopping online	127	71%
Get information about hobbies, lifestyle	124	69%
View news	112	62%
Get information about jobs	96	53%
Download music	94	52%
Online banking	74	41%
Download video	66	37%
Online games	50	28%
Download software	43	24%
Other	7	4%

We investigated the type of security incidents affected the students' mobile devices in the last 2 years. The virus infection was the main issue; 116 of the respondents (out of 180) experienced virus infection and, surprisingly, 30 declared never had to deal with this kind of infections. There is an evident contradiction in the respondents' answers. Taking into consideration that 26% of the respondents are not sure if they use good security measures and 13% think they are not using enough security measures we conclude that part of these 30 of respondents could be subjects of malware attacks and they are not aware of it.

Table 5. Security incidents in the last 2 years

Types of security incidents	No. of respondents	%
Unauthorized access to data	15	8%
Virus infection	116	64%
Fraud one-click	0	0%
Defamation on the Internet	2	1%
Phishing	2	1%
Password sniffing	9	5%
Spyware infections	6	3%
I did not have such problems	30	18%

The last question "Whom are you asking for help when you have a security issue?" disclosed the following results: 47% consider that they can solve any problem on their own and 36% would seek the help of an IT specialist.

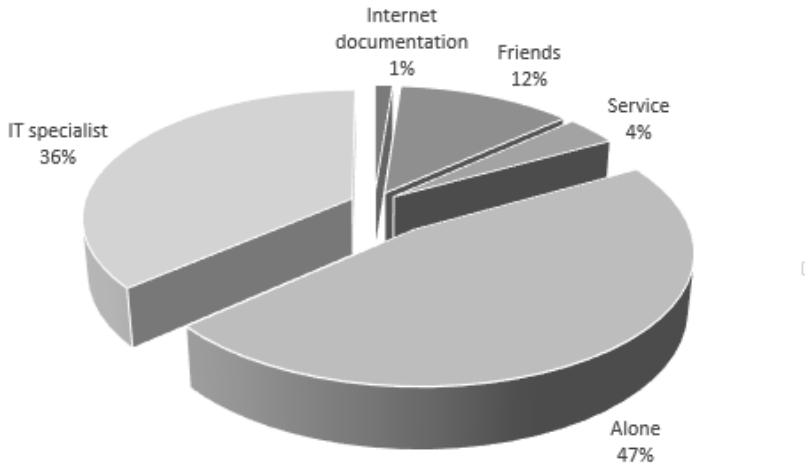

Figure 8. Whom are you addressing for help when you have a security issue?

Following the questions representing the initial starting point of our investigation the authors can conclude that:

- The students are daily users of laptops and smartphones, and less oriented towards tablets and other mobile devices (like cell phone, PDA, MP3Player).
- The producer, the price and the operating system are the main criteria for purchasing a mobile device while the connectivity and the service system are less important.
- The most used security measures for laptops are anti-virus and firewall software along with the periodically password change and data backup. The students did not indicate specific smartphones' security measures.
- The complexity of the software, complicated settings and difficulties in performing updates are the causes for no security measures' use. These reflect insufficient skills and information in regard with IT issues.
- Socializing is the most preferred online activity.
- The virus infection is the most frequent incident among the online users.
- For the security incidents and security measures the respondents focus more on laptops issues than other mobile devices that reflecting insufficient awareness and knowledge on mobile security threats.

5. Conclusions

The mobile wave has already impacted the individuals' life and behaviour and also the companies' IT environment. BYOD is the companies' response to the employees' device preferences and financial coordinates in regard with mobile

devices integration in the business activities (as a result of the employees' preferences for these kind of devices). The BYOD brings a new paradigm, affects the companies' culture and business activities and IT environment. The mobile security threats increase the companies' risk exposure and requires new integrated security policies and, as a main frame, a threat intelligent program.

The authors' empirical study aimed at providing an in-depth understanding of the accounting students' profile as mobile devices' users and their knowledge and awareness in regard with mobile security threats. The study's findings reflect the students' insufficient information in regard with mobile devices features and security issues. The respondents' security knowledge is linked more on computers (laptops) and less on other mobile devices. This is the result of the limited IT lectures and seminars in the curriculum and the insufficient focus on mobile devices' use in the accounting profession. Students should understand the smartphones, for example, as complex devices providing diverse features, not limited to communication with friends and Internet information searching.

There is significant room for the students' behaviour improvement in regard with mobile devices' use and security awareness.

The objective of the authors' study was to address some of the research gaps on mobile devices' security and to discuss practical implications in regard with the academic curriculum and students' training on information security. The paper aims to raise awareness on the insufficient knowledge of the mobile devices' users on security threats affecting the companies' information security in the context of the BYOD trend.

Acknowledgements

The present paper was presented in the 13th International Conference Accounting and Management Information Systems – AMIS 2018, Bucharest, Romania. The present paper integrates the suggestions and feedbacks of the researchers participating at the conference.

References

Androulidakis, I. (2016) *Mobile phone security and forensics*, Springer International Publishing, Switzerland

Check Point Research Team (2016) "An in-depth look at the Gooligan Malware campaign", [Online] Available at: http://blog.checkpoint.com/2016/12/13/depth-look-gooligan-malware-campain/ (Accessed: 10 December 2017)

Dahlberg, T., Guo, J. & Ondrus, J. (2015) "A critical review of mobile payment research", *Electronic Commerce Research and Applications*, no.14, 265-284

Dimensional Research (2014) "The impact of mobile devices on information security: A survey of IT and security professionals", [Online] Available at: https://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report2013.pdf (Accessed: 10 December 2017)

Dimensional Research (2017) "The growing threat of mobile device security breaches. A global survey of security professionals", April 2017. [Online] Available at: blog.checkpoint.com/wp-content/uploads/2017/04 /Dimensional_Entreprise-Mobile-Security-Survey.pdf (Accessed: 27 October 2017)

Gartner (2017) "Gartner says worldwide sales of smartphones grew 9 percent in the first quarter of 2017", [Online] Available at: http://www.gartner.comnewsroom/ id/3725117 (Accessed: 22 February 2018)

Grant Thornton (2013) "Social media risks and rewards", [Online] Available at: www.grantthorton.in/globalassets/1.-member-firms/india/assets/pdfs/adv-social-media-survey.pdf (Accessed: 20 October 2017)

Kearns, G. (2016) "Countering mobile device threats: A mobile device security model", *Journal of Forensic and Investigative Accounting*, vol. 8, no. 1: 36-48

Hautala, L. (2016) "How to tell if your Android phone has the HummingBad malware", [Online] Available at: https://www.cnet.com/how-to/ hummingbad-how-to-tell-if-your-android-phone-has-a-bad-case-of-malware/ (Accessed: 20 October 2017)

Information Security Media Group (2015) "The state of mobile security maturity. Findings from the ISMG survey sponsored by IBM", [Online] Available at http:// static.cio.nl/downloads/ The_State_of_mobile_security_maturity.pdf (Accessed: 12 December 2017)

ISACA (2016) "Mobile computing device threats, vulnerabilities and risk factors are ubiquitous", *ISACA Journal*, vol. 4: 1-5 [Online] Available at:https://www.isaca.org/Journal/archives/2016/volume-4/Documents/Mobile-Computing-Device-Threats-Vulnerabilities-and-Risk-Factors-Are-Ubiquitous_joa (Accessed: 20 January 2018)

Kaspersky (2015) "Kaspersky security bulletin 2015. Overall statistics for 2015", [Online] Available at: https://securelist.com/Kaspersky_security-bulletin-2015-overall-statistics-for-2015/73038 (Accessed: 20 October 2017)

Kassel, P., Allan, K. (2015) "Creating trust in the digital world. EY's Global Information Security Survey 2015", E&Y [Online] Available at: webforms.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf (Accessed: 15 February 2018)

Kulwer, W. (2013) "Key findings from the CCH", [Online] Available at: https://www.cchgroup.com/Leaders (Accessed: 15 February 2018)

La Polla, M., Martinelli, F. & Sgandurra, D. (2013) "A survey on security for mobile devices", *IEEE Communications Surveys and Tutorials*, vol. 15, no.1: 446-471

Madan, A., Muppidi, S., Patel, N. & Buecker, A. (2013) "Securely adopting mobile technology innovations for your enterprise Using IBM Security Solutions", IBM [Online] Available at: www.redbooks.ibm.com /redpapers/ pdfs/redp4957.pdf (Accessed: 15 February 2018)

McEnaney, M. (2016) "Cybersecurity concerns in a BYOD word", [Online] Available at: http://www.entreprisemobilityexchange.com/eme-byod/ articles/cybersecurity-concerns-in-a-byod-world (Accessed: 20 February 2018)

NIST (2013) "Guidelines for managing the security of mobile devices in the enterprise", NIST Special Publication 800-124 [Online] Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP (Accessed: 15 February 2018)

PriceWaterhouseCoopers (2017) "The Global State of Information Security Survey 2017" [Online] Available at: www.pwc.com/sg/en/risk-assurance/assets/ gsiss/global-state-of-information-security-survey-2017-sg.pdf (Accessed: 15 January 2018)

Smith, E. (2017) "Tablet market falls 9% in Q4 2016 with Apple, Samsung Down Double Digits", [Online] Available at: https://www.strategyanalytics.com/ strategy-analytics/news/strategy-analytics-press-releases/strategy-analytics-press-release/2017/02/02/tablet-market-falls-9-in-q4-2016-with-apple-samsung-down-double-digits#.Wq92fClaToF (Accessed: 15 February 2018)

Statista (2017) "The Statistics Portal", [Online] Available at: https://www.statista.com/ topics/841/tablets/ (Accessed: 25 January 2018)