Cloud Accounting as a Factor in Protection from Cyber Attacks and Theft of Accounting Data

PhD Valentina Vinšalek Stipić & Mile Vičić
Business department
University of Applied Sciences "Nikola Tesla" in Gospić
Gospić, Croatia
vvs@velegs-nikolatesla.hr
mvicic@velegs-nikolatesla.hr

Abstract* - Incidents such as cyber-attacks are becoming more frequent in the business world. Cyber-attacks cause significant damage to the operations and accounting and financial data of companies. The question arises whether cloud accounting is the solution to reduce cyber-attacks and theft of accounting data. Many companies or individuals still do not trust cloud accounting. The problem of this research is the acceptance of accounting in the cloud by accounting staff and insufficient understanding of the benefits of working in the cloud to prevent cyber-attacks and theft of accounting data. Research is conducted among accounting professionals in Croatia, randomly distributed, via anonymous survey, where 183 responses were gathered. Statistical analysis of the collected data confirmed the set hypotheses, i.e. the frequency of cyberattacks is significantly statistically related to the method of data storage ($r = 0.807$; $p < 0,001$), and partially ($r = 0.199$; $p < 0,001$) to the method of authentication in accounting software and the method of creating a backup copy of accounting data.

***Keywords* - cloud accounting; cyber attacks; protection of accounting data; perception about cloud accounting**

I. INTRODUCTION

Today's competitive business environment forces fast-growing companies to constantly monitor progress, change business strategy and adapt to the risks of the business environment. Over the past decades, the role of information technology has changed significantly [1]. The advancement of cloud technology represents one of the biggest technological trends at the moment. The cloud is a platform for data availability anytime, anywhere, from almost any device that has an Internet connection [2]. The most famous term for cloud technology is the term cloud computing [3]. Cloud computing is computing resources that companies and users can access from remote locations via the Internet [4]. Such solutions occupy a very important place in the optimization and improvement of all business processes of the company. Like other business sectors, accounting has also embraced cloud technology solutions. Cloud accounting partly changes the nature of the accounting business, so the slow adoption of cloud accounting is expected. A significant resistance to working with accounting in the cloud is due to the loss of self-control over the company's accounting and financial data and the fear of hacker attacks and complete data loss [5]. The question arises as to the cause of frequent hacker attacks on accounting information systems and is business data sufficiently protected in cloud accounting? The answers to these questions were obtained through empirical research on a sample of 183 respondents, accounting employees in the Republic of Croatia. The aim of this research is to prove that the frequency of hacker attacks in accounting depends to a significant extent on the method of data storage and the method of authentication in accounting software.

II. CLOUD ACCOUNTING

The use of new information technology, such as cloud accounting, is a challenge for users (accountants) and companies, this is due to the constant evolution of technology and the frequent appearance of new technologies that appear every day. A big challenge is the technical language and its features. Some of the computer programs come in languages that users such as accountants cannot easily understand. Therefore, accountants must raise the level of training before use, to enjoy the benefits of cloud accounting. Another challenge is the difficulty of adapting to such frequent changes [5]. Some workers may lose interest and this may reduce work morale. Cloud computing has been compared and equated to the industrial revolution. However, its transformational nature is associated with significant security and privacy risks [6]. Cloud accounting gives accountants instant and mobile access to financial information and completely changes the way accountants work. Because SMEs can quickly respond to changes in technology demand, they can be the fastest adopters of cloud accounting services [7]. Companies whose employees work remotely may also prefer cloud accounting for convenience and availability, companies that cannot ensure data security and companies that want to avoid all potential physical accidents with technology, destruction of hard drives, and thus accounting data [8].

A. Advantages and disadvantages of cloud accounting

Traditional accounting programs and cloud accounting solutions have their advantages and disadvantages. The use of cloud accounting in business operations brings many advantages, the most prominent of which are [9]:

Lower costs – the price paid for using cloud accounting services is generally lower than traditional accounting

programs. The user does not pay installation fees or have to purchase new updates in case accounting rules or tax regulations change because the monthly or annual subscription costs include the cost of updates. Also, the user doesn't have the costs of purchasing hardware, licenses for antivirus programs and operating systems, and server maintenance costs, as is the case with traditional accounting programs. All you need is a stable internet connection.

Security – by using cloud accounting, there is no risk of destruction or theft of hardware and software. All data is stored away from the company on secure servers that are under the control of the company that manages it. Such companies usually have stronger antivirus programs, which makes financial data relatively safer in the cloud than stored locally, on the user's computer.

Availability – in cloud accounting, data is always available to all authorized users, wherever they are. All that is required is a stable internet connection and a device from which to access the software. This is especially important in companies that prefer remote work. In addition, it is very easy to add new users - by setting up an authorized profile and password, which facilitates collaboration and because everyone can see the relevant financial information at any time.

Up to date – the latest and updated versions of the software that the cloud accounting service provider upgrades are immediately available to the user, which is especially important when it comes to changes in accounting rules and tax regulations. In this way, the user saves time and focuses on his business, knowing that these tasks will be done for him by the service provider.

Automatic Data Backup and Restore – With cloud accounting, there is no need to manually back up accounting data because the software does it automatically, reducing the possibility of human error and forgetfulness.

The advantages of cloud accounting overshadow the disadvantages, however, there are potential risks that users of this software may encounter, some of which are:

Internet connection - cloud accounting requires a constant and strong internet connection; cloud accounting software does not work well at low speed. Internet speed depends on the line capabilities of the user's location and can vary from place to place, which is a big disadvantage.

Security – as cloud services becomes more popular, data becomes more and more the target of attacks, which is why some businesses such as banks benefit more from keeping their sensitive financial data "in house" than with a cloud computing service provider.

Reduced control – loss of control over the accounting software, which is completely managed by the service provider, is one of the main problems of cloud accounting application. Maintaining the software in the event of failure or downtime and performing application updates is the sole responsibility of the service provider, not the user, which makes companies afraid of losing control over accounting data.

B. Cloud accounting features

The greatest impact of IT on accounting is the ability of companies to develop and use computerized systems for up-to-date recording of accounting data. Most popular accounting systems can also be tailored to specific industries or businesses [10]. This allows businesses to create individual reports quickly and easily for management and/or decision-making. Second, the advantages of computerized accounting systems can be summarized as follows: increased functionality, improved accuracy, faster processing, better external reporting. However, today's accountants need to be familiar with software tools that can help them perform accounting functions more efficiently.

III. CYBERSECURITY IN CLOUD ACCOUNTING

Cyber-attacks are deliberate attempts to disrupt, steal, alter or destroy data stored in IT systems. Attacks are often motivated by profit and many intruders are technically sophisticated and have a nuanced understanding of system functioning [11]. Cybersecurity has become more urgent as malicious actors develop sophisticated techniques. But quantifying the risk or resilience of institutions to cybersecurity incidents is difficult [12]. The lack of standardized data on such incidents and company control is a challenge for the protection of accounting systems, but above all, companies are responsible for their own security against cyber-attacks [13].

A. Forms and effects of cybersecurity incidents in accounting

Like any new technology, cloud computing is subject to security threats and vulnerabilities, including network threats, information threats, and underlying infrastructure threats [14] in the form of cyber-attacks. Attack tactics include finding weaknesses in software to get into IT systems, redirecting to fake email servers to steal passwords, redirecting to fake websites that infect users with malware, and software that wipes users from their own systems. Detailed data on the frequency, tactics and results of cybersecurity incidents are scarce. Data is scarce in part because financial firms avoid reporting incidents due to reputational concerns [15]. Concerns about cyber-attacks are growing [16]. However, an effective review creates a basis for advancing knowledge [17]. It is necessary to synthesize studies related to cyber security in the field of accounting and auditing. The number and severity of cyber threats have been unprecedented in recent years, and successful cyber-attacks are regularly reported [18]. The costs of the consequences of cyberattacks are enormous; therefore, cyber security risk management is considered extremely important for organizations [18]. In this regard, Hausken (2006) states that the intensity of cyber warfare has increased through the Internet revolution. [19]. Also, Gordon et al. (2003) suggest that the Internet revolution has

dramatically changed the way individuals, businesses, and government communicate and do business. They concluded that the widespread interconnection of industrial branches increased the vulnerability of computer systems [20]. Gansler and Lucyshyn (2005) state that the growing dependence of the public and private sectors on Internet-based technologies and networks for their financial management systems comes at a price, and that price is increased vulnerability [21]. Therefore, in 2016, the financial services sector was attacked more than any other industry [22]. In this global information society, where information travels through cyberspace, it is crucial to manage it effectively [23]. Effective management, on the other hand, is linked to awareness of increasing vulnerabilities, such as cyber threats and information warfare. Effective cyber security management is essential. Investments in cyber security are profitable if the benefits of additional activities for information security exceed its costs [24]. Although cyber security does not always benefit the organization, cyber-attacks are one of the main risks that organizations must control [25]. Earlier review studies related to this topic discussed research opportunities in IT and internal auditing [26] and the impact of information security events on the stock market [27]. Based on the above arguments, it is crucial to synthesize the previous literature related to cybersecurity and identify the research streams of the articles under review.

B. Effects of cyber security deficiency in accounting

Cyber security is often used as an analogous term for information security. However, cyber security is not necessarily only the protection of cyberspace itself, but also the protection of those who function in cyberspace and any of their assets that can be accessed through cyberspace [28]. Cyber security encompasses technologies, processes and controls designed to protect systems, networks and data from cyber-attacks. Effective cyber security reduces the risk of cyber-attacks and protects societies, organizations and individuals from unauthorized exploitation of systems, networks and technologies. Cyber security is an umbrella concept that encompasses information security and information assurance [29]. Thus, cyber security includes the protection of information that is evaluated and transmitted through any computer network [24].

While cybersecurity threats impose direct costs on businesses, incidents in cyberspace can also pose a broader risk to financial stability. Financial companies work in complex networks and rely on electronic transactions, often representing rapid management in time. They are digitally connected to other and non-financial entities, including third-party service providers. However, defending decentralized networks against cyber-attacks with many entry points can be extremely difficult [30]. Cloud has already conquered almost every business area, but it seems that the accounting profession is sceptical about this new model. According to some accountants, cloud-based software is an obvious threat [31]. Of course, it can be seen as a threat to those unwilling to adapt and clearly understand the benefits involved. Therefore, it is necessary to pay attention to cybersecurity in accounting. In the absence of cybersecurity in accounting, three effects are possible [32]:

Lack of interchangeability – the financial services industry relies on a robust IT infrastructure to complete transactions and move payments. In many financial networks, several companies or central e-services servers serve as hubs. Their services will be difficult to replace if lost or interrupted. Problems at key hubs can increase stability concerns. Policies that encourage the expansion of the financial system can reduce those risks. Regulators should consider such policies.

Loss of trust – cyber-attacks often target customer account information and financial assets. Most of these attacks were one-off events, injuring only the victim and their clients. However, the excessive occurrence of cyber theft can cause a wider loss of trust. For example, after the cyber theft of customer names, credit card information and phone numbers of a retail chain, many clients call or visit their banks to ask for information about the presence of their money in their accounts. Then many customers cancel their credit cards, which can cause a banking crisis.

Lack of data integrity – financial data integrity is critical. Many financial markets operate in real time. Financial companies need a robust data backup that can be recovered shortly after a cybersecurity incident. However, there has been a trade-off between rapid recovery and ensuring that recovered data is secure, accurate and does not spread the cyber risks, especially for markets that process orders quickly. Data corruption can disrupt market activity and can be difficult to initiate or recover from.

IV. GOALS AND HYPOTHESES OF RESEARCH

The previously presented theoretical approach shows the importance of cybersecurity in accounting. This research emphasizes the development of cybersecurity in accounting, ways of storing data and protecting them from possible cyber-attacks. Therefore, this paper tried to investigate the correlation between the frequency of cyber-attacks in accounting with the method of data storage, then with the method of authentication in accounting software, and the intensity of cloud accounting protection against cyber-attacks. Accordingly, the following research hypotheses were set:

H_1 – The frequency of cyber-attacks is statistically significantly related to the method of data storage

H_2 – The frequency of cyber-attacks is statistically significantly related to the method of authentication in the accounting software

H_3 – The frequency of cyber-attacks on accounting is statistically significantly related to the way accounting data is backed up

V. METHOD OF THE RESEARCH

Data for the implementation of this empirical research were collected through a survey on a sample of 183 accounting employees in the Republic of Croatia. The survey was conducted anonymously, through invitation for participation within accountant's professional association groups on social and business networks in March 2022 and by invitation in January 2023. The survey consisted of 20 questions, divided into three groups, including general

information about examinee, familiarity with cloud accounting and cyber security application, it used a Likert measuring scale with five intensities, from which the following variables were defined:

a) independent variables, which were obtained by the weighted average rating of the responses from the survey questionnaire:

X_1 – data storage mode (DataA)

X_2 – authentication mode (Authent)

X_3 – data backup mode (ProtectA)

b) dependent variable frequency of cyber-attacks on accounting data (CyberA) => more than three times a year; two to three times a year; once a year; once every few years; never.

The conducted research showed a correlation of the frequency of attacks on accounting information systems with the methods of storing accounting data, the methods of authentication in accounting software and the method of data backup. To prove the set hypotheses, the statistical methods of correlation and regression analysis were applied using the SPSS 26.0 statistical program. The obtained results of the statistical data processing are shown below.

VI. RESULTS OF THE RESEARCH

A total of 183 accountants from Croatia took part in the research, of which 86.9% were female, while the majority were 31 to 45 years old (48.6%), followed by 18 to 30 years old, which made up 26.2% of respondents. and the rest (25.1%) to respondents aged 46 to 65. According to the level of education, 40.4% of the respondents have a higher vocational education, followed by a bachelor's degree in 30.1%, while 26.2% of them have a secondary vocational education and the rest are university specialists or Doctor of Science. The structure of respondents according to the level of work experience in accounting is shown in table I.

TABLE I: YEARS OF WORKING EXPERIENCE IN ACCOUNTING

Work experience in years	Number of respondents	%
until 2	48	26,2
3 to 5	27	14,8
6 to 10	25	13,7
11 to 15	29	15,8
16 and over	54	29,5

Performed simple regression analysis between the observed variables (DataA and CyberA) shows a strong significant linear correlation between the frequency of cyberattacks and the way data is stored in accounting. From Table II., a correlation coefficient of 0.807 is visible, while the F ratio is significantly higher than the theoretical value (65.2% of variations in the dependent variable are the result of variations in the independent variable), with a significance level of 0.05 and the number of degrees of freedom 1.182, it can be concluded that the first hypothesis is confirmed. Also, Durbin-Watson is 2.070 which means no existence of autocorrelation of relationship errors.

TABLE II. STATISTICAL RELATIONSHIP OF THE FREQUENCY OF CYBER ATTACKS AND THE METHOD OF STORAGE OF ACCOUNTING DATA

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	,807[a]	,652	,650	,663
a. Predictors: (Constant), DataA b. Dependent Variable: CyberA				

By analysing the statistical connection between the frequency of cyber-attacks and the method of authentication in the accounting software shown in Table III. a positive but weak significant correlation is visible ($r = 0.199$; $p < 0,001$). The coefficient of determination R2 is closer to zero than to one, therefore we cannot talk about good representativeness of the model, with a significance level of 0.05 the second hypothesis is partially confirmed, there is a weak positive correlation between the frequency of cyber-attacks and authentication in accounting software.

TABLE III. STATISTICAL RELATIONSHIP OF THE FREQUENCY OF CYBER ATTACKS AND THE METHOD OF AUTHENTICATION IN ACCOUNTING SOFTWARE

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	,199[a]	,040	,034	1,101
a. Predictors: (Constant), Authent b. Dependent Variable: CyberA				

Below, from table III. is visible a positive but weak statistical correlation between the frequency of cyber-attack and the method of backup of accounting data. Durbin-Watson has a value close to 2, which indicates the absence of autocorrelation of relational errors. With a significance level of 0.05 and from the coefficient of determination, it is visible that 40% of the variations of the dependent variable are the result of variations of the independent variable. The obtained results partially confirm the third hypothesis.

TABLE IV: STATISTICAL RELATIONSHIP OF THE FREQUENCY OF CYBER ATTACKS AND THE BACKUP METHOD OF ACCOUNTING DATA

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	,199[a]	,040	,034	1,101
a. Predictors: (Constant), ProtectA b. Dependent Variable: CyberA				

The collected responses to the conducted survey revealed that 60.9% of respondents use a username and password for authentication to work in accounting software, and 20.7% of respondents use only a password. The fact that 8.7% of respondents do not have any security authentication for accessing accounting data is worrying, which can be considered inadequate protection of accounting data. It is also worrying that 19.6% of respondents save a backup copy of accounting data locally, that is, on the same computer on which they use the accounting program.

VII. CONCLUSION

By conducting empirical research on a sample of 183 accounting employees in Croatia, this research wanted to prove that the frequency of cyber-attacks in accounting depends to a significant extent on the method of data storage and the method of authentication in accounting software. Statistical analysis of the collected data confirmed the set hypotheses, and it can be concluded that the frequency of cyberattacks is significantly positively statistically related to the method of data storage ($p = 0.807$; $p < 0{,}001$) and there is a weak positive correlation between cyberattacks and authentication methods in accounting software and the method of creating a backup copy of accounting data ($r = 0.199$; $p < 0{,}001$). Earlier research showed a significant correlation between cyber-attacks and the age structure of accounting employees and their level of education, that is, older accounting employees with a lower level of education are more significantly exposed to cyber-attacks [33, 34]. This research led to the realization that 20.7% of respondents use only a password for authentication to work in accounting software, but a more worrying fact is that 8.7% of respondents do not have any security authentication for accessing accounting data, which can be considered inadequate protection of accounting data. It is also alarming that 19.6% of respondents save a backup copy of accounting data locally, that is, on the same computer on which they use the accounting program. This research confirmed that more complex authentication and data storage outside the location of the accounting program itself reduces the possibility of cyber-attacks in accounting. Also, storing accounting data on the cloud significantly reduces the possibility of cyber-attacks.

The shortcomings of this research are reflected in the impossibility of identifying the total number of accountants in the Republic of Croatia in relation to the number of respondents included in this research. Also, due to the unavailability of data, it was not possible to compare the obtained data on the frequency of cyber attacks in the Republic of Croatia (data obtained through this research) with the frequency of cyber attacks in other countries. It is recommended to repeat the research on a more representative sample with a more detailed investigation of the type of cyberattacks and their frequency.

REFERENCE

[1] F. Altınay, G. Dagli, Z. Altınay, „The Role of Information Technology in Becoming Learning Organization," Procedia Computer Science, 102, 2016, pp. 663–667.

[2] P. Kumar Paul and M. K. Ghose, „Cloud Computing: Possibilities, Challenges and Opportunities with Special Reference to its Emerging Need in the Academic and Working Area of Information Science," Procedia Engineering, 38, 2012, pp. 2222–2227.

[3] N. Bačanin Džakula and I. Štrumberger, "Klaud računarstvo," Beograd: Univerzitet Singidunum, 2018.

[4] N. Ž. Budimir, "Primjena oblak računarstva u računovodstvo," Putokazi: Sveučilište Hercegovina, 7(1), 2019, 137–148.

[5] V. Vinšalek Stipić and M. Vičić, "An analysis of accountants' resistance to cloud accounting," Journal of Economic and Business Issues, 2(2), 2022, pp. 15–23.

[6] N. Kshetri, „Privacy and security issues in cloud computing: The role of institutions and institutional evolution," Telecommunications Policy, 37(4–5), 2013, pp. 372–386.

[7] C. Christauskas, and R. Miseviciene, "Cloud–Computing Based Accounting for Small to Medium Sized Business," Engineering Economics, 23(1), 2012, pp. 14–21.

[8] T. Khanom, "Cloud Accounting: A Theoretical Overview," IOSR Journal of Business and Management, 19(6), 2017, pp. 31–38.

[9] P. A. Abdalla and A. Varol, "Advantages to Disadvantages of Cloud Computing for Small-Sized Business," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1–6.

[10] O. Dimitriu and M. Matei, „Cloud Accounting: A New Business Model in a Challenging Context," Procedia Economics and Finance, 32, 2015, pp. 665–671.

[11] J. Jang-Jaccard and S. Nepal, „A survey of emerging threats in cybersecurity," Journal of Computer and System Sciences, 80(5), 2014, pp. 973–993.

[12] D. P. David, L. Maréchal, W. Lacube, S. Gillard, M. Tsesmelis, T. Maillart and A. Mermoud, „Measuring security development in information technologies: A scientometric framework using arXiv e-prints," Technological Forecasting and Social Change, 188, 2023, 122316.

[13] White House. Critical Infrastructure Security and Resilience. Presidential Policy Directive (21). Washington: White House, Feb. 12, 2013. https://www.whitehouse.gov/ the-press-office/2013/02/12/ presidential-policy-directive-critical-infrastructure-security-and-resil

[14] R. M. Jabir, S. I. R. Khanji, L. A. Ahmad, O. Alfandi and H. Said, "Analysis of cloud computing attacks and countermeasures," 2016 18th International Conference on Advanced Communication Technology, PyeongChang, Korea (South), 2016, pp. 1–1.

[15] Office of Financial Research. 2015 Financial Stability Report. Washington: OFR, Dec. 15, 2015.

[16] Symantec Corp. Internet Security Threat Report. Herndon, Va.: Symantec, April 2016.

[17] J. Webster, and R. Watson, "Analysing the past to prepare for the future: writing a literature review", MIS Quarterly, 26(2), 2002, pp. 13–23.

[18] M. S. Islam, N. Farah, and T. S. Stafford, "Factors associated with security/cybersecurity audit by internal audit function: an international study", Managerial Auditing Journal, 33(4), 2018, pp. 377–409.

[19] K. Hausken, "Income, interdependence, and substitution effects affecting incentives for security investment", Journal of Accounting and Public Policy, 25(6), 2006, pp. 629–665.

[20] L. A. Gordon, M. P. Loeb and W. Lucyshyn, "Sharing information on computer systems security: an economic analysis", Journal of Accounting and Public Policy, 22(6), 2003, pp. 461–485.

[21] J. Gansler, and W. Lucyshyn, "Improving the security of financial management systems: what are we to do?", Journal of Accounting and Public Policy, 24(1), 2005, pp. 1–9.

[22] The World Bank (2018), "Financial sector's cybersecurity: regulations and supervision", available at: http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf

[23] J. W. Lainhart, "COBIT™: a methodology for managing and controlling information and information technology risks and vulnerabilities", Journal of Information Systems, 14(1), 2000, pp. 21–25.

[24] A. L. Gordon, and P. M. Loeb, "Managing Cybersecurity Resources: A Cost–Benefit Analysis," New York: McGraw Hill, 2006.

[25] E. Amir, S. Levi, and T. Livne, "Do firms underreport information on cyber-attacks? Evidence from capital markets", Review of Accounting Studies, 23(3), 2018, pp. 1177–1206.

[26] M. Weidenmier and S. Ramamoorti, "Research opportunities in information technology and internal auditing", Journal of Information Systems, 20(1), 2006, pp. 205–219.

[27] G. Spanos and L. Angelis, "The impact of information security events to the stock market: a systematic literature review", Computers and Security, 58, 2016, pp. 216–229.

[28] Von Solms, R. and van Niekerk, J. (2013), "From information security to cyber security", Computers and Security, Vol. 38, pp. 97-102.

[29] Gyun No, W. and Vasarhelyi, M.A. (2017), "Cybersecurity and continuous assurance", Journal of Emerging Technologies in Accounting, Vol. 14 No. 1, pp. 1-12.

[30] E. Rosengren, "Cyber Security and Financial Stability." Speech to the Basel Committee on Banking Supervision, Cape Town, Jan. 30, 2015, available at: www.bostonfed.org/news/ speeches/rosengren/2015/013015/ 013015text.pdf

[31] CCH. Cloud Computing - A matter of survival for the accounting industry. CCH Research Report. 2013, available at: http://www.cchifirm.com/why_ifirm/cloud-computing-and-the-accounting-industry

[32] Office of Financial Research. 2022 Financial Stability Report. Washington: OFR, available at:
https://www.financialresearch.gov/reports/

[33] Boban, M., Vinšalek Stipić, V. & Grabić, J. (2018). Infuence of IT on Accounting Practice and Exposure to Cyber Attacks, 2nd ISIP 2018, Symposium on Information Security and Intellectual Property, September 13 – 15, 2018. in Split – Supetar in the frame of the 26th International Conference on Software – SoftCom 2018, No. 1570485850, available at: https://www.bib.irb.hr/996659

[34] Boban, M. & Vinšalek Stipić, V. (2020), „Cloud accounting – security, reliability and propensity of accounting staff to work in cloud accounting.", 28th International Conference on Software, Telecommunications and Computer Networks - SoftCOM 2020, September 17 – 19, 2020. Hvar, No. 1570674979, available at: https://www.bib.irb.hr/1091437