Interdisciplinary Description of Complex Systems 19(3), 375-390, 2021

CYBER-SECURITY RISKS ASSESSMENT BY EXTERNAL AUDITORS

Tran Nguen Bao Ngo[1] and Andrea Tick[2,*]

[1]University of Danang
Danang, Vietnam

[2]Óbuda University
Budapest, Hungary

DOI: 10.7906/indecs.19.3.3
Regular article

Received: 17 July 2020.
Accepted: 14 May 2021.

ABSTRACT

The rise in cybercriminal activities in recent years has sparked concern about the costs of technological advancement and the growing reliance of humans on technology. The seriousness of this situation in the business world is indeed more noteworthy and more prominent than other areas, prompting many people to wonder how external auditors – who are responsible for identifying any accounting flaws – will respond to cybersecurity-affected businesses – the ones which can make an honest effort to mask and conceal their difficulties and challenges from their investors and stakeholders. Consequently, the aim of this study is to search whether external auditors focus harder on cybersecurity-attacked firms and businesses by charging higher audit fees. The study found a positive correlation between audit fees and breach employing a sample of 100 global small-, medium-sized, and large businesses. This indicates that external auditors find more risks and spend more effort while auditing cybersecurity-attacked businesses.

KEY WORDS

audit fees, Cybersecurity risks, OLS model

CLASSIFICATION

JEL: A29, C12, G30, Y80

*Corresponding author, η: Tick.Andrea@kgk.uni-obuda.hu; +36 1 6665261;
H-1084 Budapest, Tavaszmező street 15-17.

INTRODUCTION

Since the beginning of the 21st centuries, the world has been experiencing a large number of severe cyber criminals which demonstrates the fact about the growing dependence of human beings on the usefulness of technological advance. The severity of this situation in the business world is even greater and greater than other fields, which leads many people raise a question about the response of external auditors – the ones who are responsible for detecting any accounting faults – towards cybersecurity-attacked companies – the ones which can try their best to hide their difficulties from their investors and stakeholders. In the business world, the technological advance has been possessing a dominant position thanks to their supply of powerful managerial tools for each single organization when the majority of today operational procedures are accomplished with the help of information technology systems. Unfortunately, along with the development of the information technology systems, threats related to data and information security at companies and enterprises have appeared and evolved through time. Although the security risks have received the most concern from all companies with a lot of actions to protect themselves from data and information security attacks, the complete mitigation of vulnerabilities has been still unfeasible and the number of cyber-attacked companies has been increasing day by day. There are many evident facts that a cybersecurity attack can easily knock a big company down and no investors or stakeholders of a company expect any news about cybersecurity attack. As indicated in the efficient market theory of Fama [1] the stock market is the reflection of all investors' information about a company. Hence, the cyber-attacked company will have a tendency to hide any bad information or terrible consequences related to their cyber-attacks, which then leads people to feel curious about the role of external auditors in the case of auditing a cyber-attacked companies – whether external auditors are put under much pressure to detect any faults of these companies, which forces them to charge a higher fees for their higher auditing efforts.

Tempted from this current issue, this research is designed to answer the question whether external auditors will pay more attention to cyber-attacked companies to assure the credibility of their auditing opinions by charging higher audit fees to these companies. Using a sample of 100 global small, medium and big companies from Wharton Research Data Service, this study has proved that higher audit fees will be charged for cyber-attacked companies, which means that external auditors will pay more attention to audit these companies.

The remaining parts of this study are organized as follows. Firstly, the research demonstrates the current socio-economic background of cybersecurity as well as the general background information about audit fees and previous academic literature about the relationship between audit fees and cybersecurity risks, which then paves the way for the development of the hypotheses on the impact of audit security risk on audit fees. The following part illustrates the research method and the formation of the regression model. Finally, using a sample of 100 global small, medium and large companies, the study finds out that there is a positive relationship between audit fees and breach, which means that external auditors find more risks and exert more efforts when auditing the cybersecurity-attacked companies. The research draws conclusions as well and points out any limitations and makes several suggestions for future research.

LITERATURE REVIEW

SOCIO-ECONOMIC BACKGROUND OF CYBERSECURITY

The advent of Internet and the rapid revolution of information technology have brought a high degree of advantages to the human life. The presence of technology can be seen in any aspects of life and has become a lifeblood in both civilized society and the world of business. However,

it is the advance of technology which opens many rooms for cybercrime, and cybersecurity is among one of the most day-to-day struggling issues of every individual around the world. A report about Cyber Security of the European Commission [2] states that each single day experiences one million people becoming victims of cyber criminals, and there is one hacker attack of Internet-accessing computer in every 39 seconds [3].

In the business world, the picture of cybercrime is even gloomier due to the dependence of most current businesses on electronic data and computer networks for the sake of their daily operations, which then leads to the exposure of personal, confidential and competitive information to the hackers. Cyber criminals have knocked a lot of businesses down and shot them to the hell (e.g.: the hack of 77 million PlayStation Network accounts caused losses of $ 171 million while the site was down for a month in 2011; the exposure of 3 billion Yahoo user accounts knocked $ 350 million off Yahoo's sale price in 2014; the theft of 57 million Uber users personal information and 600 000 driver license numbers ruined Uber's both reputation and money in 2016; the show-up of 419 million - 540 million records of Facebook IDs and phone numbers in April and September 2019 is the most horrible scandal in Facebook history).

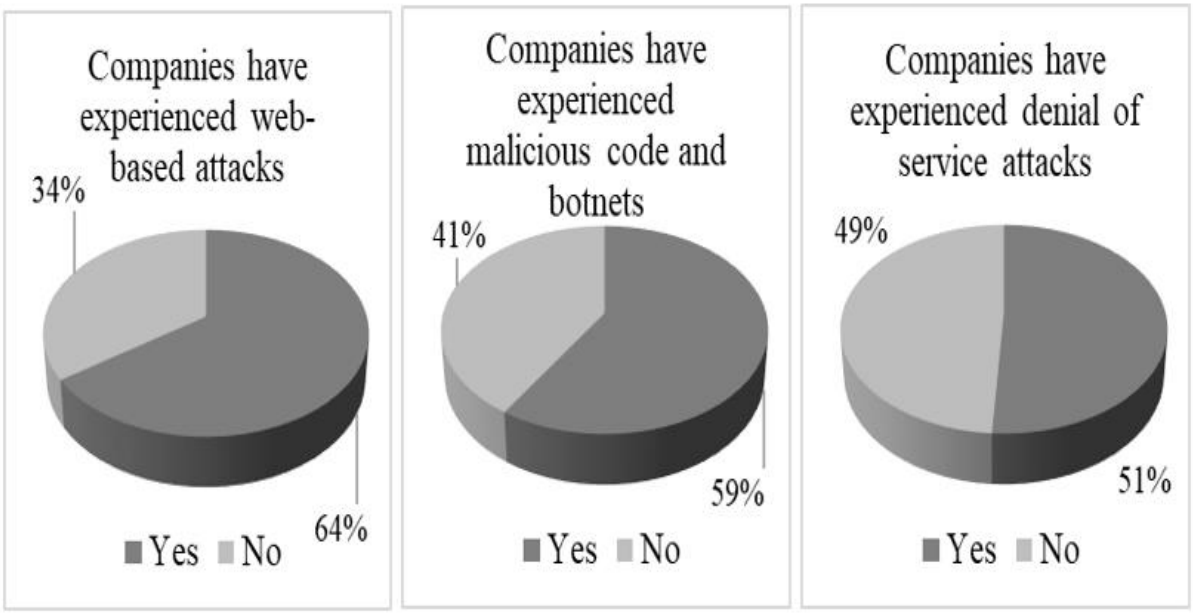

Figure 1. Cybercriminals in business world [4].

In fact, according to recent statistics, the business world has been in highly vulnerable to cyber-attacks these days. In 2018, "64 % of companies have experienced web-based attacks. 62 % experienced phishing & social engineering attacks. 59 % of companies experienced malicious code and botnets and 51 % experienced denial of service attacks." [4]; "68 percent of business leaders said their cybersecurity risks are also increasing" [5]; "Only 5 % of folders were protected" [6]; "3,813 breaches were reported through June 30, exposing over 4,1 billion records. Compared to the midyear of 2018, the number of reported breaches was up 54 % and the number of exposed records was up 52 %." [7]; "Worldwide spending on information security products and services will reach more than $ 114 billion in 2018, an increase of 12,4 percent from last year, according to the latest forecast from Gartner, Inc. In 2019, the market is forecast to grow 8,7 percent to $ 124 billion." [8]. Those impressive numbers actually have provoked an alarm about the severe risks of the world business's cyber security.

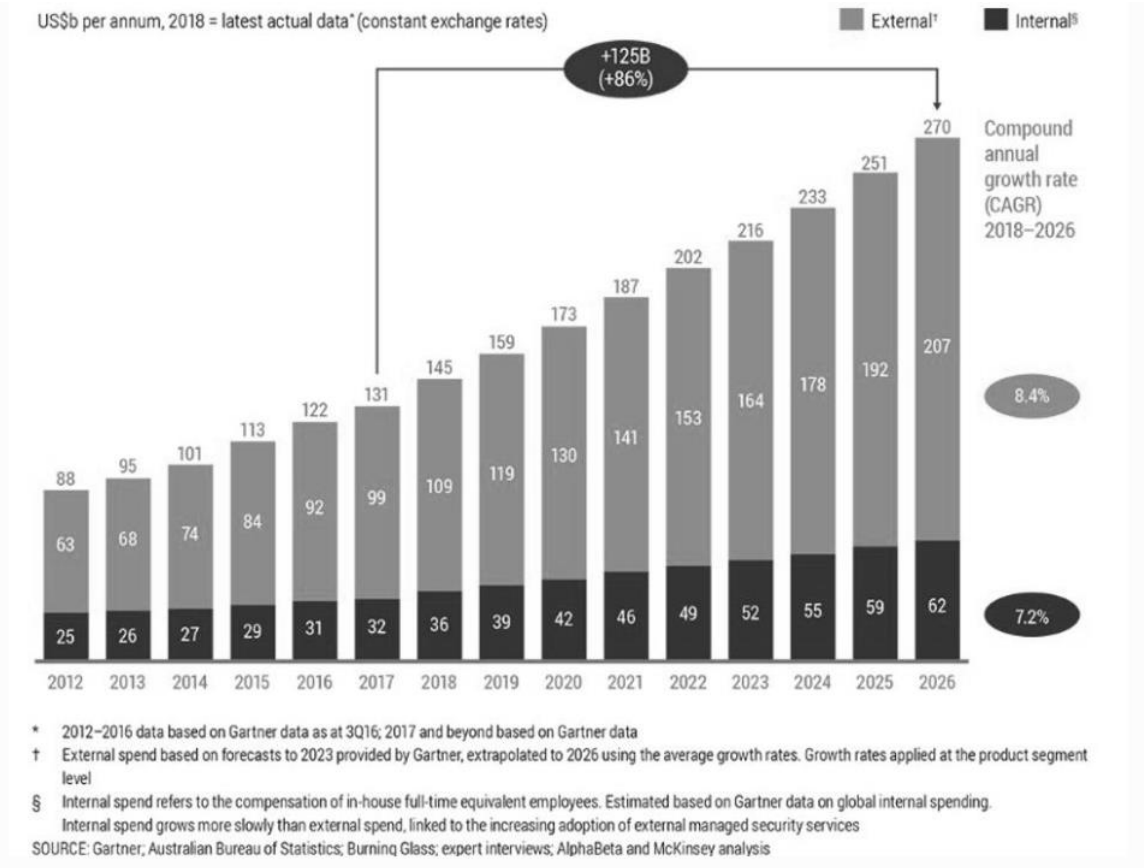

Figure 2. Worldwide spending on information security products and services [9].

Fully aware of the severity of cyberattacks, many companies have adopted different methods to manage cybersecurity threats. While several companies have tried to build their own cyber security metrics and measures with the hope of verifying their security controls, exploring their security strengths and weaknesses; and detecting security trends [10]; others label their information basing on subdivided degree of sensitivity which allows people at different level having particular authorization to access to sensitive information for better information management and protection [11]. Besides, in Smetters's research [12], the author demonstrates that the failure of existing security system is attributed to users difficulties in managing security and their inability to figure out their security-critical tasks accomplishment, which leads to only 51 % of users actually update their antivirus software although 92 % of them think that they have already done and 73 % users think that they have turned on a firewall while only 64 % actually do that. Therefore, according to Smetters [12], an organization need well-designed information visualization tools for a stronger system administration management.

In a macro perspective, to tackle with the ever-present threats from cyber criminals, governments, regulators and legislators around the world have been enacted many laws and rules for governing privacy and security protections (e.g.: In US: The National Strategy to Secure Cyberspace [13]; International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World [14]; In France: French National Digital Security Strategy [15]; In Germany: Cyber Security Strategy for Germany [16] and IT Security Act [17]; In China: The Decision of the Standing Committee of the National People's Congress on Strengthening the Network Information Protection [18]; In Canada: Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada [19]; In Albania: National Security Strategy [20] and Cyber Security Strategy [21].

CYBERSECURITY AND AUDIT FEE

Although the implication of cybersecurity stretch across all business regions, the most attention of the cybersecurity in business world focuses on the financial sector because according to Kamiya et al. [22], financial information attack leads to a negative stock-market reaction, a decline in sales growth for large firms and retail firms, a rise in leverage, a deterioration in financial health, and a reduction in investment in the short run. Hence, it is no doubt that a scandal in financial information security hack can easily knock even a big company down in a short period of time. As results, in these recent years, regulators and standard setters have been exert much more concern about cybersecurity threats on the level of attention of external auditors [23-28]. There are many reasons for regulators and standard setters forcing external auditors to pay more attention to cybersecurity-incident-occurring companies. Firstly, it is the mission of external auditors to assess the client's accounting for losses, claims, and liabilities related to a cyber-security incident once it happens in the context of a company finding difficult to cope with considerable and unexpected direct and indirect cost [29]. Secondly, in case of direct cyber-attacks to a company's accounting system, external auditors are required to take into consideration the Internal Control over Financial Reporting (ICFR) because the incident could involve in the risk of the company' accounting record manipulation, which results in the less trustful financial statements [24]. Even if cyber-attacks do not affect the accounting recording system, the auditors are still required to put additional efforts in their auditing work since there is indication about weaknesses in the company's internal control, which could be risks in ICFR [30]). As external auditors are put under enormous pressure when auditing cybersecurity-incident-occurring companies, it is necessary to discover how external auditors responds to cybersecurity incidents, and one of the common indicator is audit fee charges [30, 31].

"Audit fee is the economic remuneration for auditors who provide audit services, which are an agency fee according to certain standards. The audit fee includes the total cost of audit through the overall audit work, the risk compensation and the profit demand." [32]

In other words, audit fees serve as compensation for auditing services which include both auditing work performance and auditing risk [33]. Since the risk is increasing in cybersecurity-incident-occurring companies as stated above, there are many hypotheses in academic literature about the impact of cybersecurity incident on external auditors' response through audit fees [30, 31, 34]. To be more specific, using 229 cyber incidents from the Audit Analytics cybersecurity database and Privacy Rights Clearinghouse for the period between 2010 and 2014, Li et al. [30] finds out that cyber incidents exerts positive impact on the audit fees. It means that higher audit fees are charged for the companies experiences cybersecurity hacks. Smith and Pinsker's research [34] result also shares the same conclusion as Li et al.'s [30] when demonstrates that there is positive association between both past and future breach disclosures and audit fees. On the other hand, investigating 5,687 companies from the Audit Analytics Audit Fees database for 12-year period between 2003 and 2015, Rosati et al. states that audit fees increasing just occurs in temporary and auditors take into consideration of cyber-security risk in their audit risk assessment in advance of the occurrence of an incident [31].

Owing to the fact that there are few researchers investigating the relationship between cybersecurity risk and audit fees, and the final conclusion about this relationship has not been reached yet, this research will fill this gap in academic literature by building the hypothesis as followed:

H_1: The cybersecurity incidents have positive impact on the high audit fees.

METHODOLOGY

On the basis of the literature reviews and in order to test the hypothesis above, a detailed description of this research's methodology is provided in this chapter. As quantitative analysis can help 'to explore, present, describe and examine relationship and trends within our data' [35], quantitative method is adopted throughout this study.

DATA

The sample firms used to answer the research questions are 100 worldwide firms listed Wharton Research Data Service. This database is chosen because it comprises 100 small, medium and big companies with diverse major throughout the world, which will present a vivid picture relating to the effect of cyber security attacks on audit fees in the world. Also, the financial information with these companies can be collected via Wharton Research Data Service website, which then can support to answer this research's question. However, due to the lack of many missing financial data or no audit fee information, this study just focuses on only 78 companies instead of 100 companies. The reduced number of companies still holds the qualitaties of the full data set since according to Groubner et al. [36; p.307, 37] "samples of 25 to 30 produce sampling distributions that are approximately normal", therefore a sample of 78 is considered a sufficiently large sample. Meanwhile, the data set contains historical financial data between the time period of 2005 and 2014 i.e. for the majority of companies a ten-year period is covered providing large enough sample to study. On the other hand, keeping the businesses in the dataset with a shortage of relevant financial and audit fee information would have provided unreliable results while reducing the data set to companies possessing all the data required has beneficial impact on the analysis; it does not cause bias while the analysis remains reliable and is capable to reflect a real phenomenon.

All the data used in this research are secondary data. Yearly historical financial data of 100 companies are scrutinized for the period between 2005 and 2014, because this period experienced a variety of significant occurrences in the worldwide cyber security as mentioned in the literature review above. While yearly historical financial data of 100 companies are obtained from Wharton Research Data Service, the companies breach information is collected from Data Breaches shared by Privacy Rights Clearinghouse.

RESEARCH DESIGN

Audit fees are used in this research to represent the degree of auditors' concern about cyber securities incidents, because they are proved to be powerful tools to measure the attention of auditors to cyber-attacked companies in academic research. Several researchers imply that higher audit fees related to: higher IT investments as the IT complexity brings difficulties for auditors to detect accounting irregularities [38]; higher information asymmetry [33]; more severe cyber incidents [30]; less active audit committees [34]. Consistent with prior studies, in this research, audit fees are used as proxies for the measurement of external auditors' concern for cyber security risks.

The multivariate regression models used to test the research hypothesis is semi-logarithmic model developed from the model in Rosati et al.'s research [31]. As stated in Rosati et al., audit fees "vary with size, complexity, riskiness and other client-specific characteristics" [31; p.17] as the size of the business, the auditee complexity, the business's asset structure, its financial condition, the arising business risk, earnings quality, corporate directorship and a company's regulatory environment [31]. The method adopted to estimate the regression model mentioned above will be Ordinary Least Square (OLS) method.

The target of this study is to examine external auditors concern for cyber security risks by exploring whether cyber security incidents can lead to high audit fees. Therefore, the hypothesis stating that cybersecurity incidents have a positive impact on high audit fees is to be tested by a multivariate regression model including predicting variables in case of which data were available. Variables with extensive missing data were excluded, however, employing a reduced number of variables with exhaustive data probably results in stronger explanatory effect (higher R_2 in the regression model) than including variables with extensive missing values. The revised multivariate regression model used to test Hypothesis 1 is estimated as the following:

$$LAF_{i,t} = \beta_0 + \beta_1 BREACH + \beta_2 LTA + \beta_3 LLEV + \beta_4 CUR + \beta_5 QUICK + \beta_6 ROA + \beta_7 DEBTEQ + \varepsilon_{i,t} \quad (1)$$

where:

$LAF_{i,t}$ = logarithm of audit fees of firm i in year t, a proxy for the external auditors concern for cyber security risks;

BREACH = 1 if a firm experiences a cyber-security incident in year t, 0 otherwise;

LTA = logarithm of end of year total assets of firm i in year t;

LLEV = logarithm of the ratio (current liabilities divided by total assets) of firm i in year t;

CUR = the ratio (current assets divided by total assets) of firm i in year t;

QUICK = difference between current assets and inventory divided by current liabilities of firm i in year t;

ROA = earnings before interest and taxes divided by total assets of firm i in year t;

DEBTEQ = the ratio (total debt divided by equity book value) of firm i in year t.

The predicting variables in the model include in a large number factors that control for audit risk such as the ratio of current assets to total assets (CUR), the quick ratio (QUICK), profitability (ROA) and the debt-to-equity ratio (DeBTEQ), while for audit effort the size of the company (LTA) is employed. The occurrence of a cyber attack is also included (BREACH) to confirm an increase in audit fees after a cyber incident occurrence. The model was calibrated to the present data set and can be applied in similar cases as well; and should data be available further and additional variables reflecting business complexity or regulatory environment can be added to the model.

The purpose of the regression model is to figure out the relationship between the main independent variable (audit fees) and dependent variable (breach), which represents for the impact of cyber-security incidents on audit fees. However, besides the main independent variable, the regression model as followed the model in Rosati et al.'s research [31] contains six other independent variables in order to clearly indicate the relationship between an independent variable and a dependent variable.

FINDINGS

CORRELATION BETWEEN AUDIT FEES AND CYBER INCIDENTS

The first signal for the relationship between the two examined variables is correlation coefficients as "The correlation measures the direction and strength of the linear relationship between two quantitative variables correlation" [39]. The purpose of correlation analysis in this research is to measure the linear association between the proxy for auditors' concern (audit fees) and other independent variables with the main dependent variable accounting for cybersecurity attack risks (breach).

Table 1 below will shows the pairwise correlations between the variables indicated in the regression model. The result expects to obtain positive correlation between the two main variables: audit fees and breach, which means that cybersecurity attacks exert positive effect on the higher audit fees. All the predictors show significant correlation with the dependant variable LAF ($p < 0,05$) but LLEV.

Table 1. Pearson correlations between variables of the model (Source: Eviews stat).

Correlations								
	LAF	**BREACH**	**LTA**	**LLEV**	**CUR**	**QUICK**	**ROA**	**DEBTEQ**
LAF	1							
BREACH	,085*	1						
Sig. (2-tailed)	0,032							
LTA	,577**	0,035	1					
Sig. (2-tailed)	0,000	0,377						
LLEV	–0,022	0,060	–,281**	1				
Sig. (2-tailed)	0,572	0,130	0,000					
CUR	,174**	–0,060	–0,014	–0,054	1			
Sig. (2-tailed)	0,000	0,131	0,728	0,170				
QUICK	–0,127**	–0,050	–0,056	–,360**	–0,023	1		
Sig. (2-tailed)	0,001	0,204	0,157	0,000	0,563			
ROA	,081*	–0,059	,188**	–,219**	0,020	0,007	1	
Sig. (2-tailed)	0,042	0,139	0,000	0,000	0,621	0,868		
DEBTEQ	,133**	0,034	,310**	–0,033	–0,023	–0,036	0,023	1
Sig. (2-tailed)	0,001	0,392	0,000	0,412	0,569	0,359	0,557	

*Correlation is significant at the 0,05 level (2-tailed)
**Correlation is significant at the 0,01 level (2-tailed)

As can be seen from the Pearson correlations matrix in Table 1, the correlation between the audit fees and the breach is positive (0,08), which means that a rise in breach is associated with an increase in audit fees. In other words, an implication could be made from the correlation between audit fees and breach is that a climbing number of cybersecurity attacks of 100 investigated companies from 2005 to 2014 relates to a growth extent of auditors' concern. This preliminary finding is consistent with the explanation that it should take more time and efforts for auditors to examine the correctness of the financial data of a company which has experienced a criminal cyberattacks.

REGRESSION MODEL ANALYSIS

Since Hypothesis 1 in this study aims to examine the positive influence of cybersecurity incidents on audit fees, the coefficient β_1 in the regression model (1) is expected to be positive ($\beta_1 > 0$). This is because positive β_1 means that cybersecurity incidents result in higher external auditors' concern for their auditing companies via higher audit fees, which supports Hypothesis 1. Figure 3 displays and illustrates the higher audit fee in terms of the total asset of the firm i at time t and cyber security incident. The correlation proves to be significant with R^2 = 31,7 % in case of no cyber incident and R^2 = 36,4 % in case of a cyber incident. Excluding the cyber incident factor decreases the multiple R^2 from R^2 = 39,9 % to R^2 = 39,4 % in the entire model implying that the inclusion of the factor cyber breach has increased the robustness of the model and serves as an explanatory factor in rising audit fees.

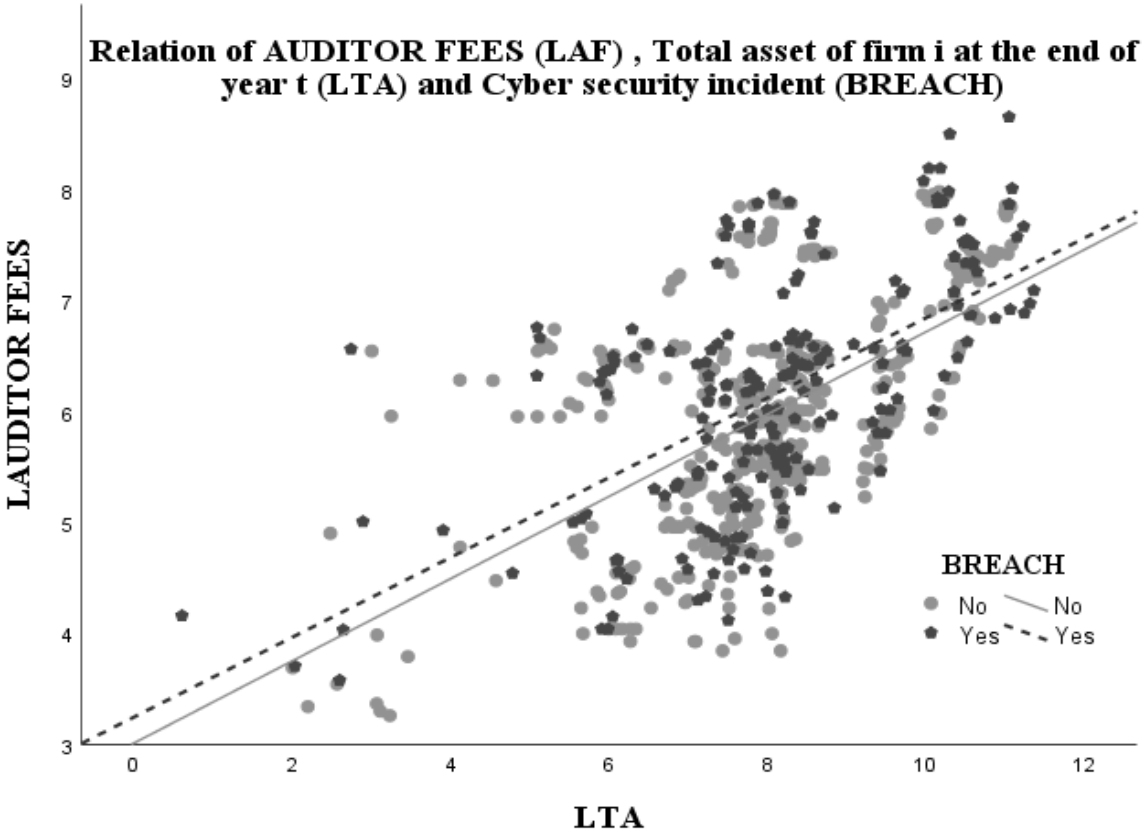

Figure 3. Relation of LAF, LTE and BREACH.

To address the timely increase in audit fees due to cyber incidents Figure 4 visualises the assessment and increase of audit fees due to cyber security incidents throughout the years under observation.

External auditors have become more aware of cyber security breaches as assumed based on the opening gap of the linear trends for audit fees with and without cyber incident. While audit fees are slightly increasing with time in case of companies without recognised cyber breach, they are continuously increasing at a higher rate and pace in case of firms with the occurrence of cyber incidents. The trend equations show the different steep of growth in audit fees resulting in an ongoing widening gap in audit fees for companies with and without cyber breach. According to the regression model companies could calculate with the same audit fee size during the years 2005 and 2006 while from that point of time auditing firms focused more on cyber-attacked companies and raised audit fees to a higher extent in case of those with cyber incident.

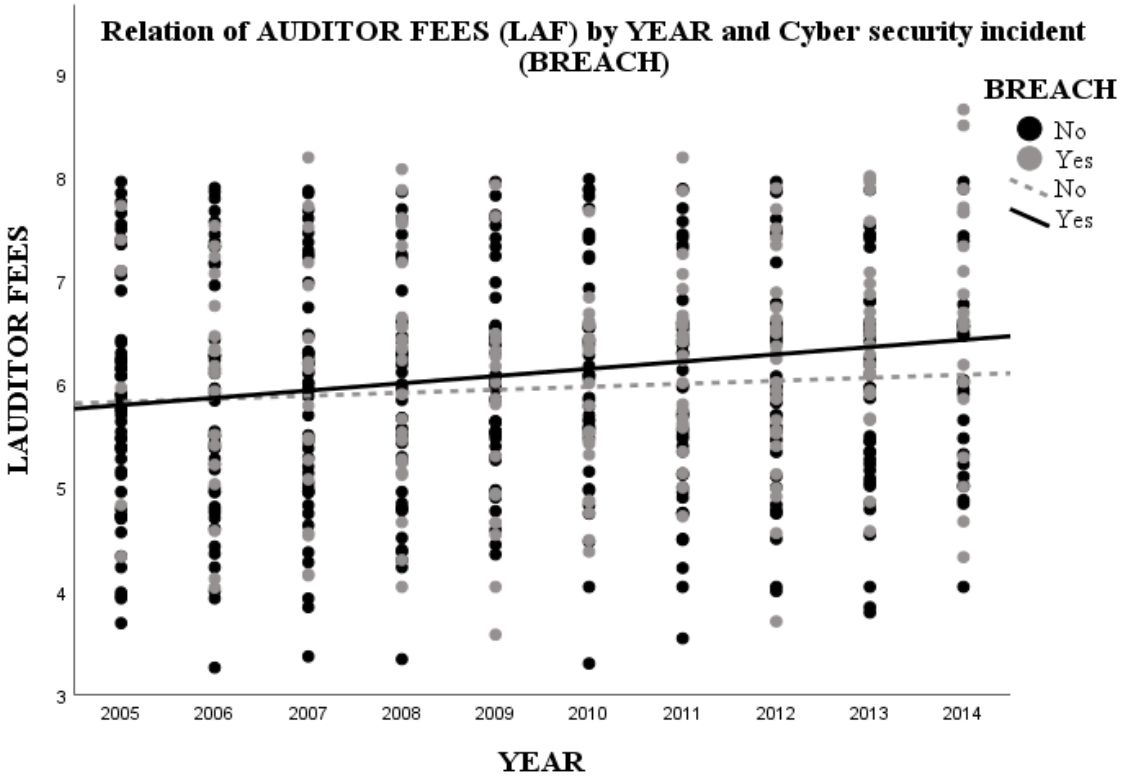

Figure 4. Relation of LAF, YEAR and BREACH.

The regression model justifies the relevance of the time period and provides a reference starting point for higher cyber security awareness amongst audit firms. In this model the variable YEAR proved to be significant at a 5 % significance level.

$$\widehat{LAF}_{No\ breach} = -52.37 + 0.03t, \quad (2)$$

$$\widehat{LAF}_{Breach} = -1.35E2 + 0.07t, \quad (3)$$

The results indicate a gradual and ongoing raise in audit fees even in the time period following the observed one based on external auditor assessment. The trend for audit fees in case of firms with no detected cyber breach shows a much flatter shape (2). To conclude, the nature of the trend signals that external auditor assessment resulting in detecting cyber incidents and breach raises awareness and results in higher audit fees.

Table 2 below provides Eviews results for the original regression model (1) testing the influence of cybersecurity incidents on audit fees. The model itself proved to be significant since F = 59,672 while p = 0,000, i.e. the influential factors are worth examining. The correlation analysis showed, however, that the strongest relationship exists between the total asset of firm i at the and of year t (LTA) and audit fees (LAF) while LTA and BREACH are in positive correlation, i.e. a firm with higher total asset is rather exposed to cybersecurity incidents.

As can be seen from Eviews results in Table 2, the coefficient of BREACH is significantly positive (0,148793) at 5 % level of confidence (*p-value* = 0,0364), which confirms the expectation mentioned above ($\beta_1 > 0$). The coefficient of BREACH estimated at 0,148973 means that with all other variables unchanged, the increase of one cybersecurity incident of 100 examined companies from 2005 to 2014 will lead to nearly 14,9 % increase in the audit fees. This result consists with the result from descriptive statistics analysis above. Also, the result shows an evident fact about

the positive relationship between the audit fees charge and cybersecurity incidents, which means that companies that experience cybersecurity attacks have a tendency to tolerate higher audit fees charge.

Table 2. Eviews results of the multivariate regression model 1 (Source: Eviews stat).

Dependent Variable: LAUDITOR_FEES				
Method: Least Squares				
Date: 12/08/19 Time: 17:28				
Sample: 1 638				
Included observations: 638				
Variable	**Coefficient**	**Std. Error**	**t-Statistic**	**Prob.**
C	2,722944	0,177025	15,38167	0,0000
BREACH	0,148973	0,071041	2,097017	0,0364
LTA	0,405316	0,022127	18,31757	0,0000
LLEV	0,207780	0,050081	4,148915	0,0000
CUR	0,001502	0,000242	6,209198	0,0000
QUICK	–0,000766	0,000795	–0,963576	0,3356*
ROA	–9,32E–06	6,31E–05	–0,147731	0,8826*
DEBTEQ	–0,014589	0,008152	–1,789540	0,0740*
R-squared	0,398685	**Mean dependent var**		6,013722
Adjusted R-squared	0,392003	**S.D. dependent var**		1,065984
S.E. of regression	0,831192	**Akaike info criterion**		2,480547
Sum squared resid	435,2542	**Schwarz criterion**		2,536451
Log likelihood	–783,2946	**Hannan-Quinn criter.**		2,502249
F-statistic	59,67185	**Durbin-Watson stat**		0,363616
Prob (F-statistic)	0,000000			

*The variable is significant at the 0,05 level

For the controlling variables, except from the coefficients of variables QUICK, ROA and DEBTEQ which are statistically insignificant, coefficients of other controlling variables are positively significant at both 1 % and 5 % level of confidence.

The R-square of the regression model is used to measure the level of percentage of independent variables explaining the dependent variable in the regression model. In this regression model, the R-Square is acquired at nearly 40 % which shows that the regression model quite fits the data collected and means that 40 % of the observed variable could be explained by the model's input independent variables.

The linear regression function is the following based on the model:

$$\widehat{LAF} = 2.722944 + 0.148973BREACH + 0{,}405316LTA + 0.207780LLEV + 0.001502CUR - 0.000766QUICK - 0.00000932ROA - 0.014589DEBTEQ \quad (4)$$

Noting that the time period under study depicts the date when auditors started to raise awareness of the significance of cyber attacks, and noting that the business segment as a company's complexity factor is supposedly has an effect on potential cyber incident the regression model was extended and tested with two additional factors: time (YEAR) and regulatory business environment (SIC), namely the mdoel was run with the inclusion of the year (YEAR) and the two-digit code for industry indicators (SIC). The regression model improved to R^2 = 40,7 % i.e the explanatory size of the predictors slightly increased while the model remained significant (F = 47,930, p = 0,000). As predictors, business sector (SIC) proved to be significant *(*t = –2,742, p = 0,006) while the YEAR has turned into an insignificant variable (t = 1,164, p = 0,245). Consequently, the exclusion of the variable YEAR is justified while the analysis of audit fees for the different industry sectors in case of cyber-attacked companies is grounded.

CONCLUSION

This article addresses the question of whether external auditors provoke any response towards cybersecurity incident risks. This study is designed in the context of the mushrooming increase in the number of criminal cybersecurity occurrences around the world and the introduction of many rules and laws to protect technology users from cybercrimes. Especially in the business world where the cybercrimes consequences have been becoming more and more severe these days and the cybersecurity-attacked companies are put in such terrible conditions that they have more tendency to hide the true picture of their companies in order to keep calm their investors and stockholders. This result will then exert more pressure on external auditors who are responsible for providing reasonable assurance that financial statements of a company are presented fairly and in conformity. Hence, the research question of this study test whether external auditors pay more attention to cybersecurity incidents by examining whether higher audit fees will be applied to cybersecurity-attacked companies.

Consistent with the research's hypothesis, the corresponding regression model reveals an evident fact that higher criminal cyber incidents of 100 global companies from 2005 to 2014 result in higher audit fees charged. The ten-year time series model reveals that based on the model and the data available there was a turning point in the year 2005 and 2006 when auditing firms commenced to put more emphasis on cyber-attacked companies and auditing fees started to increase at a higher speed in case of such businesses. The model extended with the two-digit business code unveiled that audit fees for cyber-attacked companies vary depending also on the industry sector. As this result demonstrates the fact that external auditors express more concern for cybersecurity-attacked companies, it provides support for those regulations and laws related to the role of external auditors in the context of terrible cyber crimes [23-28] and previous academic literature [30-31]. On the whole, this research brings new perspectives and evidence to the growing body of literature about the relationship between external auditors' concern and cybersecurity risks. The study helps to reassure the business world that external

auditors are still trying their best to pay more attention to cybersecurity-attacked companies on the purpose of supplying the most reliable financial reports of the companies to the public.

Nevertheless, there are still three limitations recognized in this study. The first issue is accounted for the short-reviewed period of time of this research, just ten years from 2005 to 2014 due to the difficulties in approaching latest financial data supported for the regression model. If the period of time can be extended longer up to date, the research will provide a clearer picture about the relationship between external auditors' concern and cyber criminals. Secondly, there are missing financial data for some companies which then leads to the reduction of some controlling variables compared to the original model in Rosati et al.'s research [31] and the insignificance of three controlling variables. The reduction in the number of the controlling variables did not affect the significance of the model, the inlcusion of the industry sector (SIC) and the YEAR controlling variables slightly increased the explanatory size of the model. The inclusion of the business sector and the year improved the model and proved that industrial sectors need to be analysed separately and be compared in the light of cyber-attacks in the future. Based on these limitations, further research can be conducted with longer and latest examined period of time and the full collection of financial data to support for the regression model.

REFERENCES

[1] Fama, E.F.: *Efficient Capital Markets: A Review of Theory and Empirical Work*. The Journal of Finance **25**(2), 383-417, 1970, http://dx.doi.org/10.2307/2325486,

[2] European Commission: *Cyber Security Report*. https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_390_en.pdf, accessed 18th December 2019,

[3] Cukier, M.: *Study: Hackers Attack Every 39 Seconds.* A. James Clark School of Engineering, 2007, https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds, accessed 10th December 2019,

[4] Milkovich, D.: *15 Alarming Cyber Security Facts and Stats.* Cybintsolutions, 2019, https://www.cybintsolutions.com/cyber-security-facts-stats/, accessed 10th December 2019,

[5] Accenture Security: *The cost of Cybercrime*. Ponemon Institue LLC, North Traverse City, Michigan, 2019, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50, accessed 11th December 2019,

[6] Varonis: *Global Data Risk Report From The Varonis Data Lab.* https://info.varonis.com/hubfs/Varonis%202019%20Global%20Data%20Risk%20Report.pdf, accessed 16th December 2019,

[7] RiskBased Security: *2019 MidYear QuickReview Data Breach Report*. Cyber Risk Analytics, 2019, https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report, accessed 18th December 2019,

[8] Gartner: *Gartner Forecasts Worldwide Information Security Spending to Exceed $ 124 Billion in 2019.* Gartner, Sydney, 2018, https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019, accessed 14th December 2019,

[9] Columbus. L.: *2020 Roundup of Cybersecurity Forecasts And Market Estimates.* Forbes, 2020, https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#298b8fd7381d, accessed 10th April 2020,

[10] Black, P.E.; Scarfone, K. and Souppaya, M.: *Cyber Security Metrics and Measures.*
In: Voeller, J.G., ed.: *Cybersecurity.*
John Wiley & Sons, Inc, New Jersey, pp.1-7, 2014,
[11] Irvine, C.E.: *Multilevel Security*.
In: Voeller, J.G., ed.: *Cyber Security*.
John Wiley & Sons Inc, New Jersey, pp.9-28, 2014,
[12] Smetters, D.K.: *Cyber Security Technology Usability and Management*.
In: Voeller, J.G., ed.: *Cyber Security*,
John Wiley & Sons, Inc, New Jersey, pp.41-55, 2014,
[13] US: *The National Strategy to Secure Cyberspace*.
Department of Homeland Security (DHS), 2003,
https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, accessed 12th December 2019,
[14] US: *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World.*
Department of Homeland Security (DHS), 2011,
https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, accessed 12th December 2019,
[15] France: *French National Digital Security Strategy*.
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf, accessed 12th December 2019,
[16] Germany: *Cyber Security Strategy for Germany*.
https://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1, accessed 12th December 2019,
[17] Federal Office for Infrormation Society: *IT Security Act*.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2, accessed 19th December 2019,
[18] Standing Committee of the National People's Congress: *The Decision of the Standing Committee of the National People's Congress on Strengthening the Network Information Protection 2012.*
National People's Congress, China, 2012,
https://uk.practicallaw.thomsonreuters.com/7-543-6885?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1, accessed 12th December 2019,
[19] Government of Canada: *Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada.*
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-cbr-scrt-strtgy/archive-cbr-scrt-strtgy-eng.pdf, accessed 19th December 2019,
[20] Republic of Albania: *National Security Strategy*.
Republic of Albania, Ministry of Protection, 2014,
http://www.mod.gov.al/images/PDF/strategjia_sigurise_kombetare_republikes_se_shqiperise.pdf, accessed 18th December 2019,
[21] Republic of Albania: *Cyber Security Strategy.*
http://www.mod.gov.al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf, accessed 19th December 2019,
[22] Kamiya, S., et al.: *What is the Impact of Successful Cyberattacks on Target Firms?*
Working Paper series: no.w24409, National Bureau of Economic Research, NBER, Cambridge, 2018,
http://dx.doi.org/0.3386/w24409,
[23] International organization of securities commissions: *Cyber Security in Securities Markets – An International Perspective*
The Board of the International Organization of Securities Commissions, Madrid, 2016,
https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf, accessed 10th December 2019,

[24] Public Company Accounting Oversight Board: *Standing Advisory Group Meeting: Cybersecurity*.
Public Company Accounting Oversight Board, Washington D.C., 2014,
http://pcaobus.org/News/Events/Documents/0624252014_SAG_Meeting/06252014_Cybersecurity.pdf, accessed 10th December 2019,

[25] Public Company Accounting Oversight Board: *Staff Inspection Brief*.
Public Company Accounting Oversight Board, Division of Registration and Inspections, Washington D.C., 2015,
https://pcaobus.org/Inspections/Documents/Inspection-Brief-2015-2-2015-Inspections.pdf, accessed 10th December 2019,

[26] Public Company Accounting Oversight Board: *Staff Inspection Brief*.
Public Company Accounting Oversight Board, Division of Registration and Inspections, Washington D.C., 2016,
https://pcaobus.org/Inspections/Documents/Inspection-Brief-2016-3-Issuers.pdf, accessed 10th December 2019,

[27] Securities and Exchange Commission: *Cybersecurity Roundtable*.
Securities and Exchange Commission, Washington D.C., 2014,
https://www.sec.gov/spotlight/cybersecurity-roundtable.shtml, accessed 13th December 2019,

[28] Securities and Exchange Commission: *Commission Statement and Guidance on Public Company Cybersecurity Disclosures.*
Securities and Exchange Commission, 17 CFR Parts 229 and 249, Washington D.C., 2018,
https://www.sec.gov/rules/interp/2018/33-10459.pdf, accessed 13th December 2019,

[29] Center for Audit Quality: *Cybersecurity and the External Audit*.
CAQ Alert #2014-3, Center for Audit Quality, Washington D.C., 2014,
http://www.thecaq.org/caq-alert-2014-03-cybersecurity-and-external-audit, accessed 19th December 2019,

[30] Li, H.; No, W.G. and Boritz, J.E.: *Are External Auditors Concerned About Cyber Incidents? Evidence from Audit Fees.*
Auditing: A Journal of Practice & Theory **39**(1), 151-171, 2020,
http://dx.doi.org/10.2308/ajpt-52593,

[31] Rosati, P.; Gogolin, F. and Lynn, T.: *Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters*.
The International Journal of Accounting **53**(3),1-58, 2019,
http://dx.doi.org/0.1142/S1094406019500136,

[32] Liu, S.: *An Empirical Study: Auditors' Characteristics and Audit Fee*.
Open Journal of Accounting **6**(2), 52-70, 2017,
http://dx.doi.org/10.4236/ojacct.2017.62005,

[33] Frino, A.; Palumbo, R. and Rosati, P.: *Does Information Asymmetry Predict Audit Fees? Evidence from Italian Listed Companies.*
American Accounting Association Annual Meeting, August 3-7, Anaheim, CA, 2013,

[34] Smith, T. and Pinsker, R.: *Do Auditors Price Breach Risk in Their Audit Fees?*
Journal of Information Systems **33**(2), 177-204, 2019,
http://dx.doi.org/10.2308/isys-52241,

[35] Lewis, P.; Saunders, M. and Thornhill, A.: *Research methods for business students*.
Fifth Ed., Pearson Education Limited, Essex, 2009,

[36] Groubner, D.F.; Whannon, P.W.; Fry, P.C. and Smith, K.D.: *Business Statistics: A Decision Making Approach.*
Seventh Ed. Pearson Education Inc., New Jersey, p.307, 2008,

[37] Swift, L. and Piff, S.: *Quantitative Methods for Business, Management and Finance*.
Fourth Ed., Macmillan Education, UK, 2014,

[38] Han, S.; Rezaee, Z.; Xue, L. and Zhang, J.H.: *The association between information technology investments and audit risk*.
Journal of Information Systems **30**(1), 93-116, 2016,
https://dx.doi.org/10.2308/isys-51317,

[39] Moore, D.S., et al.: *The Practice of Statistics for Business and Economics*.
Third Ed., W. H. Freeman and Company, New York, 2011.