UNIVERSIDADE CATÓLICA PORTUGUESA

Cybersecurity and External Audit

The disclosure of risk factors in annual reports

Gonçalo Peres Moreira

Católica Porto Business School

2019

UNIVERSIDADE CATÓLICA PORTUGUESA

Cybersecurity and external audit

The disclosure of risk factors in annual reports

Trabalho Final na modalidade de Dissertação
apresentado à Universidade Católica Portuguesa
para obtenção do grau de mestre em Auditoria e Fiscalidade

por

Gonçalo Peres Moreira

sob orientação de
Eleonora Monaco

Católica Porto Business School,
Março de 2019

Acknowledgment

First of all, an exceptional mention to my principal mentor Prof. Eleonora Monaco, for the guidance, support and help that turn possible to elaborate this Master's Thesis.

To the Prof. Pierangelo Rosati and Prof. Theo Lynn, for the time spent in Dublin, at Dublin City University, and for the help when dealing with Data Bases.

To my partner in foreign countries, Diogo Cruz, for the companionship, support and all the time we spent together.

To all my friends, with a special mention to Gonçalo Branco, to Beatriz Soares, to Luísa Dias and to Sara Maia Couto, for making this journey with me and turning the Masters in Audit and Taxation into something outstanding.

Last but not least, to my family. To my father António Júlio Caseiro Moreira, for the constant motivation and for making sure that I had all the necessary conditions to make a good paper. To my mother Maria da Graça Ramos Peres for always believe in me and to my brother for the friendship that we shared all these years.

Resumo

O presente trabalho examina a questão dos incidentes de cibersegurança. Mais especificamente, este trabalho examina se existe relação e em caso de existir, avalia como é que, de facto, os incidentes de cibersegurança estão envolvidos com a quantidade de taxas de auditoria cobradas, assim como com algumas características específicas dos auditores externos. Os resultados da análise permitem demonstrar que existe uma relação positiva e significativa entre a alteração nas taxas de auditoria no ano da violação dos dados. Os. auditores aumentam as taxas de auditoria com o objectivo de reduzir o risco de auditoria associado aos incidentes e eventos de cibersegurança, bem como nos esforços adicionais para avaliar a empresa afectada.

Além disso, o aumento nas taxas de auditoria cobradas é confirmado não só através do ano em que ocorreu o evento, mas também nos 2 anos seguintes, aquando da existência de uma mudança de auditor.

Keywords: Riscos de cibersegurança, quebras, auditores externos, taxas de auditoria, especialista da indústria, mudança de auditor.

Abstract

The present work examines whether and how the cybersecurity incidents are related to the amount of audit fees as well as to some specific characteristics of external auditors. Results of the analysis allow to demonstrate that there is a positive and significant relation between the change in audit fees in the year of the data breach. Auditors increase the audit fees to reduce the audit risk associated with the cybersecurity incidents, as well as for the additional efforts to evaluate the breached company.

Moreover, the increase in audit fees is confirmed not only in the year of the event but also for the following two years when there is a change in auditor.

Keywords: Cybersecurity risks, breaches, external auditors, audit fees, industry specialist, auditor's change.

Index

Index of Charts, Figures and Tables

1. Introduction

Given the globalization phenomena, all the companies around the world are becoming every day more dependent from technology. According to SEC (2018), today the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century.

Turning all systems and operations connected, firms store data online and share information with different stakeholders. Therefore, as a first consequence, companies need to protect their business from the cybersecurity attacks, causing an increase in the IT investments. From a shareholder point of view, it is necessary to know how resources are allocated and whether there are any variations of IT investments pre- or post- a data breach (SEC, 2018).

Cybersecurity turned out as an issue with increasingly importance in the markets and economies nowadays that it might cause reduction of stock price as well as it might have a negative effect on the value of the companies.

In this context the external auditors play an important role given that they should guarantee that the financial statements report all facts that affect the company performance and might reduce the value of their assets. By analysing the financial reports, they should verify that the cybersecurity investments made before and after a data breach inform properly the investors (Rosati, Gogolin, and Lynn, 2017).

The main purpose of the thesis is to examine whether and how incidents are related to the amount of audit fees as well as to some specific characteristics of external auditors as well as how the cybersecurity risk factors are disclosed by the companies. Therefore, after a first examination of the concept of

cybersecurity, risks and incidents related to cybersecurity breaches will be examined.

Besides that, it will be investigated if the audit fees are related to a several characteristics like the audit effort that an auditor should present (Choi et al., 2008) or the business risk that will have impact on the audit fees (Bell, Landsman, & Shackelford, 2001) and if there are any increase/decrease of audit fees pre-post breaches. Moreover, it will be examined if the presence of Industry Specialist or the Change in Auditor can explain an increase in audit fees after the cybersecurity breaches.

Thus, for these reasons, both Regulations from SEC (2011; 2018) in force in USA and Europe are examined in order to highlight the requirements, differences and consequences on company's disclosure. This comparison allows bettering understanding how companies behave and manage the cybersecurity incidents in different ways whether faced with different legislation.

2. Literature Review

2.1. Definition and Classification of Cybersecurity Incidents

Modern economies are based on the security and trust of communication channels, as well as, on the transactions of information through sophisticated systems and networks. For these reasons, the Security Exchange Commission has recently underlined that "with the rise of digital communication, cybersecurity represents risks and threats to the capital markets. Therefore, cybersecurity risks and their risk factors, more than spoil industries, companies and investors from all countries, they can affect financial statements and annual reports" (SEC, 2018).

According to National Initiative for Cybersecurity Workforce Framework, cybersecurity is defined as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" (DHS, 2014). Therefore, one of the main goals to a company is to reduce the threats of cyberattacks and vulnerability by improving the information assurance.

The relevance of the phenomenon has been justified by a fast growing in number of studies that focus on cybersecurity issues. Gordon, Loeb, and Zhou (2011) define a cybersecurity incident as "a security breach or any events which compromises the availability, confidentiality or integrity of an information asset". Every day, companies are affected by several and different types of cybersecurity incidents such as malware, ransomware (or denial-of-service

attacks), malicious insiders, card payment fraud or human error[1]. Usually the main targets of the cybersecurity attacks are companies that detain critical data but also weak systems that facilitate its extortion. Recently, the Federal Bureau of Investigation (2018) reported that there is a fastest growing malwares (with more than 4,000 attacks since January 1 in 2016) that targeted all types of companies from different industries. For example, A.P. Moller-Maersk, a shipping company based in Copenhagen which transports about one-fifth of the world's cargo, was recently victim of a ransomware shakedown with the name of NotPetya. Its terminals' operations were impacted in four different countries causing expenses estimated more than 200 million dollars (Mathews, 2017).

One of the most critical factors for the companies is the short-term evaluation of a cybersecurity risks as well as its consequences when an incident occurs. For example, in markets with a growing number of M&As, cybercriminals tend to access into the smaller companies' IT systems (PwC, 2016) with the negative effects in term of damage of their intangible assets.

The 2017 Global Risks Report, released by World Economic Forum, underlines that the interdependence among different infrastructure networks is increasing the risk for systemic failures. Based on the latter report, USA is ranked top 7 in the ranking for cyberattacks, data fraud or theft, misuse of technologies. In Germany the situation is similar with data fraud or theft ranked in the first position and cyberattacks classified in the 6th position for risk (in Portugal, data fraud or theft and cyberattacks is in the 13th position).

Moreover, there are several ways that the companies can use to protect themselves against the cyberattacks, such as the use of Cloud based, Big Data

[1] Appendix A reports a list of the different types of cybersecurity incidents described in this study followed by an example for each type of breach. For instance, ransomware is a format of malware where act most of the times through a spread of phishing emails.

Analytics, Advanced authentication, DevOps, Internet of Things (IoT) and other cybersecurity insurances, even if many times the investments in these assets are not effective.

2.2 USA and EU regulation on data protection and cybersecurity

As recently underlined by a PwC's report (2016), even if the digitalization of business operations and the massive use of data analytics take many benefits to the companies, at the same time expose them to high cybersecurity risks.

A study published by the Ponemon Institute (2017) highlights that 25 percent of the data breaches incidents in 2016 (based on a sample of 419 companies in 13 countries and regions) were caused by the negligent employees or other human factors like contractors.

For these reasons, both USA and European Union issued some important regulations to protect personal data of both consumers and investors. Recently, the EU issued the Data Protection Directive later substituted by General Data Protection Regulation (GDPR), Electronic Commerce Directive, and Copyrights in the Information Society Directive[2], while USA's federal agencies and regulators issued a legislation to protect the national critical infrastructures through SEC, PCAOB and other institutions. In this context, the online privacy still remains a grey area that is not full regulated and that leaves space to cybersecurity initiatives (Almeida, 2016).

[2] More than the Directives presented, European Union has issued documents such as Cybersecurity Strategy for the European Union, European Agenda on Security, Digital Single Market Strategy, Digitising European Industry and Network and Information Security Directive.

The approach followed by EU on this matter, it has been disclosed in specific guidelines on *Cybersecurity Strategy document*[3] and *Code of Online Rights*[4] that highlight how, according to the General Data Protection Regulation (GDPR), cybersecurity and privacy rights[5] must be balanced into controls of IT systems.

Also the USA Government issued some new rules to guarantee the protection of online privacy although there are still some difficulties to define a global strategy that align both USA and EU approaches[6].

Both Countries underline the importance to use Open Sources Platforms that are considered sustainable platforms which detect faster the vulnerabilities and threats of a huge volume of data, in order to improve efficiency and security. While EU defined an Open Source Strategy by improving ICT security through "*state-of-art*"[7], USA Government provides a free and open source software named *"FOSS"*[8] with the same level of preference attributed to proprietary software.

However, EU and USA are still distant to have a common approach on cybersecurity and data protection, in fact, while the EU approach is based on standardization, the USA approach is based on the information exchange instead of source code access. The EU approach on the cybersecurity problem is

---

[3] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-prot-ect-open-internet-and-online-freedom-and-opportunity-cyber-security, Action 28: Reinforced Network and Information Security Policy.

[4] http://ec.europa.eu/digital-agenda/en/code-eu-online-rights, Chapter 4: Privacy, protection of personal data and security.

[5] Statement by the EU delegation at the Internet Governance Forum held in Istanbul, Turkey, in 2014.

[6] CJEU, 6 October 2015 decision – C-362/14, Cri 2016, pp. 22-28.

[7] The Commission should continue developing according to the OSS communities while implementing state-of-art government pratices: http://ec.europa.eu/dgs/informatics/oss_tech/strategy/strategy_en.htm

[8] The Department of Defense must use OSS in order to achieve effectively the missions, http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf.

based on a standard strategy to combat cyberattacks, creating platforms based on encryption patterns, removable storage, hard copy devices and smart grids.

2.2.1. Public Company Cybersecurity Disclosure and Risk Factors in Annual Reports

Prior studies highlight that investors evaluate the voluntary disclosure in a positive way both management forecast, reports, conference calls or press releases released by a company are considered valuable and credible information (Healy and Palepu, 2001).

The first SEC Regulation (CF Disclosure Guidance: Topic n.2) issued in October 2011 was inspired by a similar approach, SEC issued "a set of principles to follow" more than mandatory rules. The main purpose was to help managers, lawyers and auditors to evaluate both companies' and cybersecurity's risks caused by business operations allowing them to prepare an "accurate disclosure". Basically, despite of not being mandatory, every company should have taken into account all financial and operational risks on a regular basis to inform if "there would be anything material to disclose that could have impact for investors. For instance, in 2011, a company might disclose a risk of occurring a cyberincident because it was considered as a significant factor to make an investment speculative or risky" (SEC, 2011).

As reported by the Guideline (2011) "although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements impose an obligation on registrants to disclose such risks and incidents". Therefore, in this sense the disclosure of

these risk factors should be considered a "mandatory disclosure"[9]. According to this Guideline (2011), every disclosure of cybersecurity risks must specify the nature and details of material risks and not being a generic disclosure. Therefore, a material disclosure should include:

- Cybersecurity risks, potential costs or consequences caused by business or operations aspects;
- Description and addressing of material cybersecurity risks when are presented as outsourced functions;
- Description of the costs and consequences when describing a cyber incident;
- Undetected incident risks;
- Insurance protection and coverage's description.

After the issue of this document, companies had the advantage to better explore and evaluate their risk factors related to cyber risks in advance and to predict future incidents, threats and potential expenses. In 2011, in most of the data breaches incidents, customer data were compromised by a malware embedded in the company's networks systems and even if this was not consider relevant to be disclosed, at the same time the negative event was evaluated and actions were taken to avoid other unexpected expenses (SEC, 2011).

From an external point of view, it is important to clearly understand the exact time when a breach occurred and when, instead, this information has been released given that this could be strictly related to the presence of pending and legal proceedings.

[9] Every company should have followed the requirements established in the Regulation S-K Item 503 (c).

Furthermore, the 2011 Guideline defined the companies' disclosure controls and subsequent procedures: companies need to elaborate an effective disclosure about their controls and procedures related to their businesses' operations. The process involves four steps: i) the record, ii) the process, and iii) summary of the information.

Afterwards the release of the 2011 Guidance, many companies followed the requirements, defined as "risk factors". Willis North America's report (2013) declares that nearly 88% of public companies included in Fortune 500 and nearly 78% of public companies included Fortune 501-1000 disclosed the cybersecurity risks factors in their annual reports. Similarly, another study (Audit Analytics, 2016) demonstrates that in 2015, more than 88% of Russell's 3000 companies released a disclosure about cybersecurity risks and over 2% of these companies reported that they experienced a cybersecurity incident.

In 2018, SEC issued a new Regulation for all public companies, independently weather the company suffered or not a cyberattack, they have the "obligation to notify and inform their investors about both cybersecurity incidents, potential threats and all material cybersecurity risks in a reasonable time" (SEC, 2018).

Compared to the 2011 Guidelines, the new Regulations 2018 presents some novelty:

- the materiality of cybersecurity risks and the subsequent impacts have to be disclosed;
- prohibition of insider trading;
- the obligations are imposed by the exchange listing requirements[10]. For example, the NYSE listed requirements obligate companies to "release

[10] The requirement should be aligned with the Securities Act of 1993 ("Securities Act") and the Security Exchange Act of 1934 ("Exchange Act"). Moreover, in case of dealing with periodic and current reports, they need to follow the Exchange Act (SEC, 2018).

quickly to the public any news of information which might reasonably be expected to materially affect the market for its securities" (NYSE, 2015). The NASDAQ's rule 5250(b)(1), requires also that listed companies are have to "make prompt disclosure to the public of any material information that would reasonably be expected to affect the value of its securities or influence investors' decisions".

Companies have to reveal a detailed disclosure that could compromise the cybersecurity defences, it is not supposed to give a "roadmap" to the flaws and entrances through specific and technical information of the systems and networks. However, companies need to disclose material cybersecurity risks including the consequences that could be financial, reputational or legal (SEC, 2018).

All public companies are required to follow the obligation to fill the requirements in form of: i) Periodic Reports, ii) Current Reports and iii) Security Act, and Exchange Act Obligations. The main contents that should be disclosed are the following:

i) In the Periodic Reports companies have to provide timely and ongoing information about cybersecurity risks and incidents that trigger disclosure obligations" (SEC, 2018). The Periodic Report are those regular filled by the companies to disclose detailed information on regular basis, they include both the annual reports on Form 10-K[11] and Form 10-Q. In the first one, companies have to disclose all business and operations, risk factors, proceedings, management's discussion and analysis of financial condition and results of operations, financial statements, disclosure controls and procedures and corporate governance. The second one, includes quarterly

[11] 17 CFR 249.310.

reports on Form 10-Q [12], both in term of financial statements, management's discussion and analysis of financial condition and results of operations and risk factors. For all private foreign companies, they need to fill the periodic reports on Form 20-F[13].

ii) Current Reports, both Form 8-K[14]and 6-K[15], have report all the costs and consequences of material cybersecurity incidents.

iii) The Securities Act and Exchange Act Obligations require that all public listed companies must reveal all material incidents in order to make a statement clear[16] (SEC, 2018).

By comparing the risk factors reported in the 2011 Guideline and in the new Regulation (SEC, 2018), the latter requires that companies disclosure the risk factors associated with investments and cybersecurity incidents, as defined in Item 503 (c)[17] of Regulation S-K and Item 3.D[18] of Form 20-F. In order to assess the risk factors, companies should report:

- the severity and frequency of prior cybersecurity incidents;
- the probability and magnitude of the cybersecurity incidents';
- the preventive actions that the company will take to prevent the incidents, included the relative costs;
- aspects of business operations and associate costs and consequences of material risks;
- the costs of protection and insurance coverage in a potential incident;

[12] 17 CFR 249.308a.
[13] 17 CFR 249.220f.
[14] 17 CFR 249.308.
[15] 17 CFR 249.306.
[16] Companies should take into consideration Sections 11, 12 and 17 of the Securities Act, as well as Section 10(b) and Rule 10b-5 of the Exchange Act.
[17] 17 CFR 229.503(c).
[18] 17 CFR 249.220f.

- the potential damage in reputation;
- existing or pending potential laws as well as litigations that could affect the requirements and associated costs;
- remediation, litigation, regulatory investigation costs related to cybersecurity incidents.

Companies have to disclosure previous and ongoing cybersecurity incidents to communicate effectively these risks to investors. In a case of a data breach, a company should disclose it but also underline the reasons why the incident occurred and its consequences in term of business operations (SEC, 2018).

Moreover, the company must provide information weather the cybersecurity material risks are related with products, services, competition or relationship with customer or suppliers.

In relation to the legal proceedings (Item 103 of Regulation S-K prevails[19]) companies have to disclose any material information related to it, especially if it is related to customer information. In this case, the company must detail the litigation itself, the name of the court, the proceedings pending and so on and so forth (SEC, 2018).

2.3 Strategies to contain cybersecurity risks

Business executives and IT manages seek to improve the company performance by decreasing risk factors. The random acquisition of the IT tools cannot help to resolve all company cyber issues, smart organizations, instead, need to start a specific cybersecurity program to decrease risks of cybersecurity incidents. As report a recent study (PwC, 2016) companies can use specific tools

[19] 17 CFR 229.103.

to decrease risk factors such as: i) Cloud Computing, ii) DevOps, iii) Internet of Things (IoT), iv) Big Data analytics and v) specific security framework, vi) advanced authentication and vii) cyber-insurance[20].

i) The usefulness of the cloud is related to the possibility to update intelligence gathering and threat modelling, block attacks more efficiently, highlight collective learning and increase the incident response. These tools are considered efficient investments given that allow companies employees to manage the cybersecurity risk and to analyse huge volumes of data. For instance, Global Payments, a company based in Atlanta, allows payment technology services worldwide using private cloud managed services. These services allow to monitor threats and incident response by providing all alerts and threats and filter them to show which ones should be considered as a security threat or a false positive;

ii) DevOps is a software development model which can promote a closer collaboration between IT operations and application developers. The software, used for example by Netflix, is an outstanding tool to reinforce the cybersecurity programs. Companies with thousands of active applications and with implementation of codes updates regularly, find the best use of this tool;

iii) IoT, instead, is an ecosystem that consists in the devices internet connected and other operational tools. Despite of the advantages, companies are increasing the risk in security the data and the privacy. For these reasons, companies are also trying to figure it how common privacy and cybersecurity protocols can work together to protect their business' operations. For example, Steelcase, a company that produce furniture in

[20] The Cloud Computing allows to interconnect the digital ecosystem between individuals, businesses and governments. This platform permits companies to connect through Cloud-Based Cybersecurity tools, including Big Data analytics and advanced authentication.

USA, uses an IoT accelerator called Seamless to better understand the technology behind the moving parts and the privacy requirements.

iv) Furthermore, Big Data analytics is a model that monitors cybersecurity threats, implement an audit, review data and can respond to incidents in order to understand how and when it is used by whom. Besides of the software expertise, it is required an enormous commitment to computing resources. Big Data analytics can notice patterns that a company did not know that existed before, as well as to monitor and detect the employee's behaviour for any suspicious activity.

v) Risks based framework is a structure that allows to measure the yearly progress through a cybersecurity program that focuses on clients and on its information. For instance, the Canadian Imperial Bank of Commerce (CIBC) created a scorecard based on frameworks controls and it measures the maturity of the security program.

vi) Moreover, advanced authentication is a tool used to reinforce the relationship between a customer and a business partner. Besides that, it can reinforce company's security and stop any movement of fraud like payment card data, bad transactions like intellectual property and regulatory compliance like damage to the company itself (PwC, 2016).

vii) Cybersecurity insurance appears is one of the ways that companies can follow to protect themselves from cybercriminals. Insurers assess the current capabilities and risks as a precondition to purchasing any policy. These estimations can help businesses to predict their legal and regulatory exposures, their costs of response and their potential brand damage related to the cybersecurity risks. However, nowadays, insurances products are mainly focused on data destruction, theft and extortion, denial of services attacks and cybersecurity audit expenses (PwC, 2017).

However, some studies demonstrate that in many occasions, the cybersecurity incidents are generally caused by vulnerabilities related to cybersecurity risks that increase with the use of the Internet, cloud computing, mobile devices and so on and so forth (Romanosky, Hoffman, & Acquisti, 2014; Abbasi, Sarker, & Chiang, 2016). The damages generated by the cybersecurity incidents depend on both the type of incident, industry, time period and firms' visibility (Gordon, Loeb & Zhou, 2011) but also on the weakness and vulnerability of the information system of the company.

Some "tangible" effects of the damage caused by the incidents are evident in terms of remediation costs, fines and reputation for the breached companies (Cavusoglu, Mishra, & Raghunathan, 2004; Gordon, Loeb, & Zhou, 2011) with negative consequences in term of value of the company. In fact, prior researches highlighted that cybersecurity incidents can lead up to a five percent loss in the market value (Campbell et al., 2003; Garg, Curtis, & Halper, 2003).

2.4. The role of Auditors in firm's disclosure and risk assessment

According to SEC (2011, 2018), principal executives and financial officers should follow specific requirements both in the quarterly and in the annual reports. Even if the evaluation of the cybersecurity risks and the existence and maintenance of efficient internal controls remain the responsibility of the company, both internal and external auditors play a critical role in

understanding how the business should use IT and their impact on the financial statements.

One of the main issues related to the cybersecurity incidents is the identification of the exact time when the data breaches occurred. Several times, many customers records are stolen or lost, therefore the estimation of both the actual and future damages (expenses/provisions) for the company becomes really difficult (Rosati, Gogolin, and Lynn, 2017) both for internal managers and even more for the external auditors. Therefore, the cybersecurity incidents[21] (data breaches) represent large threats not only for the companies affected but as well as for the reputation of their auditors (CAQ, 2017).

The Deloitte's report (2017), *"Cybersecurity and the role of internal audit"*, underlines the relevance of the role of the internal auditors by providing an independent assessment of the controls and helping the board to understand the digital risks, in this sense they are fundamental to contain cyber threats.

Generally, the internal auditors have to assess and identify all opportunities in order to improve the enterprise security and to inform the board and the auditee committee about the controls, the potential legal issues and financial liabilities. An internal audit plan for cybersecurity should be embraced but it requires a constant testing and an assessment of the risk (Deloitte, 2017).

In the last decade, IT has been considered as a cornerstone for an effective internal control system and it represents an important part in financial reporting (Masli et al., 2010; Li, Sun, & Ettredge, 2010; Haislip et al., 2016) at the

[21] There many definition of cybersecurity incidents, among them: *cyber-terrorism* as defined as an act are committed to the use of technology, being defined as "the purposeful act or the threat of the act of violence to create fear and/or compliant behaviour in a victim and/or audience of the act or threat" (Stohl, 2007); *hactivism*: Explained as "the marriage of hacking with political activism" (Stohl, 2007); *cyber-crime.* instead as explained as "criminal offenses committed on-line or through other forms of information technology" (Quigley et al., 2015); *cyber-warfare* as explained as "the role of information technology as an enabler of warfare" (Colarik & Janczewski, 2012).

same time it increases the vulnerability and the chance of cybersecurity incidents (Benaroch, Chernobai, & Goldstein, 2012).

The external auditors are required to evaluate both the internal controls and the subsequent information of security management controls, therefore they are responsible for monitoring and testing the material risk through the assessment of controls and cybersecurity threats. As all the data breaches generate impact on financial reporting, the potential effects have direct impact also on the auditors' careers. The understanding of company's internal control and IT systems and how they related to the financial reporting should be reported by the external auditors in their reports as well as the assessment of the risks of material misstatement of financial statements post a data breach event (PCAOB, 2013).

According to the Center for Audit Quality (ICFR), external auditors distinguish from internal auditors given that the first ones are responsible for materials reported in the financial statements and in the internal controls over financial reporting, by analysing and testing the audit risk model and the subsequent cybersecurity threats (Christopher, Sarens, & Leung, 2009).

The process involves the measurement of the losses and other liabilities or claims associated with financial statements and with customers (Stefaniak, Houston, & Cornell, 2012; Kajüter, Klassmann, & Nienhaus, 2016).

In general auditors play a fundamental role in assuring confidence in financial statements and capital markets since the Certified Public Accountants (CPAs) are viewed as trusted advisors. If a data breach occurs, the external auditor should first verify the financial statement level, by evaluating accounts

and disclosures, and then check the presence of material misstatement in the documents that the company released[22].

In the company's evaluation post data breaches, auditor should consider that the negative effects of the incidents[23] both in term of damages of the book value of equity the company and as market value. This means that a data breach generates expenses when it occurs. Usually, firms spend large amounts of money every year to prevent any damages, to protect and to secure the company from any breach, however, when a cyberattack occurs it is difficult to establish the exact value of the damage.

There are two different types of costs related to the data breaches auditor should consider: direct costs and indirect costs. Direct costs are all remediation costs, legal fees, fines and lost transactions (Aral, Dellarocas, & Godes, 2013) and protection costs, which may include the costs of making organizational changes, developing additional personnel and protection technologies, training employees and engaging third party experts and consultants. The indirect costs are those which include a loss of present and future revenues as well as the deterioration of customer and partner trust (Aral, Dellarocas, & Godes, 2013; Charette, Adams, & White, 1997).

As these costs are difficult to estimate, researchers use a proxy measure which is the stock price (Cavusoglu, Mishra, & Raghunathan, 2004). These types of costs represent for instance the reputational damage that adversely affects customer or investor confidence and damage to the company's competitiveness, stock price and long term shareholder value.

[22] About the audit procedure about the assessment of the IT environment see PCAOB Auditing Standard No.16.

[23] A data breach could represent, for example, a theft or destruction of intellectual property, financial assets or other information sensitive to the company, shareholders and customers, SEC 2018.

2.4.1 Auditors classification and changes in audit fees

According to Krishnan & Visvanathan (2009), auditors charge audit fees to control risk and diminish the audit risk (Budescu, Peecher, & Solomon, 2012), concluding that auditors realize that inly accounting financial expertise contributes to an audit process' effectiveness. Based on literature, audit fees analysed by many authors like Koh & Tong, 2013, are charged by auditors and lead in its turn to good internal controls (Benaroch, Chernobai, & Goldstein, 2012; Masli et al., 2010; Li, Sun, & Ettredge, 2010; Haislip et al., 2016).

There is a large body of literature that demonstrates that the level of audit fees should compensate the auditors for the services provided and at the same time should include the audit risk (Bell, Landsman & Shackelford, 2001; Frino, Palumbo, and Rosati, 2017). The audit service (and consequently the level of audit fees) includes both the risk of material misstatement, when financial statements are misstated before the audit evaluation, and the detection risk, that includes the risk that the auditor will not be able to identify the misstatement (Lobo & Zhao, 2013).

2.4.1.1. Industry Specialist

Prior studies investigate the role of the industry specialist what are auditors designated by firms and whose training and practice experience largely are in a particular industry (Solomon, Shields and Whittington, 1999). Given that the effectiveness and efficiency in the audit tasks are related to the auditor's knowledge, the industry specialist has a fundamental role and could better evaluate the company risk and misstatements.

Therefore, an auditor that is an industry specialist should be able to assess the cybersecurity risks if the company that is under evaluation operate in the same sector of "auditor specialization". Within this process, the outcome should

not originate a reassessment of the audit risk (Rosati, Gogolin, and Lynn, 2017). The main idea followed by prior studies (Vonna Palmrose, 1986) is based on the fact that the audit size and knowledge should provide a better service and therefore industry specialist should charge higher fees.

2.4.1.2. Change in Audit Fees

First of all, audit fees represent the compensation that auditors get for the provision of the audit services, and they can be established based on audit effort, litigation risk and normal profits (Simunic, 1980; Choi et al., 2008). Audit fees represent the compensation for the auditing services determined by the amount of work that an auditor must perform and the audit risk (Pratt & Stice, 1994; Bell, Landsman, & Shackelford, 2001), therefore they reflect the auditor's economic costs and it changes depending on auditor's size, company risk, complexity and other specific client characteristics (Johnstone & Bedard, 2003; Gul & Goodwin, 2010).

Given that audit risk is a function of material misstatement and of the detection risk (Lobo & Zhao, 2013), a change in audit fees should be interpreted as a red flag of a change in the risk of the company.

According to the literature, audit fees can change towards several different factors. They depend on company size (Simunic, 1980; Koh & Tong, 2013; Gietzmann & Pettinicchio, 2014; Han et al., 2016), financial condition (Stice, 1991; Craswell, Francis, & Taylor, 1995; Chang & Hwang, 2003; Desai Hogan, & Wilkings, 2006), auditee complexity (Craswell, Francis, & Taylor, 1995; Choi et al., 2008; Han et al., 2016), business risk (Bell, Landasman, & Shackelford, 2001; Koh & Tong, 2013), asset structure (Stice, 1991; Sundgren, 1998; Krishnan & Visvanathan 2009), earnings quality (Bartov, Gul & Tsui, 2000; Bedard & Johnstone, 2004; Abbott, Parker, & Peters, 2006; Dechow, Ge, & Schrand, 2010),

corporate governance (Chen et al., 2014; Srinidhi, Yan, & Tayi, 2015), and regulatory environment (Jaggi & Low, 2011; Su & Wu, 2017).

Based on prior research, auditors respond to the increase of risk of material misstatement by increasing their audit effort. This will decrease the detection risk and as result audit fees will increase subsequently (Allen et al., 2006; Budescu, Peecher, & Solomon, 2012). Also, with an emerging IT functions in the labour markets, auditors presenting outstanding skills will conduct to stronger internal controls and that will decrease the auditors' risk and audit fees (Chen et al., 2014). The assessment of the IT risk into the cybersecurity risk will increase higher fees to those clients who have more risk even when the incident has not occurred.

3. Research Hypotheses

The questions raised in the previous section, allow to formulate three hypotheses: H1, H2 and H3 about the relationship between cybersecurity incidents and audit fees.

3.1. Cybersecurity breaches and changes in audit fees

Following Rosati et al. (2017) and previous literature (Han et al., 2016), auditors should increase the level of audit fees (changes in audit fees represent a proxy of auditor's behaviour) in the year surrounding the data breach given both the increase in audit risks as well as the increase in the efforts to evaluate the impact of the incident on the financial statements of the company. The first hypothesis is stated as follows:

Hypothesis 1: Cybersecurity incidents are positively associated with audit fees.

3.2. Effects of changes in auditor and Industry specialist on Audit fees post- cybersecurity breaches

Following the study of Vonna Palmrose (1986) the audit size and knowledge is related with the provision of a high quality service, therefore industry specialist should charge higher fees. Given the increase of the audit risk after the data breaches is expected to find an increase of fees in the year of the cybersecurity incident and in the following periods. The second hypothesis is stated as follows:

Hypothesis 2: The changes in audit fees post-cyber security incidents are positively associated with the presence of an industry specialist.

Prior literature (Francis, 1984; Palmrose, 1986; Simon and Francis, 1988) highlighted that with a new auditor engagement client companies tend to pay lower fees compared to those expected given the characteristics of the customer.

The "fee cutting" has been demonstrated to be around 24% (Simon and Francis, 1988) and many times the fee reductions and auditor change is associated to a change in auditor quality which threatens auditor independence. Therefore following the prior literature is expected to find a decrease in audit fees in the year in which a new auditor has been hired but an increase of the fees after a data breach event. The third hypothesis is stated as follows:

Hypothesis 3 The changes in audit fees post-cybersecurity incidents are positively associated with a change of auditor.

4. Methodology

4.1 Sample selection

Similarly, to Rosati (2017), we begin the construction of our sample by identifying all firms in the database Audit Analytics Audit Fees from the 2015 to 2018. We applied a series of filters and eliminated all financial companies (with SIC Codes 6000-6999, since the different nature of their financial statements) firms which are not in Compustat, and firms with missing data.

To identify the cybersecurity data breaches, Privacy Rights Clearinghouse (PRC) database[24] has been used. This database identifies trends in privacy protection and enunciates its findings to advocates, policymakers, industry, media and consumers[25]. Previous studies like Garrison & Ncube (2011), Higgs et al. (2016) and Rosati et al. (2017) have adopted this dataset given that this database reports information that is detailed regarding the cybersecurity incidents which have affected US citizens. According to Rosati et al. (2017), the disclosure requirements allow researchers to consider the disclosure date of a subsequent incident through a close approximation of the discovery date, meaning that it is worth nothing the situations where some security breaches may only be found and discovered towards a significant amount of time or in some situations where the exact time and the duration of the breach may not be determined. Despite of some corporate events like mergers and acquisitions or earnings announcement, it is complex and hard to put together an extent list of

[24] Due to the increase in disclosure requirements and in the fact that PRC reunites information from multiple different sources, this dataset it gathers 1026 cybersecurity incidents disclosed by firms, non-profit organizations, healthcare organizations and government agencies in the US from April 2005 to September 2018.

[25] PRC is a California based non-profit corporation. The website for detailed information on data breaches is available at http://www.privacyrights.org/data-breach.

cybersecurity breaches since "many organizations are not aware they have been breached or are not required to report it based on reporting laws" (PRC, 2017).

In order to distinguish all the different types of cybersecurity incidents, the sample is not restricted to hacker attacks, meaning that the sample also includes other types of cybersecurity incidents (see Table 2 and Appendix A for more detailed information). As reported in Table 1, after matching with the Audit Analytics Fees and Compustat database, the final sample consists of 4,024 firms, 167 breached firms and 3,857 non-breached firms.

Table *1*

Sample selection

This table summarizes the sample selection process. Number of firms deleted at each step in parenthesis.

Data Source	Firms
AuditAnalytics audit fees file (2015-2018)	12,923
Less:	
Financial Companies	-2,249
Non-Compustat	-5,456
Missing Data	-1,194
Final sample	4,024
Breached	167
Non-breached	3857

4.2 A model to detect audit fees changes in the year of the data breaches

Following prior studies (e.g. Han et al., 2016; Hogan & Wilkins, 2008) and in order to test the first hypothesis from Rosati, Gogolin, and Lynn (2017), it has been used the yearly audit fees as a proxy for auditor's behaviour. Given that data are cross sectional and time-series in nature, according to the robust cluster

technique by Petersen (2009), the following regression model has been tested and controlled for heteroscedasticy and autocorrelation.

Therefore, similarly to Rosati (2017) the following regression model has been tested to verify the hypothesis 1:

$$LAF_{i,t} = \beta_0 + \beta_1 BREACH_{i,t} + \beta_2 LTA_{i,t} + \beta_3 LEV_{i,t} + \beta_4 CUR_{i,t} + \beta_5 QUICK_{i,t} + \beta_6 ROA_{i,t} + \beta_7 Log\_DEBTEQ_{i,t} + \beta_8 YE_{i,t} + \beta_9 BUSSEG_{i,t} + \beta_{10} ICWEAK_{i,t} + \beta\ Industry\ Indicators + \beta\ Year\ Indicators + \varepsilon_{i,t} \quad (1)$$

Where:

LAF= natural logarithm of audit fees;

BREACH= 1 if a firm experiences a cybersecurity incident in the year *t*, 0 otherwise;

LTA= natural logarithm of end of year total assets;

LEV= current liabilities divided by total assets;

CUR= current assets divided by total assets;

QUICK= difference between current assets and inventory divided by current liabilities;

ROA= net income (loss) divided by total assets;

Log_DEBTEQ= total debt divided by equity book value;

YE= 1 if a firm's fiscal year does not end on December 31, 0 otherwise;

BUSSEG= natural logarithm of the number of business segments in which a firm operates;

ICWEAK= 1 if a firm's internal controls were not found to be effective under Section 302 of the Sarbanes-Oxley Act of 2002, 0 otherwise;

Year Indicators= year indicators;

Industry Indicators= industry indicators based on two-digit SIC codes;

ε = error term.

Following the proxy model by Rosati, Gogolin, and Lynn (2017) and in order to be consistent with prior studies like Gul & Goodwin (2010), the first hypothesis represents a regression which includes controls variables for all the factors. First, in terms of firm size (*LTA*), there is a control for the audit effort. Second, the number of the business segments (*BUSSEG*) controls the firms' complexity. Third, there is an inclusion of the quick ratio (*QUICK*) and the ratio of current assets to total assets (*CUR*), in order to control for audit inherent risk. There are other factors which usually affect audit risk like firm's profitability (*ROA*), leverage (*LEV*), logarithm of debt-to-equity ratio (*Log_DEBTEQ*) and internal control weaknesses (*ICWEAK*). Last but not least, in this model it is included control variables for off-peak fiscal year-end (*YE*).

Furthermore, the first regression model in this paper goes forward from the studies presented in the paper of Rosati, Gogolin, and Lynn (2017), once new control variables have been included: Big4, Industry Specialist and Auditor Change. These three new variables have been integrated in the first regression model as well as in the following to test the hypothesis H2 and H3.

According to previous studies, the dummy Big4 assume value 1 if the auditor is a Big4 company, 0 otherwise, allowing to control for higher audit quality (Eshleman & Guo, 2014), more strictly control (Krishnan, Rama, & Zhang, 2008; De Franco et al., 2011), and also because Big4 auditors are able to charge higher fees to their clients (Choi et al., 2008) than non-Big4 auditors. For that reasons, the first regression includes the variable Big4 to ensure homogeneity in terms of audit quality (Blankley, Hurtt, & MacGegor, 2012). On the other hand, the variable Auditor Change represents the turnover within the companies' auditor after having a data breach. In this case, turns up to be interesting to study the relationship between audit fees and auditor change. The dummy variable

Industry Specialist supports the idea of an auditor being a market specialist (dummy=1) or not (dummy=0). Through the years and activities, this variable has been calculated considering the market share of the full sample of auditors included in Audit Analytics.

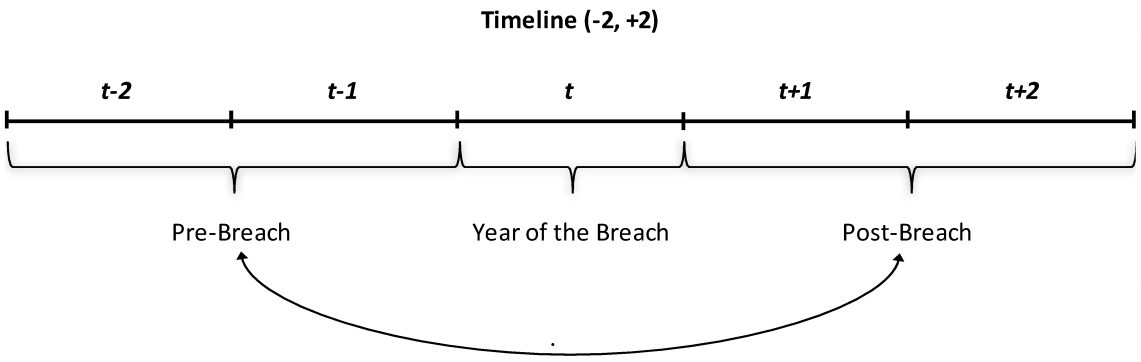
Moreover, each type of incident has been classified according with PRC: a Payment Card Fraud (CARD) is an indicator variable equal to 1 if a cybersecurity incident was due to payment card fraud and 0 otherwise; Unintended Disclosure (DISC) is an indicator variable equal to 1 if a cybersecurity incident was due to unintended disclosure and 0 otherwise; Hacking or Malware (HACK) is an indicator variable equal to 1 if a cybersecurity incident was due to a malicious outsider attack and 0 otherwise; Insider (INSD) is an indicator variable equal to 1 if a cybersecurity incident was due to malicious insider(s) and 0 otherwise; Physical Loss (PHYS) is an indicator variable equal to 1 if a cybersecurity incident was due to unauthorized physical access and 0 otherwise; Portable Device (PORT) is an indicator variable equal to 1 if a cybersecurity incident was due to stolen or lost portable device(s) and 0 otherwise; Stationary Device (STAT) is an indicator variable equal to 1 if a cybersecurity incident was due to stationary device(s) and 0 otherwise; and Unknown (UNKN) is an indicator variable equal to 1 if a cybersecurity incident was due to an unknown cause and 0 otherwise.

4.3 Event study to detect audit fees changes post - data breaches

In order to test both the hypothesis 2 and 3, has been performed an event study to test if the changes in audit fees, after the data breach, in related to both Industry Specialist and Audit Change. For this reason, the dummy POST assume value 0 for the two years prior to a breach and 1 for the year of the event and the two years following the breach. It is through this variable that is possible to study the volatility of fees before and after the breach and detect the behaviour of the companies since at this event. Specifically, the pre-breach period includes the two "fiscal years" before the breach, while post breach period includes the fiscal year of the breach and "two fiscal years" after the breach.

Figure 1

This figure provides a graphical representation of the timeline adopted in our analysis where t is the year in which a cyber security incident occurs. Note: the year of cyber-security incidents (t) is not considered whose objective is to directly compare the pre- and post-breach periods.



Thereby for the H2, the regression model is:

$$LAF_{i,t} = \beta_0 + \beta_1 BIG_{i,t} + \beta_2 INDUSTRY\_SPECIALIST_{i,t} + \beta_3 POST_{i,t} + \beta_4 LTA_{i,t} + \beta_5 LEV_{i,t} + \beta_6 CUR_{i,t} + \beta_7 QUICK_{i,t} + \beta_8 ROA_{i,t} + \beta_9 Log\_DEBTEQ_{i,t} + \beta_{10} YE_{i,t} + \beta_{11} BUSSEG_{i,t} + \beta_{12} ICWEAK_{i,t} + \beta Industry\ Indicators + \beta Year\ Indicators + \varepsilon_{i,t} \quad (2)$$

Where:

LAF= natural logarithm of audit fees;

BIG= 1 if an auditor's company is a Big4 in the year *t*, 0 otherwise;

INDUSTRY_SPECIALIST= 1 if an auditor's company is an Industry Specialist in the year *t*, 0 otherwise;

POST= 1 if a fiscal year is after a cyber security incident, 0 otherwise;

All the variables are defined as in the equation 1).

An extension of this model (2) includes the interaction term between the variable $INDUSTRY\_SPECIALIST_{i,t}$ x $POST_{i,t}$, and allows to verify the impact of the Industry Specialist in the year and after the data breaches events.

In order to test the H3, the following regression model has been estimated:

$$LAF_{i,t} = \beta_0 + \beta_1 BIG_{i,t} + \beta_2 AUDITOR\_CHANGE_{i,t} + \beta_3 POST_{i,t} + \beta_4 LTA_{i,t} + \beta_5 LEV_{i,t} + \beta_6 CUR_{i,t} + \beta_7 QUICK_{i,t} + \beta_8 ROA_{i,t} + \beta_9 Log\_DEBTEQ_{i,t} + \beta_{10} YE_{i,t} + \beta_{11} BUSSEG_{i,t} + \beta_{12} ICWEAK_{i,t} + \beta Industry\ Indicators + \beta Year\ Indicators + \varepsilon_{i,t} \quad (3)$$

Where:

AUDITOR_CHANGE= 1 if an auditor's company changes when a data breach occurs in the year *t*, 0 otherwise;

All the variables are defined as in the equation 1) and 2).

An extension of this model (3) includes the interaction term between the variable $AUDITOR\_CHANGE_{i,t}$ x $POST_{i,t}$, and allows to verify the impact of the Auditor Change in the year and after the data breaches events.

In order to test both the hypotheses 2 and 3, a sample that includes only the breached companies has been used. Moreover, all models 1,2,3 have been controlled for both Tolerance test, Variance inflation factor and Multicollinearity using variance inflation factors.

5. Analysis and discussion of empirical results

5.1 Descriptive statistics and Results

Table 2 reports the descriptive statistics in three different panels. Panel A reports the frequency of the cybersecurity incidents by year, while Panel B reports the frequency of the cybersecurity incidents by firm. Moreover, Panel C reports the frequency of cybersecurity incidents by breach type. By analysing the Panel A, the largest number of incidents in the sample (73) occurred in 2017, representing approximately 35%. Moreover, from analysing the Panel A, it is evident an increase of the number of incidents over time. In the Panel B, almost 29% of the firms who were affected by cybersecurity incidents were breached more than one time. The companies Bed Bath & Beyond, Intuit and InterContinental Hotels reported the highest number of incidents (four). Panel C shows that most of the incidents in the sample were due to malicious outsider attack (HACK), unintended information disclosure (DISC) and unknown factors (UNKN).

Table *2*

This Table represents the Frequency Distribution of Cybersecurity Incidents by Year (Panel A), by Firm (B) and Type (C)

Panel A: Cyber-security incidents by Year

Year	No. of breaches	%
2015	32	15, 17
2016	46	21, 80
2017	73	34, 60
2018	60	28, 44
Total	211	100

Panel B: Cyber-security incidents by Firm

No. of breaches	No. of firms	%
1	121	72,46
2	31	18,56
3	12	7,19
4	3	1,80
Total	167	100

Panel C: Cyber-security incidents by Type

Type	No. of breaches	Percentage	No. of firms	Percentage
DISC	31	14,69	20	12,74
HACK	101	47,87	75	47,77
INSD	5	2,37	3	1,91
PHYS	5	2,37	2	1,27
PORT	4	1,90	3	1,91
UNKN	61	28,91	50	31,85
Missing values	4	1,90	4	2,55
Total	211	100	157	100

Table 3 reports the Pearson correlation among the variables used in the analysis. Starting with variable *BREACH*, the correlation with audit fees (*LAF*) is positive and significant which means that when there is a breach, audit fees

should increase. Consistent with prior studies, the variables company size (*LTA),* company liabilities (*LEV),* current assets (*CUR),* company earnings *(ROA),* company complexity *(BUSSEG)* and internal controls (*ICWEAK)* are significant correlated with audit fees. Besides that, if we look at the dummy *BREACH,* this variable confirms our hypothesis (H1) given that it results to be positively related to LAF (audit fees).

Insert Table 3 here

Table *3*

This table reports the Pearson correlation coefficients among the main variables adopted in the empirical analysis. All variables are defined in Appendix B *, **, * denote significance at 1, 5 and 10 percent levels, respectively.**

Pearson Correlation Coefficients between Variables

Variables	LAF	BREACH	LTA	LEV	CUR	QUICK	ROA	LOG_DEBTEQ	YE	BUSSEG	ICWEAK	BIG	INDUSTRY_SPECIALIST	AUDITOR_CHANGE
LAF	1.000													
BREACH	0.086 **	1.000												
LTA	0.825 **	0.086 **	1.000											
LEV	-0.067 **	-0.002	-0.145 **	1.000										
CUR	-0.349 **	-0.028 **	-0.545 **	0.074 **	1.000									
QUICK	-0.132 **	-0.011	-0.133 **	-0.033 **	0.203 **	1.000								
ROA	0.166 **	0.011	0.263 **	-0.692 **	-0.125 **	-0.004	1.000							
Log_DEBTEQ	0.226 **	0.017 *	0.331 **	-0.001	-0.440 **	-0.326 **	0.046 **	1.000						
YE	-0.013	0.030 **	-0.018 *	0.003	0.086 **	-0.025 **	0.022 **	-0.096 **	1.000					
BUSSEG	0.403 **	0.016 *	0.433 **	-0.034 **	-0.283 **	-0.149 **	0.092 **	0.173 **	0.039 **	1.000				
ICWEAK	-0.453 **	-0.032 **	-0.543 **	0.069 **	0.259 **	0.086 **	-0.142 **	-0.088 **	-0.048 **	-0.263 **	1.000			
BIG	0.541 **	0.021 **	0.480 **	-0.055 **	-0.167 **	-0.041 **	0.098 **	0.123 **	-0.067 **	0.136 **	-0.286 **	1.000		
INDUSTRY_SPECIALIST	0.251 **	0.036 **	0.229 **	-0.016 *	-0.096 **	-0.023 **	0.035 **	0.047 **	-0.011	0.072 **	-0.114 **	0.315 **	1.000	
AUDITOR_CHANGE	-0.181 **	-0.016	-0.131 **	-0.008	0.049 **	0.015 **	-0.026 **	-0.018	0.001	-0.035 **	0.089 **	-0.182 **	-0.049 **	1.000

According to Table 4, the first regression based on the full sample (breached and not breached companies) is reported across four panels (1,2,3,4). In each panel it is adding more control variables in order to study the impact on audit fees. The results of the cross-sectional regression analysis demonstrate the impact of the cybersecurity incidents on audit fees, therefore the hypothesis of the positive relationship between cybersecurity incidents and change in audit fees in the year of the breach is verified. Column 1 suggests that in the year of the breach, audit fees increase. In fact, the dummy (*BREACH*) identifies the presence of a cybersecurity incidents in a specific year is significant and present a positive coefficient by explaining the increase in audit fees. The variables BREACH remains statistically significant ($p<0.001$) and positive across all models.

The auditors charge, on average, 26% higher audit fees to the breached firms in the year of the data breach. Therefore, the results allow to confirm the hypothesis 1 (H1). Moreover, Column B, demonstrates also an increase in audit fees increase when the auditor is a Big4. Additional results can be found in the Column C, that demonstrates that when the auditor is an industry specialist, audit fees are higher, this variable is positive and significant. The fourth panel, Column D shows that in presence of an AUDITOR CHANGE audit fees decrease, which are also in line with prior studies (Simon and Francis, 1988).

The Column E includes both INDUSTRY SPECIALIST and AUDITOR CHANGE. This means that even if it was controlled for industry specialist, big4 or auditor change, the variable BREACH remains positive and significant demonstrating that in the year of the incident, audit fees increase. Controls variables audit effort (*LTA*), audit risk (*LEV* and *CUR*) and auditee's complexity (*BUSEEG*), have a positive impact on audit fees. If the variable natural logarithm of total assets is positive and significant to audit fees, the complexity

of the companies increase, meaning the size of the company and subsequent audit fees also increase. Moreover, if the variable business segments (*BUSSEG*) is positive and significant to audit fees, this means that the complexity increases as well as the charges implemented. On the other hand, the variables audit risk (*QUICK, ROA, Log_DEBTEQ*) and the variable that reveals that auditees whose fiscal years do not end on December 31 (*YE*) are significant, but have a negative coefficient. This means that, for example, on variable QUICK, liabilities are higher than the sum of assets and inventory, which means there is more risk. Moreover, if ROA is significant but has also a negative coefficient, means that the risk is higher to get more operating income assets.

Insert Table 4 here

Table *4*

This table presents the results of the regression analysis for the model presented in Equation (1). The dependent variable is the natural logarithm of audit fees (LAF) for all the regressions. All other variables are defined in Appendix A. *, **, * denote significance at 1, 5 and 10 percent levels, respectively.**

Regression Results: Effect of Cyber-Security Incidents on Audit Fees - Full Sample (breached and not breached companies)

	(1)		(2)		(3)		(4)		(5)	
Variables	Coeff.	p-value	Coeff.	p-value	Coeff.	p-value	Coeff.	p-value	Coeff.	p-value
INTERCEPT	9.566	0.000 ***	9.606	0.000 ***	9.611	0.000 ***	9.386	0.000 ***	9.388	0.000 ***
BREACH	0.257	0.003 ***	0.274	0.001 ***	0.276	0.001 ***	0.259	0.002 ***	0.261	0.002 ***
LTA	0.554	0.000 ***	0.493	0.000 ***	0.491	0.000 ***	0.489	0.000 ***	0.488	0.000 ***
LEV	0.018	0.002 ***	0.018	0.001 ***	0.018	0.001 ***	0.049	0.000 ***	0.049	0.000 ***
CUR	1.081	0.000 ***	0.999	0.000 ***	0.999	0.000 ***	0.993	0.000 ***	0.994	0.000 ***
QUICK	-0.032	0.000 ***	-0.034	0.000 ***	-0.034	0.000 ***	-0.032	0.000 ***	-0.032	0.000 ***
ROA	-0.021	0.000 ***	-0.018	0.000 ***	-0.018	0.000 ***	-0.015	0.001 ***	-0.015	0.001 ***
LOG_DEBTEQ	-0.009	0.019 **	-0.008	0.036 **	-0.008	0.042 **	-0.006	0.136	-0.006	0.150
YE	-0.092	0.000 ***	-0.070	0.000 ***	-0.070	0.000 ***	-0.071	0.000 ***	-0.071	0.000 ***
BUSSEG	0.058	0.000 ***	0.064	0.000 ***	0.064	0.000 ***	0.067	0.000 ***	0.067	0.000 ***
ICWEAK	-0.038	0.036 **	0.012	0.487	0.012	0.502	0.015	0.442	0.014	0.462
BIG			0.531	0.000 ***	0.515	0.000 ***	0.526	0.000 ***	0.511	0.000 ***
INDUSTRY_SPECIALIST					0.059	0.000 ***			0.054	0.002 ***
AUDITOR_CHANGE							-0.288	0.000 ***	-0.2869	0.000 ***
Industry fixed-effect	0.002	0.000 ***	0.001	0.000 ***	0.001	0.000 ***	0.002	0.000 ***	0.002	0.000 ***
Year fixed-effect		Yes		Yes		Yes		Yes		Yes
R-squared		0.724		0.745		0.745		0.742		0.742
Adj. R-squared		0.723		0.744		0.745		0.741		0.742

Table 5 reports the results of the second model needed to test the second hypothesis. First, in Column 1, the variable POST breach is strongly positive and significant which explains that audit fees increase in the year and after the cybersecurity event despite but the dummy INDUSTRY SPECIALIST is not significant. However, in the Column 2, it has been examined the interaction term between POST x INDUSTRY SPECIALIST. In this case, the interaction is not statistically significant therefore we cannot demonstrate that in presence of an industry specialist and in the year and after the incidents the audit fees increase. Therefore the Hypothesis 2 is not confirmed.

Insert Table 5 here

Table *5*

This table presents the results of the regression analysis for the model presented in Equation (1). The dependent variable is the natural logarithm of audit fees (LAF) for all the regressions. All other variables are defined in Appendix B. *, **, * denote significance at 1, 5 and 10 percent levels, respectively.**

Regression Results: Effect of Cyber-Security Incidents on Audit Fees - Breached Firms

	(H2A)			(H2B)		
Variables	Coeff.	p-value		Coeff.	p-value	
INTERCEPT	10.759	0.000	***	10.767	0.000	***
LTA	0.490	0.000	***	0.490	0.000	***
LEV	-0.028	0.935		-0.035	0.919	
CUR	0.498	0.021	**	0.498	0.021	**
QUICK	0.025	0.328		0.025	0.327	
ROA	-1.096	0.009	***	-1.086	0.010	**
LOG_DEBTEQ	0.043	0.043	**	0.042	0.045	**
YE	-0.111	0.066	*	-0.111	0.067	**
BUSSEG	0.106	0.000	***	0.107	0.000	***
ICWEAK	0.258	0.006	***	0.258	0.006	***
BIG	0.137	0.298		0.138	0.296	
INDUSTRY_SPECIALIST	0.012	0.833		0.023	0.740	
POST	0.237	0.001	***	0.247	0.002	***
POST_AUDITOR_LEADER				-0.036	0.771	
Industry fixed-effect	-0.005	0.002	***	-0.005	0.002	***
Year fixed-effect		Yes			Yes	
R-squared		0.779			0.779	
Adj. R-squared		0.768			0.768	

Table 6, reports the results of the last model (3) needed to test the hypothesis of the changes in audit fees post-cybersecurity data breach when there is a change in auditor. The variable POST reported in Column 1 is positive and statistically significant which means that in the year and "post" breach the audit fees increase. The Column 2 includes the interaction term POST x AUDITOR CHANGE, the coefficient is positive and statistically significant, therefore post event and with the change in auditor audit fees increase. This means that new auditor face more audit risk and increase the audit fees.

Insert Table 6 here

Table *6*

This table presents the results of the regression analysis for the model presented in Equation (1). The dependent variable is the natural logarithm of audit fees (LAF) for all the regressions. All other variables are defined in Appendix B. *, **, * denote significance at 1, 5 and 10 percent levels, respectively.**

Regression Results: Effect of Cyber-Security Incidents on Audit Fees - Breached Firms

	Panel A (H3A)		Panel B (H3B)	
Variables	Coeff.	p-value	Coeff.	p-value
INTERCEPT	10.540	0.000 ***	10.490	0.000 ***
LTA	0.490	0.000 ***	0.487	0.000 ***
LEV	-0.013	0.969	-0.025	0.939
CUR	0.483	0.021 **	0.497	0.017 **
QUICK	0.026	0.283	0.025	0.306
ROA	-1.054	0.011 **	-1.049	0.011 **
LOG_DEBTEQ	0.044	0.037 **	0.043	0.041 **
YE	-0.109	0.074 *	-0.108	0.075 *
BUSSEG	0.106	0.000 ***	0.107	0.000 ***
ICWEAK	0.260	0.006 ***	0.261	0.006 ***
BIG	0.135	0.306	0.186	0.164
AUDITOR_CHANGE	-0.131	0.488	-0.262	0.192
POST	0.230	0.002 ***	0.221	0.002 ***
POST_AUDITOR_CHANGE			1.062	0.060 *
Industry fixed-effect	-0.005	0.002 ***	-0.005	0.002 ***
Year fixed-effect		Yes		Yes
R-squared		0.779		0.780
Adj. R-squared		0.769		0.770

6. Conclusion and Limitations

This paper addressed the question of how risk factors are disclosure in annual reports. Auditors have a key role in this development, they integrate the risks in of cybersecurity incidents in the audit fees. In this sense, the audit fees can be considered as a proxy to audit effort, audit risk and audit behaviour in the year and after the cybersecurity incidents. Basically, this paper approaches three questions. The first one investigates if the firms who have suffered a cybersecurity incident are charged with higher audit fees in the year of the breach, a positive and statistically significant relation between the increase in audit fees and the year of the breach has been found. The second one whether auditors are aware of the potential security issues before an incident occurs or if they revise their risk assessment following a cybersecurity breach, in other words if how an auditor that is industry specialist behave pre-post the cybersecurity events, this hypothesis is not demonstrated. The third result is related to the investigation weather the audit fees increase in the post-event and with the change in auditor. Differently from results of a prior study (Simon and Francis, 1988) that demonstrate a decrease in audit fees related with the change in auditor, after the breach and with an auditor changes, the fees increase.

Generally, the results obtained suggest that cybersecurity risk is positively associated with audit fees. This idea can be simply explained by the supposition where cybersecurity incidents and the subsequent perceived vulnerability of a firm towards these incidents result in higher risk of material misstatement, like audit risk. For that reason, audit firms increase their effort to ensure the endurance of their clients and reduce the risk from the disclosure of annual reports. This increase in audit risk and efforts lead to an increase in audit fees.

The empirical analysis provides more insights about the amount that auditors charge, on average, 26 percent higher audit fees to breached firms in the year when a cybersecurity incident occurs. Secondly, when there is an increase in audit fees on average of 53 percent when the auditor is a Big4.

The results obtained in thesis provide a little contribution in the research area of audit and cybersecurity. More than that, this study goes a long way in explaining empirical evidence on the effectiveness of auditing guidelines and risk assessment procedures, which can be interesting to regulators and practitioners.

About limitations, there is a possibility to go further in terms of studying the true effort and audit risk through another perceived vulnerabilities. Furthermore, according to Higgs et al. (2016), the database PRC does not incorporate the entire population of breaches. Alongside to this idea, this study is limited to US publicity traded firms and in the context of changes to the European Data Protection implementation; an international study in this area can be useful.

Despite of our study suggest that auditors incorporate cybersecurity risk into their audit risk model, the data does not provide insights into how and what extent is done. According to previous studies like Asare & Wright (2004), expert consultation, Low (2004), auditor specialization, Knapp & Knapp (2001), formalized instructions, they result in better audit risk assessment. Experimental or interview based studies might shed light on the tools and techniques that auditors adopt when considering client specific cybersecurity risk and the method for incorporating such risk into audit fees.

The question concerning how auditors are able to accurately assess cybersecurity risks is still an open question for future research. Internal data

provided by auditors or experimental study designs may be able to provide further insights in this respect.

In conclusion, there is still space for future research to examine how auditors perceived IT outsourcing or the use of cloud computing or other cybersecurity strategies that could contain both the company and audit risks.

References

Abbasi, A., Sarker, S., & Chiang, R. H. (2016). Big Data Research in Information Systems: Toward an Inclusive Research Agenda. *Journal of the Association for Information Systems,* 17(2), 1-22.

Abbott, L. J., Parker, S., & Peters, G. F. (2006). Earnings management, litigation risk, and asymmetric audit fee responses. *Auditing: A Journal of Practice & Theory,* 25(1), 85-98.

Almeida, G. (2016). Cybersecurity policy and lawmaking in the EU, US and Brazil. *Computer Law Review International,* 17(3), 71-75.

Allen, R. D., Hermanson, D. R., Kozloski, T. M., & Ramsay, R. J. (2006). Auditor risk assessment: Insights from the academic literature. *Accounting Horizons,* 20(2), 157-177.

Anderson, S. W., Christ, M. H., Decker, H. C., & Sedatole, K. (2014). The use of management controls to mitigate risk in strategic alliances: Field and survey evidence. *Journal of Management Accounting Research,* 26(1), 1-32.

Aral, S., Dellarocas, C., & Godes, D. (2013). Introduction to the special issue-social media and business transformation: A framework for research. *Information Systems Research,* 24(1), 3-13.

Asare, S. K., & Wright, A. M. (2004). The effectiveness of alternative risk assessment and program planning tools in a fraud setting. *Contemporary Accounting Research,* 21(2), 325-352.

Audit Analytics. (2016, January 14). *Cybersecurity Disclosure in Risk Factors*. Retrieved from https://www.auditanalytics.com/blog/cybersecurity-disclosures-in-risk-factors/

Bartov, E., Gul, F. A., & Tsui, J. S. (2000). Discretionary-accruals models and audit qualifications. *Journal of Accounting and Economics,* 30(3), 421-452.

Bedard, J. C., & Johnstone, K. M. (2004). Earnings manipulation risk, corporate governance risk, and auditors' planning and pricing decisions. *The Accounting Review,* 79(2), 277-304.

Bell, T. B., Landsman, W. R., & Shackelford, D. A. (2001). Auditors' perceived business risk and audit fees: Analysis and evidence. *Journal of Accounting Research,* 39(1), 35-43.

Benaroch, M., Chernobai, A., & Golstein, J. (2012). An internal control perspective on the market value consequences of IT operational risk events. *Accounting Information Systems,* 13(4), 357-381.

Biddle, G. C., Hilary, G. and Verdi, R. S. (2009). How does financial reporting quality relate to investment efficiency?. *Journal of Accounting and Economics,* 48(2), 112-131.

Bierend, D. (2012, March 12). It's time to take Cybersecurity Seriously. *Wired.* Retrieved from https://www.wired.com/2012/03/opinion-busseri-cybersecurity/

Blankley, A. I., Hurtt, D. N., & MacGregor, J. E. (2012). Abnormal audit fees and restatements. *Auditing: A Journal of Practice & Theory,* 31(1), 79-96.

Budescu, D. V., Peecher, M. E., & Solomon, I. (2012). The joint influence of the extent and nature of audit evidence, materiality thresholds, and misstatement type on achieved audit risk. *Auditing: A Journal of Practice & Theory,* 31(2), 19-41.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3), 431-448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1), 70-104.

Charette, R. N., Adams, K. M., & White, M. B. (1997). Managing risk in software maintenance. *IEE Software*, 14(3), 43-50.

Center for Audit Quality – CAQ. (2017, May 24). *How Auditing Profession Promotes Cybersecurity Resilience*. Retrieved from https://www.thecaq.org/cpas-role-addressing-cybersecurity-risk

Chang, C. J., & Hwang, N. C. (2003). The impact of retention incentives and client business risks on auditors' decisions involving aggressive reporting practices. *Auditing: A Journal of Practice & Theory*, 22(2), 207-218.

Chen, Y., Smith, A. L., Cao, J., & Xia, W. (2014). Information technology capability, internal control effectiveness, and audit fees and delays. *Journal of Information Systems*, 28(2), 149-180.

Choi, J. H., Kim, J. B., Liu, X. & Simunic, D.A. (2008). Audit pricing, legal liability regimes, and big 4 premiums: Theory and cross – country evidence. *Contemporary Accounting Research*, 25(1), 55-99.

Christopher, J., Sarens, G., & Leung, P. (2009). A critical analysis of the independence of the internal audit function: evidence from Australia. *Accounting, Auditing & Accountability Journal*, 22(2), 200-220.

CIO. (2016, March 24). *Why you need a CSO/CISO*. Retrieved from https://www.cio.com/article/3048074/careers-staffing/why-you-need-a-cso-ciso.html

Clarke, R. A., & Knake, R. K. (2010). Cyber war: The next threat to national security and what to do about it. *Harper Collins Canada*.

Colarik, A., & Janczewski, L. (2012). Establishing cyber warfare doctrine. *Journal of Strategic Security*, 5(1), 31-48.

Craswell, A. T., Francis, J. R., & Taylor, S. L. (1995). Auditor brand name reputations and industry specializations. *Journal of Accounting and Economics*, 20(3), 297-322.

Dechow, P., Ge, W., & Schrand, C. (2010). Understanding earnings quality: A review of the proxies, their determinants and their consequences. *Journal of Accounting and Economics*, 50(2), 344-401.

De Franco, G., Gavious, I., Jin, J. Y., & Richarson, G. D. (2011). Do private company targets that hire Big4 auditors receive higher proceeds?. *Contemporary Accounting Research,* 28(1), 215-262.

Deloitte. (2017). *Cybersecurity and the role of internal audit: An urgent call for action.* Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-cyber-ia-urgent-call-to-action.pdf

Desai, H., Hogan, C. E., & Wilkins, M. S. (2006). The reputational penalty for aggressive accounting: Earnings restatements and management turnover. *The Accounting Review,* 81(1), 83-112.

DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014:http://niccs.us-cert.gov/glossary#letter_c

Ernst and Young – EY. (2018). *Understanding the Cybersecurity Threat: The Board's Role.* Retrieved from

https://www.eds.b.ebscohost.com/eds/pdfviewer?vid=0&sid=2ca617da-bfa1-4c23-af48-cbc53b47c18a%40sessionmgr103

Eshleman, J. D., & Guo, P. (2014). Do Big4 auditors provide higher audit quality after controlling for the endenous choice of auditor?. *Auditing: A Journal of Practice & Theory*, *33(4), 197-219*.

Fennis, B., & Stroebe, W. (2014). Softening the Blow: Company Self-Disclosure of Negative Information Lessens Damaging Effects on Consumer Judgment and Decision Making. *Journal of Business Ethics*, 120(1), 109-120.

Francis, J. R. (1984). The effect of audit firm size on audit prices: A study of the Australian Market. *Journal of Accounting and Economics*, 6(2), 133-151.

Frino, A., Palumbo, R., & Rosati, P. 2017. Does Information Asymmetry Predict Audit Fees?. Capital Markets Cooperative Research Center (CMCRC), and University of Chieti - Pescara.

Garrison, C. P., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, 19(4), 216-230.

Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT security breaches: what do investors think?. *Information Systems Security*, 12(1), 22-33.

Gietzmann, M. B., & Pettinicchio, A. K. (2014). External auditor reassessment of client business risk following the issuance of a comment letter by the SEC. *European Accounting Review*, 23(1), 57-85.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security,* 19(1), 33-56.

Graham, J. R., Harvey, C. R., and Rajgopal, S. (2005). The economic implications of corporate financial reporting. *Journal of Accounting and Economics,* 40(1), 3-73.

Gul, F. A., & Goodwin, J. (2010). Short-term debt maturity structures, credit ratings, and the pricing of audit services. *The Accounting Review,* 85(3), 877-909.

Haislip, J. Z., Masli, A., Richardson, V. J., & Sanchez, J. M. (2016). Repairing Organizational Legitimacy Following Information Technology (IT) Material Weaknesses: Executive Turnover, IT Expertise, and IT System Upgrades. *Journal of Information Systems,* 30(1), 41-70.

Han, K., & Mithas, S. (2013). Information Technology Outsourcing and Non-IT Operating Costs: An Empirical Investigation. *MIS Quarterly,* 37(1), 315-331.

Han, S., Rezaee, Z., Xue, L., & Zhang, J. H. (2016). The association between information technology investments and audit risk. *Journal of Information Systems,* 30(1), 93-116.

Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics,* 31(3), 405-440.

Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The Relationship between Board-Level Technology Committees and Reported Security Breaches. *Journal of Information Systems,* 30(3), 79-98.

Hogan, C. E., & Wilkins, M. S. (2008). Evidence on the audit risk model: Do

auditors increase audit fees in the presence of internal control deficiencies? *Contemporary Accounting Research,* 25(1), 219-242.

Jaggi, B., & Low, P.Y. (2011). Joint effect of investor protection and securities regulations on audit fees. *The International Journal of Accounting,* 46(3), 241-270.

Johnstone, K. M., & Bedard, J. C. (2003). Risk management in client acceptance decisions. *The Accounting Review,* 78(4), 1003-1025.

Kajüter, P., Klassman, F., & Nienhaus, M. (2016). Do Reviews by External Auditors Improve the Information Content of Interim Financial Statements?. *The International Journal of Accounting,* 51(1), 23-50.

Klamm, B. K., Kobelsky, K. W., & Watson, M. W. (2012). Determinants of the persistence of internal control weaknesses. *Accounting Horizons,* 26(2), 307-333.

Knapp, C. A., & Knapp, M. C. (2001). The effects of experience and explicit fraud risk assessment in detecting fraud with analytical procedures. *Accounting, Organizations and Society,* 26(1), 25-37.

Koh, K., & Tong, Y. H. (2013). The effects of clients' controversial activities on audit pricing. *Auditing: A Journal of Practice & Theory,* 32(2), 67-96.

Krishnan, J., Rama, D., & Zhang, Y. (2008). Costs to comply with SOX Section 404. *Auditing: A Journal of Practice & Theory,* 27(1), 169-186.

Krishnan, G., & Visvanathan, G. (2009). Do auditors price audit committee's expertise? The case of accounting versus nonaccounting financial experts. *Journal of Accounting, Auditing & Finance,* 24(1), 115-144.

Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly,* 18(2), 122-136.

Li, C., Sun, L., & Ettredge, M. (2010). Financial executive qualifications, financial executive turnover, and adverse SOX 404 opinions. *Journal of Accounting and Economics*, 50(1), 93-110.

Lobo, G. J., & Zhao, Y. (2013). Relation between audit effort and financial report misstatements: Evidence from quarterly and annual restatements. *The Accounting Review*, 88(4), 1385-1412.

Low, K. Y. (2004). The effects of industry specialization on audit risk assessments and audit-planning decisions. *The Accounting Review*, 79(1), 201-219.

Masli, A., Peters, G. F., Richardson, V.J., & Sanchez, J. M. (2010). Examining the potential benefits of internal control monitoring technology. *The Accounting Review*, 85(3), 1001-1034.

Mathews, L. (2017, August 16). NotPetya Ransonware Attack Cost Shipping Giant Maersk Over 200 Million. *Forbes.* Retrieved from https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransonware-attack-cost-shipping-giant-maersk-over-200-million/#48119ea44f9a

NASDAQ. (2014, November 19). *Nasdaq Application*. Retrieved from https://listingcenter.nasdaq.com/ViewPDF.aspx?Material_Search.aspx?mcd=CD&cid=110&years=2018,2017,2016,2018,2017,2016,2015,2014,2013,2012,2011,2010,2009,2008,2007,2006,2005,2004,2003,2002&sub_cid=21&searchkeywords=&exactsearchddvalue=1&Print=N&materials=0&popularfl=

New York Stock Exchange – NYSE. (2018, December 27). *NYSE Listed Company Manual Rule 202.05 – Timely Disclosure of Material News Development*. Retrieved from http://wallstreet.cch.com/LCMTools/PlatformViewer.asp?selectednode=chp_1_3_2_3&manual=%2Flcm%2Fsections%2Flcm-sections%2F

Petersen, M. A. (2009). Estimating standard errors in finance panel data sets: Comparing approaches. *Review of Financial Studies,* 22(1), 435-480.

Ponemon Institute LLC. (2017, June 13). *2017 Cost of Data Breach Study: Global Overview.* Retrieved from http://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states?s=2017+Cost+of+Data+Breach+Study

Pratt, J., & Stice, J. D. (1994). The effects of client characteristics on auditor litigation risk judgements, required audit evidence, and recommended audit fees. *The Accounting Review,* 69(4), 639-656.

PricewaterhouseCoopers – PwC. (2016). *Turnaround and transformation in cybersecurity.* Retrieved from https://www.pwccn.com/en/retail-and-consumer/rcs-info-security-2016.pdf

PricewaterhouseCoopers – PwC. (2017). *Insurance 2020 & beyond: Reaping the dividends of cyber resilience.* Retrieved from https://www.pwccn.com/gx/industries/financial-services/publications/insurace-2020-cyber.html

Quigley, K., Burns, C., Stallard, K. (2015). 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly,* 32(2), 108-117.

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies,* 11(1), 74-104.

Rosati, P., Gogolin, F., and Lynn, T. (2017). *Audit Firm Assessments of Cyber-security Risk: Evidence from Audit Fees and SEC Comments*. Working Paper. Irish Centre for Cloud Computing & Commerce (IC4), and Queen's University Management School.

Securities and Exchanges Commission. (2018). *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (DHHS Publication Nos. 33-10459; 34-82746). Washington, DC: U.S. Securities and Exchange Commission.

Securities and Exchange Commission. (2015). *Regulation Systems Compliance and Integrity* (DHHS Publication No. 34-73639). Washington, DC: U.S. Securities and Exchange Commission.

Securities and Exchanges Commission. (2011). *CF Disclosure Guidance: Topic No.2* (DHHS Publication No. 2). Washington, DC: U.S. Securities and Exchange Commission.

Securities and Exchange Commission. (2002). *Certification of Disclosure in Companies' Quarterly and Annual Reports* (DHHS Publication Nos. 33-8124, 34-46427). Washington, DC: U.S. Securities and Exchange Commission.

Simon, D. T., Francis, J. R., & Tavi, G. K. (1988). The Effects of Auditor Change on Audit Fees: Tests of Price Cutting and Price Recovery. *The Accounting Review,* 63(2), 255-269.

Simunic, D. A. (1980). The pricing of audit services: Theory and evidence. *Journal of Accounting and Research*, 18(1), 161-190.

Solomon I., Shields, D., & Whittington, O. (1999). What Do Industry-Specialists Auditors Know?. *Auditing: A Journal of Accounting and Research,* 71(1), 191-208.

Srinidhi, B., Yan, J., & Tavi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems,* 75, 49-62.

Stefaniak, C. M., Houston, R. W., & Cornell, R. M. (2012). The effects of employer and client identification on internal and external auditors' evaluations of internal control deficiencies. *Auditing: A Journal of Practice & Theory*, 31(1), 39-56.

Stice, J. D. (1991). Using financial and market information to identify pre-engagement factors associated with lawsuits against auditors. *The Accounting Review*, 66(3), 516-533.

Stohl, M. (2007). Cyber terrorism: A clear and present danger, the sum of all fears, breaking point or patriot games?. *Crime, Law and Social Change,* 46, 223-238.

Su, X., & Wu, X. (2017). Public Disclosure of Audit Fees and Bargaining Power between the Client and Auditor: Evidence from China. *The International Journal of Accounting,* forthcoming.

Sundgren, S. (1998). Auditor choices and auditor reporting practices: evidence from Finish small firms. *European Accounting Review*, 7(3), 441-465.

Palmrose, Z. V. (1986). Audit Fees and Auditor Size: Further Evidence. *Journal of Accounting and Research*, 24(1), 97-110.

Willis North America. (2013, August). *Willis Fortune 1000 Cyber Disclosure Report.* Retrieved from http://blog.willis.com/wp-content/uploads/2013/08/Willis-Fortune-1000-Cyber-Report_09-13.pdf

Wittenberg-Moerman, R. (2008). The role of information asymmetry and financial reporting quality in debt trading: Evidence from the secondary loan market. *Journal of Accounting and Economics*, 46(2), 240-260.

World Economic Forum. (2016, January 11). *Global Risks Report 2017.* Retrieved from https://www.weforum.org/reports/the-global-risks-report-2017

Appendix A

This appendix presents a table where a definition in example cases regarding the different types of cybersecurity incidents are classify and reported, according to the Database Privacy Rights Clearinghouse.

Type	Definition	Example
CARD	Payment card fraud.	Company's Name: McFadden. Disclosure Date: January 6, 2016. No. Records Breached: Unknown. Brief Description: McFadden's costumers received phone calls about fraudulent charges made to their credit card, concerning the use of a fake one.
DISC	Unintended information disclosure.	Company's Name: DXC Technology. Disclosure Date: July 5, 2017. No. Records Breached: Unknown. Brief Description: An internet hyperlink containing patient information was accessible between a certain periods of time. The information included patient´s names, Medicaid ID numbers, names and addresses of healthcare providers, patient numbers, procedures codes, dates of service, and payment amounts.
HACK	Malicious outsider attack.	Company's name: Vtech. Disclosure Date: November 30, 2015. No. Records Breached: 5,100,000. Brief Description: Vtech notified customers of a data breach when hackers were able to gain access to children's photos, chat logs, children's names, genders and birthdates, account email addresses, passwords, secret questions and answers for password retrieval, IP addresses, mailing addresses and download history.
INSD	Malicious insider.	Company's Name: Anthem. Disclosure Date: July 31, 2017. No. Records Breached: 18,500. Brief Description: Anthem's had one employee who had been involved in a case of identity theft, and further investigation discovered that the worker had "emailed a file with information about Anthem companies' members to his personal email address", a year ago. In all, more than 18,500 Anthem Medicare members' Social Security and Medicare

		identification data may have been exposed.
PHYS	Physical loss.	Company's Name: T-Bird Restaurant Group, Inc. Disclosure Date: September 17, 2015. No. Records Breached: Unknown. Brief Description: The Outback Steakhouse notified employees of a data breach when the location was burglarized. The individual(s) managed to steal computer equipment including their point of sale computer terminal and back office computer. The point of sale computer contained information that included employee time sheet information, files that contained names and Social Security numbers.
PORT	A lost, discarded or stolen portable device.	Company's Name: Humana. Disclosure Date: October 9, 2015. No. Records Breached: 2,800. Brief Description: Humana notified Wisconsin members of a breach of customer information after an employee's vehicle was broken into and a company laptop was stolen along with a file containing customer information. The information compromised included member names, dates of birth, Humana and clinic names. The documents also included Humana member identification numbers of 250 of those individuals.
STAT	Stationary device.	Company's Name: Capital Financial Group. Disclosure Date: November 11, 2015. No. Records Breached: Unknown. Brief Description: Capital Financial Group had the Cindi Philips' office broken into and two computers were stolen. The computers stored files which included your personal information. The information included your name, marital status, employer information, net worth, home phone number, E-mail address, cell phone number, address, and Social Security Number.

Appendix B

This table provides the definition of the variables included in the analysis and the respective data sources.

Variables	Source	Definition
LAF	Audit Analytics - Audit Fees	Natural logarithm of audit fees.
LTA	Compustat	Natural logarithm of end of year total assets.
LEV	Compustat	Current liabilities divided by total assets.
CUR	Compustat	Current assets divided by total assets.
QUICK	Compustat	Difference between current assets and inventory divided by current liabilities.
ROA	Compustat	Earnings before interest and taxes divided by total assets.
LOG_DEBTEQ	Compustat	Total debt divided by equity book value.
BUSSEG	Compustat	Natural logarithm of number of business segments.
YE	Compustat	1 if a firm's fiscal year does not end on December 31, 0 otherwise.
ICWEAK	Compustat	1 if a firm's disclosure controls were not found to be effective under Section 302 of the Sarbanes-Oxley Act of 2002, 0 otherwise.
BREACH	Privacy Rights Clearinghouse	1 if a firm has a cyber-security incident in year t, 0 otherwise.
TREATMENT		1 if a firm belongs to the treatment sample (i.e. breached) used in the DID analysis for the effect of cyber-security incidents on audit fees, 0 otherwise.
CARD	Privacy Rights Clearinghouse	1 if a cyber-security security incident was due to payment cards, 0 otherwise.
DISC	Privacy Rights Clearinghouse	1 if a cyber-security security incident was due to unintended information disclosure, 0 otherwise.
HACK	Privacy Rights Clearinghouse	1 if a cyber-security security incident was due to a malicious outsider attack, 0 otherwise.
INSD	Privacy Rights Clearinghouse	1 if a cyber-security security incident was due to a malicious insider, 0 otherwise.
PHYS	Privacy Rights Clearinghouse	1 if a cyber-security security incident was due to unauthorized physical access, 0 otherwise..
PORT	Privacy Rights Clearinghouse	1 if a cyber-security security incident was due to lost or missing portable device(s), 0 otherwise.
STAT	Privacy Rights Clearinghouse	1 if a cyber-security security incident was due to stationary device(s), 0 otherwise.
POST		1 if a fiscal-year is after a cyber-security incident (Table 10) or after a SEC Comment Letter related to cybersecurity (Table 12), 0 otherwise.