THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF ACCOUNTING

Cybersecurity: The Evolution of Auditing

STEPHEN MORREALE
SPRING 2020

A thesis
submitted in partial fulfillment
of the requirements
for a degree in
Accounting
with honors in
Accounting

Reviewed and approved* by the following:

Shelley Curling
Assistant Teaching Professor of Accounting
Thesis Supervisor

Sam Bonsall
Associate Professor of Accounting
Honors Advisor

* Electronic approvals are on file.

ABSTRACT

This thesis explores the reasons why the Securities Exchange Commission(SEC) will require public companies to issue an audited cybersecurity report in the near future. Currently, there is no federal law or regulation in the United States that encompasses the reporting of cybersecurity information by companies. Due to government inaction, the SEC has released guidance regarding disclosure of cybersecurity information by public companies. Consequently, companies may have to report certain cybersecurity information if it will materially affect their financial statements based on the SEC guidance. These types of disclosures have been benchmarked to see how companies have responded to the guidance put forth by the SEC. However, since there is not a required audited cybersecurity report, the public's trust in this information is minimal. Through research, it was proven the factors of growing market demands and the COVID-19 Pandemic have led to the increased need of reliable cybersecurity information through an audited cybersecurity report.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

First, I would like to say thank you to my Thesis Supervisor, Shelley Curling, for supporting me throughout this whole process. Without your guidance, I would not have been able to develop my ideas into a thesis and accomplish this achievement. Next, I would also like to thank Sam Bonsall, who has served as my Honors Advisor, and all my the other Penn State professors for giving me the knowledge and work ethic to complete this thesis. Lastly, I would like to thank my family and friends for their continued support throughout my life.

Chapter 1

Current Laws and Regulations

Currently, there is increasing pressure on companies to provide investors with information surrounding their data privacy programs. Laws and regulations are even requiring companies to be more transparent with how they handle cybersecurity and consumer information. Since devastating data breaches are becoming more common, this information is crucial in determining how a company is mitigating these risks and protecting consumer privacy. However, even though the AICPA developed a cybersecurity framework called "SOC for Cybersecurity", Cybersecurity reports are not standardized nor required to be audited (Center for Audit Quality, 2019). Thus, the confidence level and quality of the cybersecurity information being released by companies is low. Due to developing market demands and the COVID-19 Pandemic, the Securities Exchange Commission(SEC) will require public companies to disclose audited cybersecurity reports in the foreseeable future. To understand the full background on why this regulation might occur, it is important to go through the current regulation, legislation, and guidance around disclosure of cybersecurity information in the United States and internationally.

1.1 International Law

Starting internationally, one of the most sweeping and impactful legislations to be passed to date was the General Data Protection Regulation(GDPR), which is specific to the European Union(EU). This legal framework became effective on May 25, 2018 after a 2-year transition period and it sets guidelines around the gathering of personal data for EU citizens (Fair, 2019). It

applies to any organization which intends to do business with EU citizens and the actual location of the business is not pertinent(Hertzberg, 2018). Any applicable organization which does not comply with the GDPR will be penalized and can pay up to the greater of $20 million or 4% of annual global revenues (Hertzberg, 2018). One of the requirements of the GDPR is the creation of Data Protection Officer(DPO), who oversees the privacy and compliance programs, procedures, and reporting (Hertzberg, 2018). The DPO also must guarantee compliance audits take place. Another important segment of the GDPR is the breach management aspect where the company must assemble a system to inform consumers no later than 72 hours after a significant data breach occurred with high risk of privacy harm (Hertzberg, 2018). The GDPR also facilitates transparency and demands organizations to store data for legitimate reasons and must tell consumers how their data is being used. Furthermore, companies have to update consumers when their data is being collected and the consumers must explicitly consent to their information being gathered. The GDPR holds companies accountable for cybersecurity and imposes sanctions when there are failures, which is what makes it so disruptive. Since the law became effective, "there has been 206,326 cases reported by supervisory authorities from 31 European Economic Area countries", which resulted in fines totaling over $63 million (Fair, 2020, p. 1). The struggle to develop a similar laws in United States is ongoing.

1.2 US Law

Because of the advent of the GDPR, cybersecurity has been a key concern for Washington legislators. In March of 2020, the Cyberspace Solarium Commission, which was established through the 2019 National Defense Authorization Act to "develop a consensus on a strategic approach to defending the US in cyberspace against cyber-attacks of significant

consequences" issued a report about cybersecurity (Smith, Neill, Klemash. 2020, p.7). The report recommended amending the Sarbanes-Oxley Act(SOX) to contain cybersecurity reporting requirements because it is a "critical component of its[The Company's] financial condition" (Smith, Neill, Klemash, 2020, p.7). Unfortunately, Congress has not made any progress toward adopting the recommendations of this report. Due to the lack of congressional action, the states have been left to fill in the gaps. For example, California passed the Consumer Privacy Act of 2018, which became effective in 2020 (Fair, 2019). This Act improved privacy rights and protections for the residents of California. Companies who do not comply with the law are subject to penalties up to $2,500 per violation and $7,500 per intentional violation (Fair, 2019). Besides the laws individual states have enacted, there is no unified law to govern cybersecurity disclosures like the GDPR. Therefore, the SEC has had to step in to issue guidance for public companies to address the cybersecurity concerns.

1.3 SEC Guidance

As mentioned before since there is no unified legislation to follow around cybersecurity, the SEC has issued guidance over the years to communicate the importance of focusing on cybersecurity. In 2011, the SEC's Division of Corporate Finance put forth guidance around cybersecurity information for the first time (Securities and Exchange Commission, 2011). With this guidance, a company may determine it is essential to disclose cybersecurity information in the 10-K report in order to keep the report from being misleading. This guidance still incorporates management's judgment in the process. These voluntary disclosures can affect the areas of risk factors, management's discussion and analysis, legal proceedings, and financial statements. The guidance, however, makes sure to state anything which would compromise the

company and provide a path to get around cybersecurity measures should not be disclosed. More recently in 2018, the SEC updated this guidance with the *Commission Statement and Guidance on Public Companies Cybersecurity Disclosures* to emphasize the continued importance of disclosing cybersecurity information without undermining the current system in place (Securities and Exchange Commission, 2018).

The main goal of the latest release was to reinforce what was said in the 2011 release, while also adding two more sections where cybersecurity information may be disclosed. The sections are "cybersecurity policies and procedures and insider trading prohibitions(Securities and Exchange Commission, 2018, p. 6)." The report focuses on the significance of producing and upholding strong policies associated with cybersecurity risks and problems. The report goes on to say that the companies are "required" to create effective disclosure controls which "enable them to make accurate and timely disclosures of material events, including those related to cybersecurity (Securities and Exchange Commission, 2018, pp. 6-7)." The effectiveness of these controls must be evaluated by management. Furthermore, the report also reminds the companies and management of the importance of the insider trading laws and their obligation to refrain from making selective disclosures of material nonpublic information related to cybersecurity. Another area highlighted in the report is the implication of making sure the periodic and current reports, like Form 10-K, Form10-Q, and Form 8-K, must include relevant, timely, and ongoing information on material cybersecurity information. Along with this guidance, the SEC Office of Compliance Inspections and Examinations(OCIE) has also issued a few risk alerts pertaining to cybersecurity(Securities and Exchange Commission, 2018; Smith, Neill, Klemash, 2020).

These risks alerts help to point to which cybersecurity risks companies may want to contemplate when assessing their own cybersecurity risks and disclosures and the most recent

alert came in 2020. For the 2020 report, the OCIE examined many broker-dealers, investment advisors, clearing agencies, national securities exchanges, and other SEC registrants(Securities and Exchange Commission, 2020). During this process, the OCIE discovered numerous industry practices for managing and maintaining cybersecurity. These incorporate the areas of "governance and risk management, access rights and controls, data loss prevention, mobile security, incident response and resiliency, vendor management, and training and awareness" (Securities and Exchange Commission, 2020, p. 2). The OCIE hoped the observations they found would help companies "to enhance their cybersecurity preparedness and operational resiliency" (Securities and Exchange Commission, 2020, p. 2). Lastly, the SEC also issued an investigative report in 2018 which reinforced the need to support effective internal controls surrounding the growing cybersecurity risks (Securities and Exchange Commission, 2018).

In this report, the SEC's Division of Enforcement along with the Division of Corporate Finance and the Office of the Chief Accountant performed an investigation into whether a sample of issuers who suffered cyber-related fraud may have violated federal securities laws by not maintaining a sufficient system of internal accounting controls. The requirements of Sections 13(b)(2)(B)(i) and (iii) of the Securities Exchange Act of 1934 are the laws called into question by this report (Securities and Exchange Commission, 2018). Each of the issuers investigated lost millions of dollars due to cyber-related frauds. Even though the SEC did not decide to pursue any actions as a result of the investigation, they still believe it was appropriate to release the report as a reminder to all issuers that these cyber risks should be considered when creating internal controls (Securities and Exchange Commission, 2018). The report calls for the issuers to reassess their internal controls due to the increasingly common cyber risks. With all of this guidance and reports developed by the SEC, it is crucial to examine how market participants

have reacted to see if they have taken everything addressed into consideration when issuing reports and to understand how there is much more room for the expansion of cybersecurity disclosures (Securities and Exchange Commission, 2018).

Chapter 2

Reaction to SEC Guidance

Due to the unprecedented times the world is in with the COVID-19 pandemic, companies had to quickly adapt to an almost complete virtual work environment. With numerous business processes moved online, risks surrounding protection of confidential and crucial company data have been amplified to a degree never seen before. At this moment in time, maintaining public trust with related cybersecurity disclosures which follow the guidance laid out by the SEC is crucial for a business's success. The public disclosures help to build trust because they aid in transparency and provide reassurance boards are astutely accomplishing their risk oversight roles. To see if these disclosures are being reported properly, the Public Accounting firm, Ernst & Young(EY), has analyzed 76 Fortune 100 public companies to see the cybersecurity disclosures they are making in proxy statements and Form 10-K filings from 2018 through May 31, 2020 (Smith, Neill, Klemash, 2020). EY has been doing this type of benchmarking analysis for the past 3 years and have uncovered some interesting findings.

Overall, EY has found through the examination companies are continuing to improve their cybersecurity disclosures with slight increases in many of the disclosures tracked. The areas EY concentrated on for this analysis were cybersecurity board oversight, statements on cybersecurity and data privacy risks, and risk management (Smith, Neill, Klemash, 2020). Furthermore, EY was able to uncover the persistent insufficiency of disclosures related to cyber-readiness simulations and the use of independent third-party advisors. From an EY perspective, these "practices are prevalent in the market and vital to enhancing cyber resiliency" (Smith,

Neill, Klemash, 2020, p. 1). Figure 1 summarizes EY's observations from 2018 to 2020. An important area discussed by EY is the Board-level committee oversight.

Table 1: Fortune 100 Company Cybersecurity Disclosures

Topic	Disclosure	2020	2019	2018
Board oversight				
Risk oversight approach	Disclosed a focus on cybersecurity in the risk oversight section of the proxy statement	89%	88%	79%
Board-level committee oversight*	Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters	87%	82%	74%
	• Disclosed that the audit committee oversees cybersecurity matters	67%	62%	59%
	• Disclosed oversight by a non-audit-focused committee (e.g., risk, technology)	26%	28%	20%
Director skills and expertise	Cybersecurity included among areas of expertise sought on the board or cited in at least one director biography	58%	51%	39%
	• Cybersecurity included among the areas of expertise sought on the board	37%	29%	22%
	• Cybersecurity cited in at least one director biography	46%	41%	30%

Management reporting structure	Provided insights into management reporting to the board and/or committee(s) overseeing cybersecurity matters	61%	58%	54%
	Identified at least one "point person" (e.g., the Chief Information Security Officer or Chief Information Officer)	33%	34%	25%
Management reporting frequency	Included language on frequency of management reporting to the board or committee(s), but most of this language was vague	47%	45%	38%
	Disclosed reporting frequency of at least annually or quarterly; remaining companies used terms like "regularly" or "periodically"	17%	17%	14%
Statements on cybersecurity risk				
Risk factor disclosure	Included cybersecurity as a risk factor	100%	100%	100%
	Included data privacy as a risk factor	99%	99%	93%
Risk management				
Cybersecurity risk management efforts	Referenced efforts to mitigate cybersecurity risk, such as the establishment of processes, procedures and systems	92%	91%	83%
	Referenced response readiness, such as planning, disaster recovery or business continuity considerations	62%	57%	50%
	Stated that preparedness includes simulations, tabletop exercises or response readiness tests	7%	3%	3%

	Included cybersecurity in executive compensation considerations	5%	1%	1%
Education and training	Disclosed use of education and training efforts to mitigate cybersecurity risk	29%	26%	18%
Engagement with outside security community	Disclosed collaborating with peers, industry groups or policymakers	12%	12%	7%
Use of external advisor	Disclosed use of an external independent advisor	16%	13%	16%
	Disclosed board engagement with an external independent advisor	5%	4%	3%

Source: (Smith, Neill, Klemash, 2020)

2.1 Board-level Committee Oversight

The data over the years showed more boards are allotting cybersecurity oversight responsibilities to a specific committee. For 2020, 87% of companies have given cybersecurity duties to at least one board-level committee, which was primarily the Audit Committee (Smith, Neill, Klemash, 2020). This was a 20% increase from 2018 and a 5% increase from 2019. In 2019, there was a major increase from 20% to 28% in boards assigning cybersecurity oversight to non-audit committees, which was usually risk or technology committees. Conversely, there was a slight decrease in 2020 to 26% (Smith, Neill, Klemash, 2020). Out of the boards who gave the oversight responsibility to the audit committee, almost 65% wrote those responsibilities in the audit committee charter. Also, out of the boards who assigned the cybersecurity duties to non-audit committees, almost all of them put the responsibilities in the charter. Another aspect

focused on in the study was whether the board identified a member on the board who possesses "skills and expertise" in cybersecurity (Smith, Neill, Klemash, 2020).

2.2 Director Skills and Expertise

The percentage of companies which talked about cybersecurity as a main qualification for board members has increased drastically throughout the past couple years. In 2020, 58% of companies looked for cybersecurity as a qualification for the board (Smith, Neill, Klemash, 2020). In years past, the percentage of boards who took this action was 39% and 51%(Smith, Neill, Klemash, 2020). However, only a few companies actually disclosed some type of cybersecurity experience in director biographies. Consequently, this means companies are starting to examine the need for board members to have cybersecurity expertise, but only a few of the companies researched have someone on the board with this type of experience (Smith, Neill, Klemash, 2020). Next, another fundamental aspect in this study is the percentage of companies who disclosed data privacy in the risk factors area in their 10-K report.

2.3 Data Privacy

Unsurprisingly, almost all(99%) of the observed companies reported data privacy in their risk factor disclosures in the 2020 10-K filings, compared with 93% in 2019 (Smith, Neill, Klemash, 2020). This follows the guidance put forth by the SEC. However, the way cybersecurity was classified as a risk varied among the companies. The companies which explicitly concentrated on data privacy as a material risk were not reported as often, which came to be about 24% (Smith, Neill, Klemash, 2020). These companies reported the risk as material because of "increasingly complex and changing data privacy regulations that create high

financial and legal exposure in addition to the reputational and operational risks involved" (Smith, Neill, Klemash, 2020, p. 3). Moreover, 30% reported data privacy together with cybersecurity. These companies believe these risks are both in the same category. Lastly, the remaining 45% of the companies broadly defined cybersecurity under information technology or regulatory risk. Overall, no matter how the risk is being classified, each company is addressing cybersecurity as a risk factor (Smith, Neill, Klemash, 2020). Another aspect reviewed in the analysis is compensation incentives, where the company considered cybersecurity in executive pay decisions.

2.4 Compensation Incentives

In relation to other areas of this study, the consideration of cybersecurity in compensation for executives was seldomly reported. Out of all the companies, only 5% made this type of disclosure, which came in the form of a qualitative factor surrounding annual incentive pay (Smith, Neill, Klemash, 2020). A few of these companies even acquired a shareholder proposal which requested to incorporate cybersecurity metrics into pay incentives for executives, which proves some key stakeholders want this to be implemented. However, out of the proposals which got to the voting stage, they averaged about 17% support (Smith, Neill, Klemash, 2020). Some of the reviewed companies explained this outcome by stating there is not a connection between executive performance and the deterrence of cybersecurity failures. Conversely, others reported this was already contemplated when assessing executives' accomplishments (Smith, Neill, Klemash, 2020). A way companies can determine if they are adequately prepared for a cyber-attack is through response readiness simulations and tabletop exercises.

2.5 Response Readiness Simulations and Tabletop Exercises

The amount of companies disclosing they performed response readiness simulations is small, but the number more than doubled from 2019 to 2020(3% to 7%) (Smith, Neill, Klemash, 2020). All of these companies reported the exercise occurred at the management level, not at the board level. According to EY, this type of simulation is vital when assessing preparation for cyber-attacks, which companies need to perform. It is logical because, if a cyber breach occurs, the companies reaction is primarily impromptu and may not be handled efficiently when a company is not adequately prepared. Also, the company can gain insights about the strengths and weaknesses of their cybersecurity program from the exercise, which can help them assess the efficiency and effectiveness of their plan (Smith, Neill, Klemash, 2020). To begin this process, management should identify the areas of concern and the board should participate in the areas where the financial impact would be most devastating to the company (Smith, Neill, Klemash, 2020). Lastly, the use of an external independent advisor or auditor would also be beneficial for a company when examining their cybersecurity program.

2.6 Independent Third Party Consultation

Similar to the reporting of response readiness simulations, the amount of companies which disclosed they consulted with an independent advisor remained low over the years. For 2020, only 12 companies made this disclosures versus 10 in 2019 and 12 in 2018 (Smith, Neill, Klemash, 2020). Additionally, only 4 companies specified the board met directly with the advisor. Having an independent third party review a company's cybersecurity system would increase the general public's trust of the effectiveness of the program. The National Association of Corporate Directors(NACD), which sole mission is to "elevate board performance by

providing information and insights", improved the Director's Handbook on Cyber-Risk Oversight in 2020 by motivating boards to communicate with external advisors to evaluate their cybersecurity programs (National Association of Corporate Directors, 2021; International Security Alliance & National Association of Corporate Directors, 2020). Even though the AICPA developed a Cybersecurity framework which includes guidelines to help assess a company's cybersecurity program, EY did not see any companies seeking an auditor to use this framework to form an attestation opinion (Smith, Neill, Klemash, 2020). After understanding the overall reaction by public companies through the research completed by EY, it is clear to see most companies have been committed to following the guidance put forth by the SEC. However, the full picture of the companies cybersecurity program is not totally clear for investors to make informed decisions, which is the overall goal of reporting. First, the pressure to achieve this goal has been brought upon by market demands.

Chapter 3

Growing Market Demands

Over the years, it has been clear cybersecurity has become a major issue for companies. Since 2011, the rise in cyber breaches has steadily increased by 400% for public companies with 140 breaches in 2019 (Hallas, 2020). This is an alarming number and it will only continue to grow due to the use of cloud services to store critical company and consumer information coupled with the progression of online business processes. Furthermore, it is also concerning that, on average, it took companies 108 days to figure out a breach had occurred (Hallas, 2020). Because of the severity of this issue, investors are searching for more clarity around how a company is preparing to stop and handle these attacks to make better investment decisions. Furthermore, the market is demanding more trustworthy cybersecurity information, which is qualitatively and quantitatively evidenced through research, because of the costliness of breaches for companies and increases in cybersecurity spending by companies. First, the qualitative evidence of the market demanding more cybersecurity information will be explored.

3.1 Qualitative Evidence of Market Demands

Most of investors believe cybersecurity is a vital factor in risk oversight and are becoming more involved with the companies they invest in to better comprehend how cybersecurity is being handled. Through EY as part of the annual *EY Center for Boards Matter* investor sentiment research, it was proven cybersecurity is one of the key issues in minds of institutional investors (Smith, Neill, Klemash, 2020). In the fall of 2018, after questioning about 60 institutional investors encompassing around $32 trillion in assets under management, 61% said “cybersecurity, regardless of sector, was among the elevated risk issues, even though

investors characterize cyber risk as a pervasive and standard risk impacting all companies" (Smith, Neill, Klemash, 2019, p. 3). The main interests identified throughout the research were:

- The organization of oversight within companies
- Director knowledge on cyber problems
- Who is reporting to the board about cyber issues and how often
- The primary ways of how management is mitigating cyber risk
- Compliance with new data privacy laws and regulations (Smith, Neill, Klemash, 2019).

In 2019, after questioning the same institutional investors, EY concluded similar findings as 2018. For this study, EY asked what the investors thought the biggest threat to their portfolio would be in the next 3 to 5 years (Smith, Neill, Klemash, 2020). Out of all the risks, cybersecurity and data privacy ranked third, keeping in mind this was well before the COVID-19 pandemic. Additionally, investors stated every company is exposed to these risks and, in a digitalized world, the risks expand exponentially (Smith, Neill, Klemash, 2020). Since the investors believed this risk cannot be completely eliminated, they were very interested in how the company would respond to a breach and mitigate the damage. Some investors even reported asking their portfolio companies if they were planning to have an independent assessment of their cybersecurity program (Smith, Neill, Klemash, 2020). These studies prove the cybersecurity risk is clearly in the minds of investors. Moreover, another angle to further prove investor sentiment about cybersecurity quantitively is to analyze how a company's share price changes after reporting a data breach.

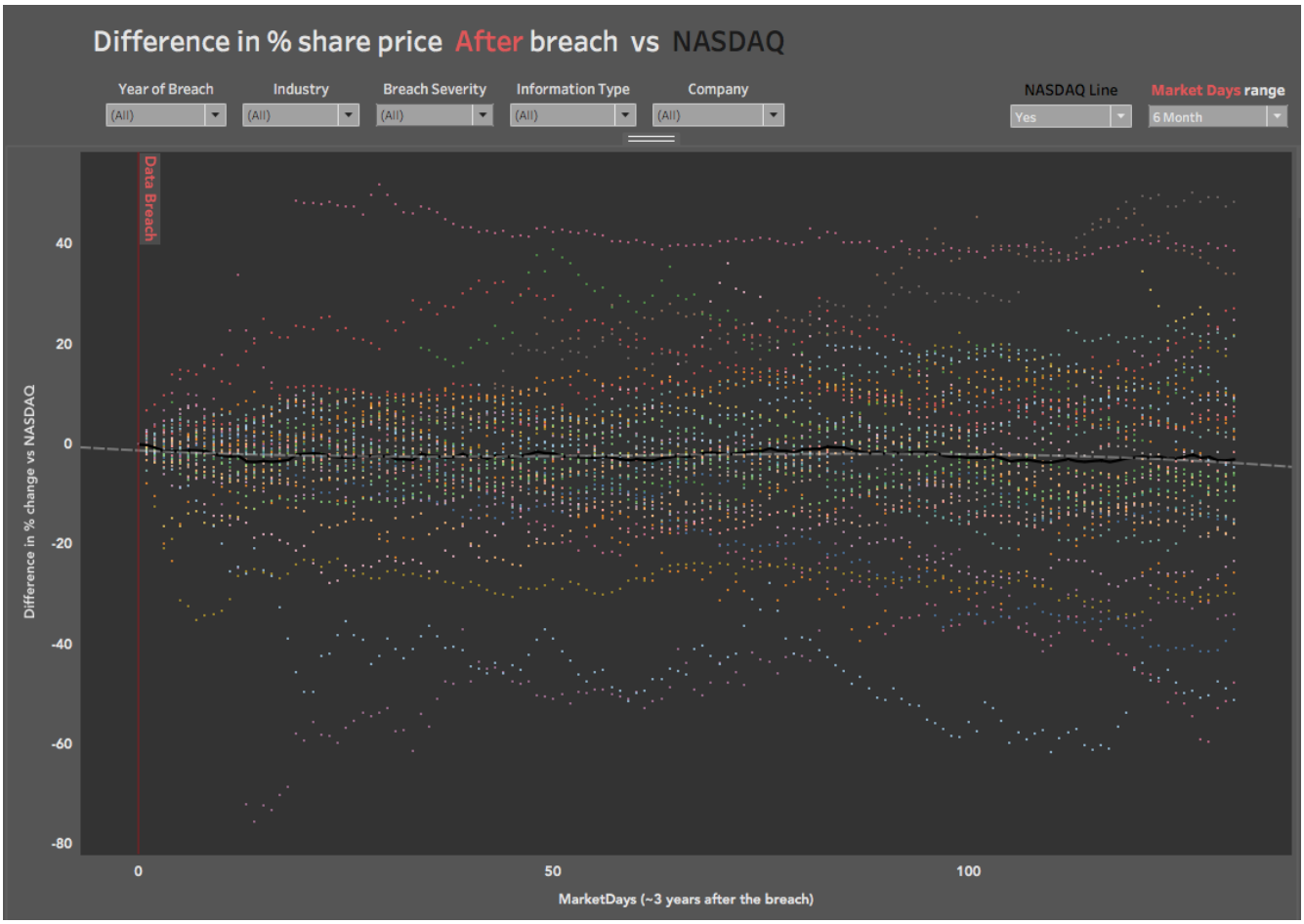
3.2 Quantitative Evidence of Market Demand

When determining if investors are demanding more cybersecurity information, it is insightful to examine how companies' share price changes after a data breach. Logically, if investors are truly concerned about cybersecurity and wanted to know more information about companies' programs, there would be negative investor reactions to breach disclosures. Through a recent study, Paul Bischoff, named a consumer privacy expert and editor of Comparitech, was able to visually show the relationship between companies' share prices and data breaches, which led to significant insights (Bischoff, 2021). The overall question Bischoff desired to answer through his study was "how do investors react to data breaches" (Bischoff, 2021, para. 2)? To attempt to answer this question, Bischoff analyzed the share price of 34 companies listed to the NYSE, encompassing roughly 5 industries (Bischoff, 2021). To begin the study, Bischoff had to determine which companies to pick and the overall basis to follow to complete the study.

For a company to be analyzed, they had to experience a breach of 1 million or more records, had to be on the listed on the NYSE at time of breach disclosure, and had to publicly disclose the breach (Bischoff, 2021). For the complete list of companies, look to Appendix A. The breaches analyzed for the 34 companies originated from 2007 to 2020. The key performance metric the researchers compared the stock price performance to was the NASDAQ, which is a common market performance indicator and many of the companies reviewed are listed on this exchange (Bischoff, 2021). Basically, the NASDAQ index was the baseline "0" value on a graph. For example, if a company's stock price fell 2% after breach disclosure and the NASDAQ rose 2%, then the calculated decrease for the study would be 4%. Furthermore, if the NASDAQ rose by 3%, but the company only rose by 2%, this would be a 1% decrease for the company in the study. Lastly, if the company's stock price fell 1% and the NASDAQ fell 2%, this would be a

relative increase of 1% for the company (Bischoff, 2021). The essential focuses of the study were the overall effect of a data breach on closing share price at different time periods and the percent difference in closing share price performance versus the NASDAQ over the same period. As with all studies, there are always limitations. The main limitation of this study is stock prices tend to be very volatile and there are many factors that can affect the price (Bischoff, 2021). It would be impossible to account for every one, so there will be some inconsistencies in the data. The tool used to conduct this analysis was tableau and Figure 1 below shows the difference in share price vs. NASDAQ after the breach for a 6 month period (Bischoff, 2021).

Figure 1: Difference in % Share Price After Breach vs NASDAQ



Source: (Bischoff, 2021)

Although slightly overwhelming, this graph is very useful and interactive while in Tableau. Across the top, the year of breach, industry, breach severity, information type, company, and more can all be adjusted for different parameters to gain different insights. The dots in the graph represent a separate company data breach incident, but the key is not pictured here due to size limitations. However, the full legend can be viewed in Appendix B. The Y axis represents the percentage change in relation to the NASDAQ, while the market days is on the X axis. Currently, the graph only shows up to 6 months or 180 market days, but this can be adjusted to show a max of 3 years. However, it is worth noting the effect of the data breach on investors likely wears off as the time period increases, so 6 months was determined to be the best time period to gain the most knowledge. As mentioned before, the "0" value, which is the gray dotted line, is the NASDAQ baseline. Appendix C shows another one of these graphs adjusted for different parameters. The main takeaways after analyzing the graphs from Bischoff's research include:

- Share prices of the companies hit a minimum point about 110 days after the breach. The prices, on average underperformed the NASDAQ by about -3.5%
- After 1 year, share prices underperformed the NASDAQ by about -8.6%. After 2 years, share prices underperformed the NASDAQ by about -11.6%. Lastly, after 3 years, the share prices underperformed NASDAQ by about 15.6%
- Breaches where very sensitive information is stolen like social security numbers see a bigger short term drop on average (Bischoff, 2021).

Additionally, through this research, it was proven investors are sensitive to cybersecurity breaches and react negatively when compared to the overall market. Now, since the market

demand for cybersecurity information has been proven to exist both qualitatively and quantitatively, it is time to look deeper into why this demand is there in the first place.

3.3 Costliness of Breaches and Increases in Cybersecurity Spending

The reasons why investors are demanding more cybersecurity information are the costliness of breaches and the increases in cybersecurity spending. As mentioned before, the number of cyber-attacks are progressively rising every year. Consequently, this is causing a rise in cost for companies. In a 2019 report completed by IBM, only 1 data breach can cost a company almost $4 million, which is 12% higher than 2014 (IBM, 2019). Moreover, the report conveys the consequences of these attacks can remain for years (IBM, 2019). Astoundingly, for some industries like healthcare and financial services, the costs incurred in the second and third years are the most costly (IBM, 2019). Wendi Whitmore, global lead for IBM X-Force Incident Response and Intelligent Services, said the following:

> "Cybercrime represents big money for cybercriminals, and unfortunately that equates to significant losses for businesses. Companies need to be aware of the full financial impact that a data breach can have on their bottom line and focus on how they can reduce this costs" (IBM, 2019, para. 4).

In addition, a 2019 Juniper Research report hypothesized that the expense from this attacks will grow to $5 trillion by 2024 (Barth, 2019). As a result of this increased threat, management of companies have judiciously increased their spending on cyber protection. A PwC Global State of Information Security Survey found that 87% of global CEOs are increasing investment into cybersecurity controls (PwC, 2018). Due to the increased cost and spending on cybersecurity, investors want to know if this risk is being effectively and efficiently alleviated. However, the

market has not sufficiently provided complete and trustworthy information yet, which creates a hole that needs to be filled by possible legislation. Another recent development has added even more pressure to this issue, which is the COVID-19 Pandemic.

Chapter 4

The COVID-19 Pandemic

The COVID-19 Pandemic has created a Cyber Pandemic. Once COVID-19 surged, businesses were forced to rapidly adapt to online working environments without any notice. Quite frankly, a Pandemic of this magnitude has not been seen since the Spanish Flu and companies were not prepared for it. Although communication and other technology made the work from home transition easier, security controls struggled to keep up with the speed of the conversion. As a consequence, cyber criminals have been empowered to take on vulnerable systems and exploit weaknesses. The COVID-19 pandemic has exponentially increased the cyber risk for companies, which has exacerbated the need for transparency through an audited cybersecurity report for investors. It is important to first recognize how and why the Pandemic has caused so much disruption in the cyber world.

4.1 Increased Risk

Companies have had to shift to all remote working to protect their employees and continue to assist their customers, which is the main reason behind the increased cybersecurity risk. 71% Security professionals in companies report increased security threat (Performance Improvement Partners, 2020). The vast majority of the businesses' activities have become virtual. Additionally, taking into account the promptness this change had to occur, the companies have been susceptible to different risks that may not have been imagined pre-COVID-19. For example, the IT Function is pressured by necessity to give access and capacity to some workers who have never worked from home before (Deo, Raj, Perumal, 2020). This calls for new cooperation software to help employees smoothly communicate and complete the same work

load. Moreover, company management needs remote access to sensitive internal services and information. Also, for most organizations, the Business Continuation Plans(BCP) and the Incident Response Plans(IPR) were not appropriate for a global pandemic. IT Departments realize the need for this to be protected and to place controls, but this is a difficult task due to limited scalability and amount of time (Deo, Raj, Perumal, 2020). As a result, hackers see the complexity of the situation and are seizing the opportunity to wreak havoc on businesses.

4.2 Common Cyber Attacks

Cybercriminals are exploiting the digitalized environment to hone in on weaknesses and steal money. According to the FBI, there has been a 300% in cyber related crimes since the start of the coronavirus (Performance Improvement Partners, 2020). One of the most common attacks is COVID-19 themed phishing emails (Deo, Raj, Perumal, 2020). Once unsuspecting employee clicks on the phishing email, he or she will have allowed malicious attachments to place malware into their system and cause disruption or steal private data (Deo, Raj, Perumal, 2020). Another common attack cybercriminals are deploying is the creation of temporary websites (Deo, Raj, Perumal, 2020). These fake websites contain malicious codes and the perpetrators try to attract employees to visit. Once the employee is on the website, it deposits the bad code into the employee's device. The websites also solicit donations from the employees. Lastly, since many businesses have begun using video conferencing systems like Zoom, cyber criminals have hacked into meetings where important company information is being discussed(Deo, Raj, Perumal, 2020). Since the heightened risk of cyber-attacks with COVID-19 is known by the SEC, it issued an alert in response to aid organizations in protecting themselves and the

addressed companies are still expected to follow the guidance brought in Chapter 1, but this does not go far enough in providing information to investors (Center for Audit Quality, 2020).

The SEC's Office of Compliance issued an Alert after noticing the increase in ransomware attacks on SEC registrants to inform companies of how they were using COVID-19 as the subject to mislead employees (Center for Audit Quality, 2020). As further explanation to help auditor's assess risks of material misstatement and to determine if the company has fairly disclosed all pertinent cybersecurity information, the Center for Audit Quality released a report titled *Understanding Cybersecurity and External Audit in the COVID-19 Environment*. This report states:

> "As companies evolve to respond to these new or increasing cyber-related risks, auditors will need to update their understanding of the IT environment accordingly, and revise risk assessments and audit procedures to be responsive to any new or different risks of material misstatement that could impact the financial statements and/or ICFR" (Center for Audit Quality, 2020, p. 3).

In other words, auditors will need to reassess how companies internal controls are performing to determine if there will be any effect on the financial statements due to COVID-19. However, with no standardized cybersecurity audit report, the quality and comparability of this information is muted. With the onset of COVID-19, the pressure to make this information available greatly increases.

4.3 Conclusion

In conclusion, the public would greatly benefit from the SEC requiring public companies to release an audited cybersecurity report. First, developing market demands have shown

investors are interested in receiving more of this information due to the high cost of data breaches and the increased spending by companies on cybersecurity. Qualitatively, it was shown cybersecurity is a key issue for investors through investor outreach research performed by EY. Additionally, a study completed by Paul Bischoff revealed the negative relationship between companies' share price and their data breaches to quantitatively indicate investor concern for cybersecurity information. Lastly, the COVID-19 Pandemic has amplified the need for audited cybersecurity reports due to the elevated cyber risk in a work-at-home environment. The market needs trust and transparency to function and investors will rely more on this cybersecurity information if it is standardized through a report and audited by an independent party.

Appendix A

List of 34 Companies Used for Bischoff's Study(2007-2020)

Adobe($ADBE)	Apple($AAPL)	Anthem($ANTM)	Capital One($COF)	Community Health Systems($CYH)
Dun & Bradstreet($DNB)	Facebook($FB)	First American Financial($FAF)	Ebay($EBAY)	Equifax($EFX)
Estee Lauder($EL)	Global Payments($GPN)	Health Net($HNT)	Heartland Payment Systems($HPY)	Home Depot($HD)
JP Morgan Chase($JPM)	LabCorp($LH)	LinkedIn($LNKD)	Marriott International($MAR)	MGM Resorts($MGM)
Microsoft($MSFT)	Monster($MWW)	Quest Diagnostics($DGX)	Royal Bank of Scotland ($RBS)	Sony($SNE)
Staples($SPLS)	Target($TGT)	TJ Maxx($TJX)	T-Mobile($TMUS)	Under Armour($UAA)
Vodafone ($VOD)	Walgreens($WBA)	Yahoo($YHOO)	Zynga($ZNGA)	

Source: (Bischoff, 2021)

Appendix B

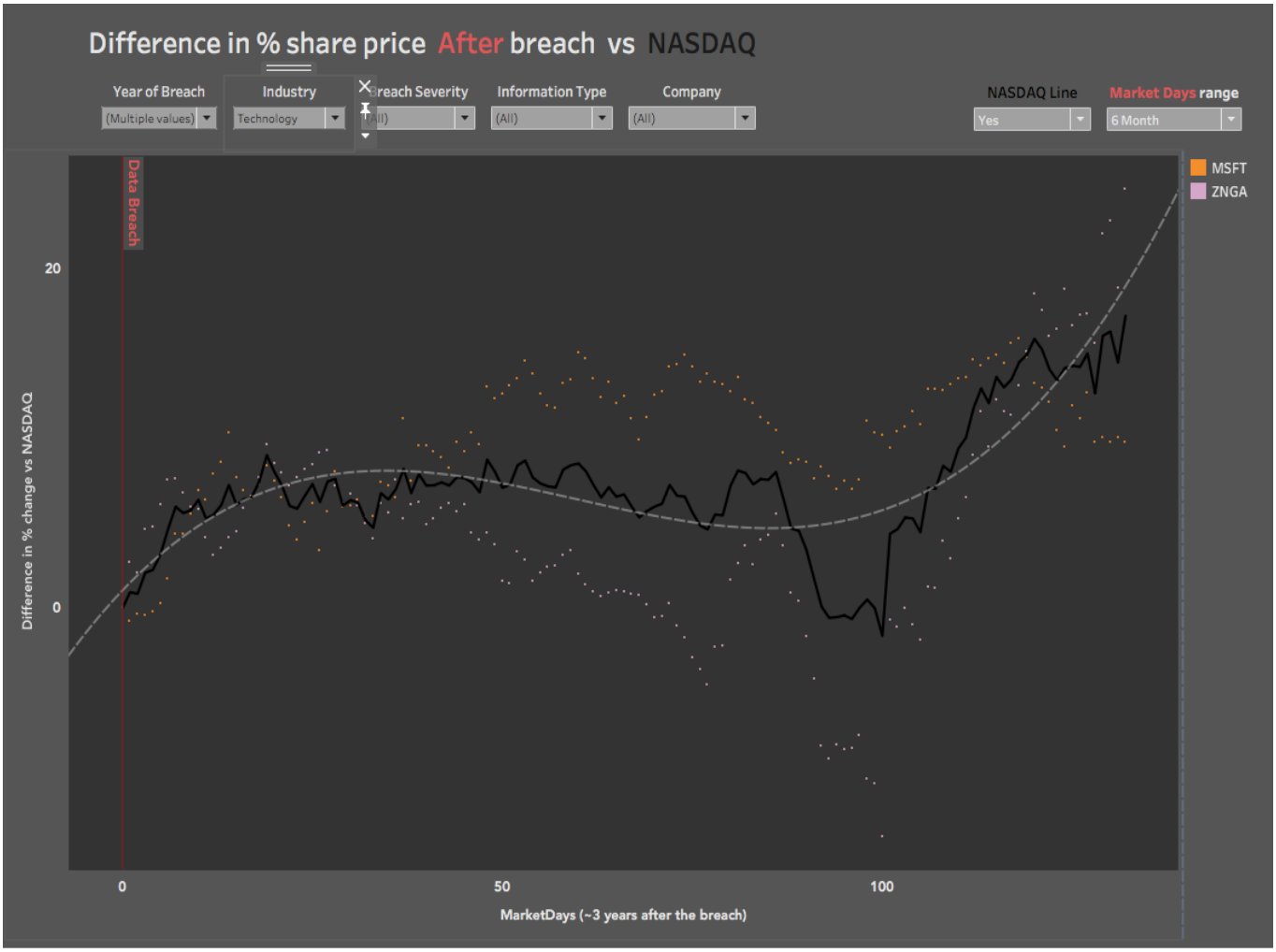
Legend for Separate Company Data Breach Incidents

Each company is listed by the stock ticker. Sometimes, if more than one data breach was tracked for the same company, it was separated by the date of the breach in the legend(Bischoff, 2021).

Appendix C

Data Breach Graph Examples from Tableau

This graph is adjusted by year of breach(only shows 2019 and 2020) and the industry(only Technology).



Source: (Bischoff, 2021)

Bibliography

Barth, B. (2019). *Date Breaches Expected to Cost $5 Trillion by 2024*. SCMagazine. Retrieved on March 11, 2021, from https://www.scmagazine.com/home/research/annual-global-data-breach-costs-to-exceed-5-trillion-by-2024-report/

Bischoff, P. (2021). *How Data Breaches Affect Stock Market Share Prices.* Comparitech. Retrieved March 7, 2021, from https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/#:~:text=Share%20prices%20of%20breached%20companies,six%20months%20prior%E2%80%94just%20barely

Center for Audit Quality. (2019). *The Role of Auditors in Company-Prepared Information: Present and Future*, CAQ, 1-5.

Center for Audit Quality. (2020). *Understanding Cybersecurity and the External Audit in the COVID-19 Environment.* CAQ. https://www.thecaq.org/wp-content/uploads/2020/07/caq_understanding-cybersecurity-covid-19_2020-07.pdf

Deo, P, Raj, G., & Perumal R. (2020). How Covid-19 is Dramatically Changing Cybersecurity. Tata Consulting Servcies. https://www.tcs.com/content/dam/tcs/pdf/perspectives/covid-19/How%20Covid-19%20is%20Dramatically%20Changing%20Cybersecurity.pdf

Division of Corporate Finance Securities Exchange Commission. (2011). *CF Disclosure Guidance: Topic No. 2*. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Fair, E. (2019). *Data Privacy in a Data-Driven World*. Pennsylvania CPA Journal, 3–4.

Frankenfield, J. (2020). *General Data Protection Regulation(GDPR).* Investopedia. Retrieved

March 5, 2021, from https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp#:~:text=The%20General%20Data%20Protection%20Regulation%20(GDPR)%20is%20a%20legal%20framework,the%20European%20Union%20(EU).&text=The%20GDPR%20mandates%20that%20EU,a%20number%20of%20data%20disclosures

Hallas, N. (2020). *Trends in Cybersecurity Disclosures.* Audit Analytics. Retrieved March 7, 2021, from https://blog.auditanalytics.com/trends-in-cybersecurity-breach-disclosures-2/

Hertzberg, J. (2018). *GDPR and Internal Audit*. Internal Auditor, 75(4), 22–23.

IBM. (2019). *IBM Study Shows Data Breach Costs on the Rise.* IBM. Retrieved on March 10, 2021, from https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

Internet Security Alliance & National Association of Corporate Directors. (2020). *Cybersecurity Risk Oversight 2020.* Isalliance. http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf

National Association of Corporate Directors. (2021). *About NACD.* NACD. Retrieved March 12, 2021, from https://www.nacdonline.org/about

Performance Improvement Partners. (2020). *COVID-19 Cybersecurity Statistics.* Pipartners. Retrieved on March 14, 2021, from https://www.pipartners.com/covid-19-cyber-security-statistics-40-stats-and-facts-you-cant-ignore/

PwC. (2018). *Revitalizing Privacy and Trust in a Data Driven World.* PwC. https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

Securities and Exchange Commission. (2018). *Commission Statement and Guidance on Public*

Company Cybersecurity Disclosures. https://www.sec.gov/rules/interp/2018/33-10459.pdf

Securities and Exchange Commission. (2020). *Cybersecurity and Resiliency Observations.* *https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf*

Securities and Exchange Commission. (2018). *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements.* https://www.sec.gov/litigation/investreport/34-84429.pdf

Smith, J., Neill, B., & Klemash, S. (2019). *What Companies Are Sharing about Cybersecurity Risk Oversight.* EY. https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/cbm/ey-cbm-cybersecurity-risk-oversight-final-eycom.pdf

Smith, J., Neill, B., & Klemash, S. (2020). *What Companies Are Sharing about Cybersecurity Risk Oversight.* EY. https://www.ey.com/en_us/board-matters/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight

ACADEMIC VITA

Stephen S. Morreale

EDUCATION

The Pennsylvania State University — **University Park, PA**
Schreyer Honors College | Smeal College of Business — *Graduation: May 2021*
Masters of Accounting | Bachelor of Science in Accounting — Dean's List All Semesters
Coursework concentration on Data Analytics

PROFESSIONAL

Philadelphia International Airport — **Philadelphia, PA**
Finance Intern for Deputy CFO — *May 2018-Aug 2018*
- Inspected the slide deck for the Investor Presentation, where the executives of the Airport presented to investors in the hopes they would invest in the Airport's bonds
- Reviewed the RFPs of candidates for the Advertising Concessionaire contract and graded each of them based on specific criteria to aid in the decision-making process
- Created an Excel spreadsheet to compare revenue producing strategies for the off-site parking companies to achieve the Airport's specific goals and prepared an executive summary for the Chief Revenue Officer

LEADERSHIP EXPERIENCE

Beta Alpha Psi — **University Park, PA**
Vice President of Corporate Relations — *April 2018-Present*
- Controlled 3 major events of the semester, including the Mock Interview Event, where Accounting Firms conducted mock interviews with students to assist in their career development
- Worked closely with the Treasurer to efficiently allocate a budget for each planned event

Vice President of Professional Development
- Developed all pledge events, which included events such as Movie Night and a Professional Workshop, so the current pledges could complete the pledging process and foster growing relationships with each other
- Held pledge meetings to inform the pledges of different events scheduled and to address any concerns from members

President of Pledge Board
- Shadowed the President of Beta Alpha Psi to learn the daily tasks of the position and to build leadership abilities
- Gained experience by working with other members to improve resume building, interviewing skills, and networking within the professional field
- Attended Board Meetings to help plan for certain events like the Organizational Meeting and to provide insight on any problems occurring during the initiation process

Pennsylvania State University, Finance Department — **University Park, PA**
Teaching Assistant — *Sept 2018-Present*
- Created online exams using the website TopHat for the class and proctored on exam day to ensure the exam ran as planned
- Compiled a list for the professor of all the most notable negative and positive feedback he received from his students

Atlas THON Organization — **University Park, PA**
Relay for Life Captain — *Aug 2017-Present*
- Raised close to $500 for Relay for Life, which is a walk to raise money for the American Cancer Society, through different fundraising events such as restaurant fundraisers

Member
- Coordinated with 50 members to organize events including fundraisers to donate to THON which has raised more than $150 million for the fight against pediatric cancer
- Attended weekly social committee meetings to help plan social events for the organization to build a strong comradery among team members

SHO TIME — **University Park, PA**
Leader on Arrival/Entertainment Committee — *Dec 2017-Oct 2018*
- Collaborated with 8 other leaders to develop, organize, and oversee a 4-day orientation program for incoming Schreyer Honors freshmen to help them adjust smoothly to college
- Served as a leader of 20 mentors on the Arrival/Entertainment Committee to organize specific events like the Finale and to motivate the mentors to effectively communicate and guide the freshmen

SKILLS/INTERESTS/AWARDS

- Working knowledge in Microsoft Products: Word, PowerPoint, and Excel
- Interests: Baseball, Community Service, Exercise, Professional Sports, Traveling
- Awards: Coach's Player of the Year (2016), 2nd Team All-Conference (2016), Captain of Varsity Baseball Team (2016)
- PricewaterhouseCoopers Case Competition, 2018, Finalist in Final Round
- KPMG Case Competition, 2018
- Deloitte Audit Innovations Case Challenge, 2018, Atlanta, only Penn State Team