Cybersecurity Threats to Small Accounting Organizations

Submitted by

Aldijana Latic

Accounting

To

The Honors College

Oakland University

In partial fulfillment of the

requirement to graduate from

The Honors College

Mentor: Dr. Kathryn Schaefer, Special Instructor of Accounting

Department of Accounting and Finance

Oakland University

December 2, 2022

Abstract

Many small organizations do not pay attention to cyberthreats, which have been occurring more frequently. Accounting firms of small organizations should invest more resources in cybersecurity awareness early on to prevent spending more money on fixing these issues in the future. This research paper focuses on reviewing the cyber training inside many small organizations worldwide. Typically, small organizations' business strategies do not focus on this issue and many recruiters do not have the skills necessary to hire the correct people for this job. The companies should be aware of identifying, analyzing, and preventing threats to their internal information technology systems. Small organizations should be supported by trained personnel to ensure effective daily activities with the highest security.

Introduction

Cyber threats occur in all organizations, regardless of size or global location. Small organizations are at a greater risk because they lack the protections and education provided to large organizations. Cybersecurity training in many small organizations should encourage awareness of cyberthreats and provide their employees essential ways to prevent them. Data and information associated with technology are under potential cyber-attacks despite everyday changes in protections. Many companies refuse responsibilities required to support cybersecurity awareness training and education, though their boards and directors are at a higher risk. Without protection from cyberthreats, many companies could lose important and confidential data and it could impact their reputation as well. This review aims to (1) research and synthesize cybersecurity literature; (2) identify the threats specific to small organizations' cybersecurity; (3) determine the significance of cybersecurity to small organizations; and (4) present a literature review that will serve as support for cybersecurity awareness education.

Methodology

This paper gathered information on cyberthreats in small businesses and the significance of cybersecurity. The researcher reviewed potential activities which could support cybersecurity. This helped to determine what is best for small accounting companies (e.g., BST & Co.) compared to large accounting companies (e.g., Deloitte) in implementing cybersecurity changes and assisting in the discovery of crucial components used in data availability for their authorized users. I defined small accounting companies as national companies in the United States, and large companies such as international accounting companies. Small national accounting businesses face the same level of cybersecurity threats as larger international accounting

businesses (e.g., EY, PwC, Deloitte, and KPMG), but typically do not protect their information like larger companies that have security teams.

The researcher used the Oakland University Library *OneSearch* website and Google Scholar to investigate the current literature on cybersecurity and cybersafety. Literature was narrowed down in two ways- (1) to 12 articles that were peer-reviewed, from reliable journals, and from the year 2017 to present; and (2) to six articles that were deemed necessary supplemental external sources sourced from governments and companies. See Table 1 below for the complete list of 18 articles for literature analysis synthesized in a review framed for small business cybersecurity.

Table 1.

Literature Synthesized for Review

Title	Authors	Year
An auditor's responsibility for cybersecurity risks	Louis	2019
A review of the impact of training on cybersecurity awareness	Alruwaili	2019
A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations	Chidukwani, Zander, & Koutsakis	2022
Blockchain	Gomber, Hinz & Schiereck	2017
Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework	Frank, Grenier & Pyzoha	2021
Combined outsourcing of accounting and cybersecurity authorities.	Zadorozhnyi, Muravskyi, & Muravskyi	2021
Cybercrime and cybersecurity in Africa	Kshetri	2019
Cyber, privacy and security actions in COVID -19	Grant Thornton	2020
Cybersecurity in accounting research	Haapamäki & Sihvonen	2019
Cybersecurity in a post-pandemic world	Deloitte	2021
Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)	Bada & Nurse	2019
Economics of artificial intelligence in cybersecurity	Kshetri	2019
Implications of cybersecurity on accounting information	Janvrin & Wang	2019
Manage the business risks behind cybersecurity	Grant Thornton	2022
One of Albany's largest accounting firms was hit with a ransomware attack — what happened next	Chelsea *(Albany Business Review)*	2020
Top cyberthreats targeting accounting firms	Politzer	2020
Ransomware the new online nightmare for business	Anderson *(Times Union)*	2020

Literature Review

According to “A Systematic Literature Review of Blockchain Cybersecurity" from 2020, blockchains, databases for decentralized data storage (Nofer et al., 2017), have turned into one of the most analyzed methods for securing data storage (Taylor et al., 2020). This method has and currently is used for cybersecurity, but unfortunately, this article did not consider that through this integration, people would be able to hide the existence of money, thus hurting the national and global economies (Taylor et al., 2020). People can encrypt the data and information, so they do not have to record their income to the Internal Revenue Service (IRS). This now publicly available information is difficult for the IRS and auditors in public organizations. Auditors must go through additional IT education so they can detect potential cybercrimes. Some of the accounting companies outsource to third parties to help them detect the cyberthreats with more skilled IT expertise. Many of the accountants must be aware of the consequences used in cybersecurity. The auditors are responsible for the reports to stakeholders and must be able to accurately present all financial information while providing cybersecurity.

Security breaches affect the stock market shares of the company. For this reason, many firms are unwilling to inform the public of past cyberattacks to prevent their equity value after attacks. Also, according to Haapamaki and Sihvonen (2019), the accidental employee entry of bad data, the accidental “destruction” of information by workers, installation of viruses, human-made disasters, sharing of passwords between co-workers, and distribution of data to unauthorized people are recognized as the most compelling security threats. For example, in December 2020, BST and Co. was attacked by ransomware, which exposed data of some of their accounting clients, including medical group, Community Care Physicians. They assured their clients that the information did not contain Social Security numbers, credit card or medical

records; it was a ransomware attack, where the hackers froze access to the company's computers until they paid ransom. However, they had to inform the public about this issue, and the public is unaware if their data was exposed on publicly accessible websites (Albany Business Journal, 2020; Times Union, 2020). These attacks hurt the reputation of the company, since many clients lost trust in companies that exposed their information. Even though some companies informed individuals about the data breach, we can never know if all companies will share this information about being attacked. Even though the law requires that the public be informed about exposing their information, the public may not find out until well after the breach. Usually, the public finds out months or years later, and sharing data could be damaging for the future.

Management is not only responding to their owners and shareholders, but cybersafety is important for their legal protections. Cybersecurity attacks are not only dangerous for the company and its clients, but also for legality purposes. According to the Journal of Accounting and Public Policy's article "Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework", many companies hold their directors liable for cyberattacks (Frank, Grenier, & Pyzoha, 2021). If directors have experienced previously immaterial cyberattacks, and they do not implement AICPA's framework regarding cybersecurity internal control, the court and juror may hold the directors liable. Since jurors believe that previous experience should warn the directors and they should use this knowledge to prevent another attack, jurors feel more prejudice towards the board as they potentially had the knowledge to monitor and manage cybersecurity risks (Frank et al., 2021). For this reason, internal prevention and awareness is key to conscientiously managing organizations.

Cybersecurity is a concern for every type of organization; individuals and organizations are exposed to targets regularly. For example, many university students give their personal

information and credit card numbers to websites. According to Alruwaili, “although cybersecurity is a concern across the world, it is of more significant concern for the government and the business world” (2019, pg. 1). Also, many students may use their parents' information and data, exposing others to cyberthreats. Most university students do not have any assurance against cyberthreats, even though they would be significantly affected by losses from potential cyberattacks (Alruwaili, 2019). Just as people of all ages can be affected and targeted differently by cyberthreats, so can organizations of any size.

Organizations should put cybersecurity into their budget. Large organizations and their clients are under constant threat from cyber-attacks. Most of these companies are covered with insurance in case of cyberthreats, but many small businesses are not protected. Many small organizations refuse to invest into cybersecurity and are open to the risk of being attacked. Small organizations are at the same level of risk as larger organizations, but do not have the same level of protection. Cyber awareness training could help many small organizations throughout the world. Cybersecurity training should be essential in every workplace, and this skill can be improved by everyday changes with the technology revolution. As stated by Bada and Nurse, all employees, along with stakeholders, executives, and cybersecurity personnel, should be trained in how to protect their businesses and be aware and responsible with management support (2019). The strategy of an organization should include this kind of awareness and seek to include a low-cost strategy as prevention for long term safety (Bada & Nurse, 2019). Prevention is crucial to reduce the risks of potential cyberthreats. Companies should invest in training all employees and keeping their information private and encrypted.

We can see why many professionals must pass an ethics test. It is not only because of the organization, there is much more at stake for businesses. Suggested guidance from regulators and

state governments indicates that cybersecurity is a crucial part of a director's/board's risk management and responsibility. Even though auditors are evaluated based on the quality of their work, directors are not legally required to be evaluated. Directors are only judged if they are in the court where jurors determine if they acted in good faith to take preventative measures for cyberattacks (Frank et al., 2021). For the organizations or management, themselves, the awareness for protecting the data minimizes the damage that occurs, preventing cybersecurity attacks.

Cybersecurity in Small Organizations

This paper will provide a literature overview of cybersecurity challenges. Since putting forth the idea of this literature review, a published review on the cybersecurity in small businesses, was released. In their 2022 review, Chidukwani and colleagues overview important statistics to note. As cited in Chidukwani et al. (2022), small businesses are responsible for more than 90% of the world's business economy (Vives, 2006), but do not implement the expected cybersecurity strategies (Renaud & Weir, 2016). They are known as easy targets- 66% of small businesses experienced a cyberattack between 2016-2017 (Chidukwani et al., 2022). Small businesses have less human, financial, and educational resources in place, but they suffer higher costs (Chidukwani et al., 2022). Additionally, small businesses are usually attached to larger businesses; an attack on one, can open both (and all other attached businesses) to cyber threats. For example, in 2013, target Corporation's network was breached, and 70 million records of personal information and 40 million credit card numbers were stolen (Shu et al., 2017). It is believed that Target was breached because their HVAC vendor was hacked (Banham, 2017). The same cybersafety measures in play at the higher, large business level (e.g., Target Corporation),

should be in place for all small businesses (e.g., HVAC companies), especially if they are connected.

With growing threats, small organizations have begun to pay more attention to cybersecurity. Specifically, organizations look at how their business receives, sends, and stores personal information and the people that see and have access to that information. Ensuring a system helps these organizations protect their information. According to Grant Thornton, a small accounting firm, challenges faced during the COVID-19 pandemic increased awareness in the organizations as they faced more threats. Possible cyberthreats include surveillance, contact tracing, health disclosures, remote work, requirements of medical exams, etc. Small firms, such as Grant Thornton, used precautions to prevent cyber risks such as usage of new company devices and tools for their remote workers and implemented cloud-based file-sharing with a cybersecurity platform (Grant Thornton, 2020). Also, they reviewed logins with a secured network. In addition to these changes, small firms should follow Grant Thornton's lead in implementing training about phishing emails and malware, the most common attacks, during the pandemic and a new work environment (2020).

Accounting firms are not only exposed to the cyberthreats, but they are also more susceptible since they are involved with other companies and individuals. Accounting firm's client's data are more vulnerable than the data of their own records as more information makes them more of a target and legal consequences. This risk could be significant, and qualified firms must control their own cybersecurity even though they do not possess Information Technology (IT) infrastructure. The IT infrastructure should be outsourced to third parties if not employed by organizations. Johnny Lee, Grant Thornton's Principal and Forensic Technology Practice Leader, said, "if you identify cybersecurity as strictly an IT domain, then you're doing it

wrong…it's a category of enterprise risk" (Grant Thornton, 2022). He wanted to say that not all IT specialists have all the technology skills necessary to protect the company, there are sometimes required different skills that require years of training and "experience". Also, the firms should be careful about outsourcing and reliability of outsourced parties. The company shares a risk with outsourced parties as a collaborative cybersecurity to achieve resilience (Grant Thornton, 2022). Most organizations, small and large, hire a third party, such as an IT specialist. However, using an outside source with advanced cyber skills could be dangerous since organizations expose their data to the third party. Third parties should be background-checked and closely monitored before, during and after performing their assignments.

Daily, many opportunities exist for cybersecurity risk. Human behavior in organizations could be a key for prevention of cybersecurity. If employees are not trained about awareness of potential threats, they could unintentionally expose the company to threats such as malware and ransomware, phishing schemes, and data breaches. A partner in the Digital Forensic Group, Vijay Rathour, emphasized how small and medium sized accounting firms are at risk for cyber-attacks since they lack sophisticated defense systems in cybersecurity like that of larger firms. Of note, he described three top cyber threats that accounting firms face:

1. Malware and ransomware- where ransomware is the type of malware designed to take computers, networks, files, and sensitive data hostage by blocking the access to wonders. Usually, the attacker will demand payment to unencrypt the data. Sometimes, the firms are forced to make a payment, or they consider that their data is not vulnerable and refuse to pay a ransom payment.
2. Phishing schemes- where most ransomware is transferred via phishing schemes, which are redistributed via emails that contain malware hidden in victim's opinion innocent file

attachments. There is “spear phishing” which uses personal information and attacks a specific individual, and “whaling” which attacks high ranking corporate employees such as the CFO, and contains subject lines familiar to their company, where the accountant would open without thinking twice.

3. Data theft has a huge impact on the financials for organizations which includes accounting firms. The cost includes investigation and forensics to determine the source of data breach, legal and consulting services, and determining the victims of data theft (AICPA, 2020).

These cyberthreats could be avoided by understanding and trusting their organization’s security and employees’ behavior. In general, cybersecurity systems should be constructed to manage potential liability. Organizations should be more prepared and educated to prevent malware and ransomware threats by constantly encrypting the data. Also, employees should be aware of the potential threats from phishing schemes via emails. While organizations endanger the reputation of its company, they are putting the clients and other companies in the same danger and exposing their information as well.

Cybersecurity Threats

Recently, organizations have had more challenges while they encounter the global COVID-19 pandemic. Because of this, firms have become more vulnerable due to the transition to work from home. Cybersecurity risks are also higher because of the pandemic. Due to COVID-19 and remote working from home, employees and companies are more likely to store significant information virtually. Organization’s management seeks to decrease the cyberthreats by limiting the access of certain data to their accounting staff. All accounting activities are

supposed to be monitored by the cybersecurity department. Large companies have the option to both outsource these services or have their own cybersecurity department (Muravskyi et al., 2021). Combined outsourcing of accounting and cybersecurity is helpful to develop the organizational process of the enterprise with minimal expenses and financial risks.

Cybersecurity threats are persistent and present in other continents and countries as well. For example, Africa is rapidly growing in cybercrime acts (Kshetri, 2019), costing the African economy $3.5 billion in 2017. Cybersecurity in African developing countries is considered a luxury, and many companies report less than 1% finances allocated to cybersecurity. Many of the African internet users are encountering their first connections to computers and technology. Because of this lack of English language and inexperience, the African population is the common target. Law enforcement does not take considerable action to protect the populations from cyberattacks. Also, they avoid training in their organizations as the trainees could gain the skills to commit the cybercrimes themselves. Currently, Africa is trying to take measures to address cyberthreats with their data protection bill, where they require companies to inform consumers how their information is being collected, used, and stored. Also, this bill gives the right to consumers to request to delete their information or be secured by a certain level of security while stored. In addition, banks are required to have a Cyber and Information Security Officer (CISO) who would offer recommendations about cybersecurity concerns, and form measures to manage potential cyber risks (Kshetri, 2019). Cybercriminals are aware of these decisions of unprepared countries, and they are building their confidence and abilities to make those countries their primary destinations of cybercrimes. The ability to prevent cybercrimes in a company and share the data of its partners or clients is the crucial basis in every business.

Cybersafety in Large & Small Organizations

Cybersecurity is taking a place in many organizations small and large. For this reason, the American Institute of Certified Public Accountants (AICPA), the Public Company Accounting Oversight Board (PCAOB), and the U.S. Securities and Exchange Commission (SEC) implemented cybersecurity risk management policies and procedures as a guidance to many accounting firms to protect their clients and future investors. These assurance frameworks for auditors include an assurance structure on cybersecurity discoveries while auditors evaluating an organization's cybersecurity risk. Economic impact on data breaches on firms affects company's returns and future accounting measures of performance that include return on sale and higher audit fees (Janvrin & Wang, 2019). The strategies that include awareness of cybersecurity in the accounting firms could prevent additional expenses and protect the data of organizations. While combining technology and human expertise, you are safeguarding your assets.

Through education, individuals and companies can understand the technology, potential threats, and cyber challenges. In 2019, Bada and colleagues emphasized the London Digital Security Center's (LDSC) mission as a non-profit organization in dealing with cybersecurity education, awareness, and training for London- based small businesses. Their concept resides in three areas of activities: engaging with the small business community, the security education and membership cycle, and the security solution. First, they engage with the local community to raise awareness of potential cyber threats. They rely on national fraud reports to target the companies for visitation. Second, they offer organization risk analysis, so they could check internal company's networks, anti-virus systems, and build relationships with the small businesses. The next is to educate the small organizations on how to protect their enterprises. LDSC targets employees, platforms, and regulatory procedures. After this stage, a small business would be

informed about their cyber risks, preparing them for testing and review (Bada et al., 2019). Raising the worldwide awareness about cybersecurity reduces the risks of cyber infrastructures. Planning the cyber defense also decreases the nation's critical threats in the accounting organizations.

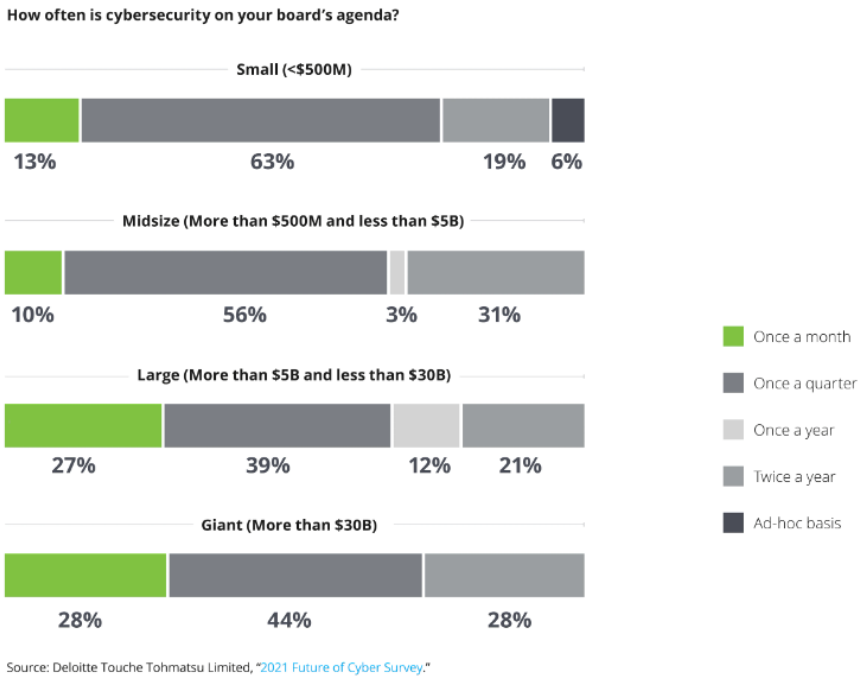
Deloitte is one of the biggest international accounting firms. To better understand cybersecurity, it is important to see how a large organization approaches cybersecurity, especially in the post-pandemic world. Their remote work has increased the risk of securing the organizational business system. Their cybersecurity has faced additional challenges since the pandemic and their transition to remote work was carefully monitored; their cybersecurity infrastructure must be the best defense to protect the organization and stakeholders. Figure 1 below demonstrates how Deloitte's company board, indicated as a 'giant' company in the figure, discusses cybersecurity at least four times a year (Deloitte, 2021). Large companies are familiar with the importance of internal control as it can become the weakness of the organization. For this reason, Deloitte invests into cybersecurity to keep the integrity and confidentiality of their clients.

Figure 1 provides additional details and suggestions for companies of all sizes. We can see how small organizations have less concerns, but still prioritize cybersecurity with 63% of companies including cybersecurity once a quarter (Deloitte, 2021). The trust and reputation of their organization is at stake. They are aware of these challenges, so they invest and are more alert into cybersecurity to empower the future of cybersecurity.

Figure 1

The Future of Cybersecurity

Note. "How often is cybersecurity on your board's agenda?" (Deloitte, 2021)



Recommendations for Cybersecurity

The most important thing for small organizations is to prioritize cyberthreats all year around. Most companies think that cybersecurity is an unnecessary expense as there is a small chance of cyber threats occurring to their organization. In this way, cybersecurity becomes a significant risk to the businesses. However, how to prevent cyberattacks, particularly for small organizations is debatable. According to Becker (2019) an organization can prevent cyberattacks if they (1) constantly evaluate cybersecurity defenses, as business is growing the companies must adapt; (2) use sources aggressively so an organization can detect potential attacks; (3) employee

awareness and training about identifying cyberattacks; (4) internal and external auditing to evaluate threats; and (5) back your data systems in case it is interrupted so you can get functionality fast. Additionally, based on the literature presented, I would suggest additional measures for cybersafety including: (1) implement a formal cybersecurity structure program or department to encourage responsibility; (2) profile the firm's potential risk on a regular basis; and (3) ensure company and personal information is encrypted.

The National Institute of Standards and Technology Cyber Security Framework (NIST CSF) puts forward a "cybersecurity framework" with five plans of actions for organizations "to better understand and improve their management of cybersecurity risk" (2022). The five functions can be seen below in Table 2. It is the NIST's hope that small organizations can use the full appendix (NIST, 2014) and its attached resources for a cost-effective, efficient source of managing cybersecurity risks.

Table 2.

NIST CSF Cybersecurity Framework

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect	Access Control
	Awareness and Training
	Data Security
	Information and Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

Note. This figure was made by the author by the information was duplicated from NIST (2014).

Conclusion

In conclusion, the purpose of this paper is to raise awareness about cybersecurity in small and large organizations, and the challenges that organizations face during their business missions. All organizations, regardless of size, are at risk of being attacked. Importantly, an attack on one organization can leave all affiliated companies vulnerable. Moving forward, many companies want to secure their workplace and network. This review discovered damaging security threats and the protections that organizations should take in the future. Successful cyberthreats are very damaging for the organization and their clients. Not only will that company have a destroyed reputation, but they could also have financial impacts such as loss of business and legal consequences. It is the best for businesses that they are aware of cybersecurity challenges and maturing core infrastructure to protect the organizational environment. Specifically, companies should work to have an aggressive approach in cyber prevention and response; they should utilize the financial resources that they have, hire at least one IT staff member and/or outsource to a third party, and educate the entirety of their staff on cyberthreats. Internationally, governments should help protect each other from cyber-attacks as some countries are more educated and advanced than others. It is also my hope that more research is done on cybersecurity threats to small businesses so the results can be used.

It is my hope that this review provides a more comprehensive knowledge about this issue in many organizations. While I personally benefited from the knowledge, these findings can also help many organizations as they encounter cybercriminals. Many small businesses might find this review helpful as a starting point before they invest in cybersecurity education and prevention of cyberthreats. Additionally, other researchers may build from and cite this review to

assist in future literature and research projects. In addition, they might be able to discover themes from the article or narrow down potential directions for future cybersecurity protections.

Acknowledgments

I want to thank my faculty adviser and professor, Dr. Kathryn Schaefer, for her support and guidance in this project. Most importantly, I want to express my appreciation and gratitude to my family, husband, and son, Emir, for inspiring me to not only finish school, but to finish with honors.

References

Alruwaili, A. (2019). A review of the impact of training on cybersecurity awareness. *International Journal of Advanced Research in Computer Science*, *10*(5).

Anderson E. (2020, February 20). Ransomware the new online 'nightmare' for business. Times Union. https://www.timesunion.com/business/article/Ransomware-the-new-online-nightmare-for-business-15071321.php

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*. https://doi.org/10.1108/ICS-07-2018-0080.

Banham, R. (2017). Cybersecurity threats proliferating for midsize and smaller businesses. *Journal of Accountancy*, *224*(1), 75.

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, *10*, 85701-85719.

Diana, C. (2020, February 20). One of Albany's largest accounting firms was hit with a ransomware attack — what happened next. Albany Business Review. https://www.bizjournals.com/albany/news/2020/02/20/bst-co-ransomware-attack-community-care.html

Deloitte. (2021). Cybersecurity in a post-pandemic world. https://www2.deloitte.com/us/en/pages/financial-advisory/articles/financial-services-cybersecurity-global-organizations.html

Frank, M.L., Grenier, J. H., & Pyzoha, J. S. (2021). Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework. *Journal of Accounting and Public Policy*, *40*(5), 106860. https://doi.org/10.1016/j.jaccpubpol.2021.106860

Grant Thornton (2020, April 21). Cyber, privacy and security actions in COVID-19.

Grant Thornton (2022, February 16). Manage the business risks behind cybersecurity.

Haapamäki E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808–834. https://doi.org/10.1108/MAJ-09-2018-2004

Janvrin D. J., & Wang, T. (2019). Implications of cybersecurity on accounting information. *The Journal of Information Systems*, *33*(3), A1–A2. https://doi.org/10.2308/isys-10715

Kshetri N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

Kshetri N. (2021). Economics of Artificial Intelligence in Cybersecurity. *IT Professional*, *23*(5), 73–77. https://doi.org/10.1109/MITP.2021.3100177

Louis J. (2019, May 14). An Auditor's Responsibility for Cybersecurity Risks. Becker. https://www.becker.com/blog/cpe/an-auditors-responsibility-for-cybersecurity-risks

NIST: National Institute of Standards and Technology (2014). Framework for improving critical infrastructure cybersecurity. *Framework*, *1*(11).

NIST: National Institute of Standards and Technology (accessed 2022). *Cybersecurity framework*. https://www.nist.gov/cyberframework

Nofer M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*(3), 183–187. https://doi.org/10.1007/s12599-017-0467-3

Politzer M., (2020, March 16). Top cyberthreats targeting accounting firms. *AICPA: Association of International Certified Professional Accountants.*

Renaud, K., & Weir, G. R. (2016, August). Cybersecurity and the Unbearability of Uncertainty. In *2016 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 137-143). IEEE.

Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the target: An analysis of target data breach and lessons learned. *arXiv preprint arXiv:1701.04940*.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147-156.

Vives, A. (2006). Social and environmental responsibility in small and medium enterprises in Latin America. *Journal of Corporate Citizenship*, (21), 39-50.

Zadorozhnyi Z.M., Muravskyi, V., & Muravskyi, V. (2021). Combined Outsourcing of Accounting and Cybersecurity Authorities. *11th International Conference on Advanced Computer Information Technologies (ACIT)*, 544–547. https://doi.org/10.1109/ACIT52158.2021.9548649