5-2021

How the Growth of Technology has Forced Accounting Firms to put an Emphasis on Cybersecurity

Holden Halbach

How the Growth of Technology has Forced Accounting Firms to put an Emphasis on Cybersecurity

by

Holden T. Halbach

Advisor: Kris Allee

An Honors Thesis in partial fulfillment of the requirements for the degree Bachelor of Science in Business Administration in Finance and Accounting.

Sam M. Walton College of Business
University of Arkansas
Fayetteville, Arkansas

May 7, 2021

Introduction:

The advancement of technology has brought many changes to accounting firms. Computer applications such as Microsoft Excel have made calculators and physical spreadsheets obsolete. Then with the introduction of cloud computing employees can store, access, and exchange large amounts of data instantaneously from any location. These technological innovations have increased the accuracy and efficiency of firms substantially. However, this growth in technology has shown the importance of putting an emphasis on cybersecurity throughout the accounting industry. The emphasis placed on cybersecurity throughout accounting firms is more prevalent than any other industry. This is primarily because accounting firms not only deal with large amounts of internal financial data, but also other companies' financial data for audit and tax purposes. This paper begins by showing the biggest and most common cybersecurity threats firms face today. It then outlines the steps firms can put in place to minimize the risk of falling victim to these threats. Moreover, it will compare the challenges of maintaining sufficient cybersecurity between large and small accounting firms and provide examples of different repercussions firms faced after experiencing a breach in their cybersecurity. Finally, it will highlight the new regulations and guidelines established in order to strengthen a firm's cybersecurity throughout the accounting field.

Biggest Threats to Cybersecurity:

According to the Journal of Accountancy, "cybersecurity breaches are estimated to cost businesses around the world a staggering 1.5 trillion per year" (Malia Politzer, 2020). While big accounting firms are certainly targeted, most often smaller firms are easier targets for data theft. This is due to smaller firms lacking the complicated cybersecurity infrastructure the big accounting firms maintain. The most common attacks on firms' cybersecurity currently are through phishing schemes. According to IBM, phishing accounts for 90 percent of all data breaches, and 76 percent of business's were the victim to some level of phishing during 2020 (Joel Witts, 2021). The most common phishing scheme seen throughout the business world is spear-phishing. Spear-Phishing is using personal information to fraudfully obtain sensitive information by impersonating a dependable business or individual digitally. The most common ways are through emails and text messages. According to DART, the initial attempt to attack cybersecurity comes through a form of spear-phishing 44 percent of the time. This percentage is broken up into 29 percent spear-phishing via an attachment and 15 percent spear-phishing via a website hyperlink (Zelijka Zorz, 2020). An example of spear-phishing would be an employee receiving an email at work from an imposter pretending to be part of their firm's HR department. This email would have a subject line such as please examine this negative review. In the email it would have a short paragraph saying it is from HR, and that they can review the report through link or attachment below. This type of email would typically fluster an employee that is poorly trained with respect to cybersecurity protocols and phishing methods. This employee would quickly click the link or attachment in the email, due to them feeling angst about a potential negative review regarding their performance at the company, and immediately threaten their firm's cybersecurity. This is merely one example of a ploy a hacker may use in phishing, but the

list is endless. Ways to stop phishing include awareness, security training, and constant reaffirmation. The first step in awareness is crucial because employees will not be on the lookout for something they do not know exists. This could be taken care of as easily as talking about phishing during on-boarding training. The security training can be taken for employees who need extra help understanding what to look out for. Finally, reaffirmation is important so that employees are constantly being reminded to be on the lookout for these cybersecurity threats.

Another common cybersecurity threat seen throughout accounting firms is Ransomware. Ransomware is a type of malware, which is a malicious software that encrypts and blocks access to files throughout an individual's computer. Once the hackers have a hold over your file, they will hold you at ransom in order to restore access to your files. The 2019 Ponemon and Accenture report states, that the number of ransomware attacks on organizations have increased by 15 percent and attacks have more than tripled in the past two years (Malia Politzer, 2020). These statistics continue to show that firms need to continue placing a huge emphasis on cybersecurity. Three common methods for defending against a ransomware is evaluating a firm's IT infrastructure, consistently updating security measures, and finally educating staff/clients. Due to each accounting firm accessing and dealing with its own and client's sensitive data, it is crucial a secure infrastructure is set up in order to protect it. The New Jersey Society of Certified Accountants advise hiring a third part security firm to perform a penetration test at least once a year. The security firm will be able to outline the weaknesses of a particular firm's infrastructure. This will allow the firm to take the necessary steps in order to prevent that issue from causing further problems. The second defense against ransomware is to update your cybersecurity with the latest security measures. Firms should be constantly performing daily backups of clients' critical data in order to protect it from loss of data in the event of a ransomware attack. The final defense method would be to educate your staff and clients. Providing training and defense techniques so individuals know what to look out for and can recognize a potential attack. The American Institute of Certified Public Accountants recommends firms provide advisory services to their clients in order to teach them about potential cybersecurity threats.

There are many techniques firms can enforce to strengthen their cybersecurity against their biggest threats. First, is the importance of informing employees about cybersecurity threats. Providing proper training to employees on what to look out for and common practices used by cyber-attackers. Training is extremely important because according to a study by IBM "95 percent of cybersecurity breaches are due to human error (Devon Mikovich, 2020)." The next technique is having an IT control that requires employees to use passwords that are strong. An example of this would be requiring a password to have at least 8 characters and the use of a symbol, number, and letter throughout the password. A firm can also establish a multi-factor authentication process. This requires an employee to provide two or more factors in order to gain access to the data. Another efficient practice is to delete old or irrelevant files. This is effective through lowering the amount of data the firm is liable for and at risk to attacks. Therefore, it cuts down on the legal ramifications a firm may face if there is a data breach. According to IBM, "data breaches can be extraordinarily expensive, costing a company an average of approximately $150 per record (Malia Politzer, 2020)." Next, conducting a proper risk-based assessment on a firm's cybersecurity is tantamount to the techniques firms can utilize to strengthen their

cybersecurity. This allows firms to be able to recognize weak points and make the appropriate changes to remedy those points. This technique requires staying well informed on the latest hacking techniques in order to see which part of the firm's cybersecurity are now vulnerable. Firms can also hire a third-party cybersecurity firms to help consult them on their vulnerable points and give them recommendations on how remedy the situation. Finally, installing antivirus and cybersecurity software to alert firms of potential threats or data breaches. These are the most common techniques to help strengthen cybersecurity used throughout the accounting industry.

Comparing Large firms v Small firms

Focusing first on what happens when a large firm has a failure in their cybersecurity. The first firm we will be looking at is Deloitte. Deloitte is currently the largest accounting firm in terms of revenue at $47.6 billion in 2020 (Statista, 2021). Deloitte has offices in over 150 countries and in 2012 was ranked the best cybersecurity consultant in the world (Statista, 2021). However, even with a complex IT infrastructure, they fell victim to a cybersecurity attack in 2016. The attack was made possible due to an administrator not being properly secured using a two-factor authentication system. 5 million emails were put at risk from the hack, but Deloitte publicly stated that only a fraction of those emails contained sensitive data for several small clients. The firm hired Hogan Lovell's law firm on special assignment to review the cybersecurity incident. The assessment showed that the hacking would have a minimal effect on Deloitte's overall business. Although the firm did suffer embarrassment from the publicity of this hack and this negative publicity likely sent potential customers to their competitors since they now questioned the reliability of Deloitte's cybersecurity. Nonetheless, since Deloitte is such a large firm, they were able to take the necessary steps to recover from the incident in 2016. They were able to review their current data security system and make the proper changes to lessen the chances of this happening again. Large firms can take hits like this and recover due to the amount of capital they have as well as the goodwill from clients that have earned over time. This allows them to get ahead of the situation and apply techniques in order to regain their clients trust. These techniques can consist of hiring a third-party cybersecurity firm to help diminish the risk of an incident happening again. Big firms also have the luxury of having experienced and capable public relation teams as well, so they will be able recover from the negative press hit.

Examining the impact, a data breach has on a smaller firm is a little more nuanced. We will next examine BST & Co which is a small private firm based out of New York. In 2019 the firm was hit by a ransomware attack that compromised patient data from one of the firm's local clients, Community Care Physicians. The breach compromised numerous names, billing codes, insurance description and other medical records. BST is now in the middle of a current class action lawsuit that is claiming that the firm was negligent and reckless when protecting sensitive data. They were accused of failing to have a reasonable data security system to protect its client's data. The lawsuit also includes that the firm did not provide immediate notification that the attack occurred. The lawsuit aims to make the firm pay compensation to the victims for having to pay for credit monitoring and the protection of their personal information since the attack. Since BST & Co is only around 100 employees the lawyer fees and possible loss of the lawsuit will be very devastating for the firm. Furthermore, the firm has to deal with loss of potential business

due to bad publicity of this data breach without the help of the public relations teams that bigger firms have access to because of their significant capital and history. Finally, they will also suffer the fees to improve their data security to prevent an incident of this caliber to happen again. These unexpected costs make it extremely difficult for smaller firms to recover from, especially with the possibility of losing additional clients due to the negative publicity as well.

From 2014 to 2020, data breaches of CPA firm have increased over 80 percent (Byron Shinn, 2020). Once a data breach has occurred litigation usually costs around $70,000 to $300,000 (Byron Shinn, 2020). Then depending on the size governmental requirements can cost another $100,000 to $300,000 (Byron Shinn, 2020). These legal fees and monitoring requirement tend to place a significantly heavier burden on smaller firms. Smaller firms tend to be more vulnerable due to the lack of capital they can retain as well as expend on protecting these attacks. That is, due to the lack of capital they are unable to devote the resources a large firm can maintaining a complex and secure IT infrastructure. The lack of capital also gives a significantly worse chance to be able to recover due to the fees associated with a data breach. The advancement of technology is constantly providing new avenues for hackers to use infiltrate a firm's sensitive data. This is another area where bigger firms have the advantage due to having the funds to constantly update their security practices. Cyber criminals are aware of the disparity of the digital security between small and large firms. Using an article from CNBC about cybersecurity of all small businesses' helps shed light to what small accounting firms go through. The article states that 43 percent of online attacks are now aimed at small businesses, and that more than half of them have suffered a breach within the last year (Scott Steinberg, 2019).

Cybersecurity Guidelines

Cybersecurity has become a threat to disrupting the United States digital infrastructure. If cyber criminals can succeed, then all the nations key industries are at major risk. In order to lower the risk of cyber breaches to those industries the US National Institute of Standards and Technology established a Cybersecurity Framework. This framework helps organizations combat cyber-attacks by teaching them how to prevent, detect, and respond. The framework includes five key functions that help organizations to strengthen their cybersecurity practices to the highest level. The five functions of the framework are Identify, Protect, Detect, Respond, and Recover. The definitions of the functions listed below are from *The Framework for Improving Critical Infrastructure Cybersecurity:*

- Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

- Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.

- Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

- Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

• Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Overall, this framework provides useful guidance for firms to be able to perform review over their cybersecurity risk management. The framework also brings about crucial communication throughout a firm and allows for major risk reduction. This framework is essential no matter the size of the firm and should be utilized throughout the accounting world.

The American Institute of Certified Public Accountants outlines the cybersecurity risk management examination report into three separate components. The first component is management's description of the entity's cybersecurity risk management program. This component outlines a company's risk management protocol for dealing with cybersecurity. AICPA defines this component by stating "this description is designed to provide information about how the entity identifies its information assets, the ways in which the entity manages the cybersecurity risks that threaten it, and the key security policies and processes implemented and operated to protect the entity's information assets against those risks (AICPA 2017)." Basically, this component has management summarize their company's risk management program. Then the firm can check for completeness and the implementation of this program, and make sure it satisfies industry standards. The second component is the management's assertion. ACIPA defines this component by stating, "Specifically, the assertion addresses whether (a) the description is presented in accordance with the description criteria and (b) the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria (AICPA 2017)." Management makes this assertion based off the control criteria outlined by AICPA and gives an opinion as to whether they are meeting their cybersecurity objectives. Finally, the last component is the practitioner's report. This is where the firm gives their opinion on if the management assertion is correct and the company's cybersecurity risk management program is effective. The AICPA define this component by stating, "Specifically, the opinion addresses whether (a) the description is presented in accordance with the description criteria and (b) the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria (AICPA 2017)" These components give a firm the guidelines for how a firm would evaluate a company's effectiveness of its cybersecurity.

To summarize these documents, *The Framework for Improving Critical Infrastructure Cybersecurity* should be used by both the client and the firm management to internally evaluate their cybersecurity of their risk management. However, only an accounting firm would use the components of AICPA reporting framework to evaluate a client's cybersecurity.

Conclusion:

The emphasis placed on cybersecurity will continue to grow alongside the advancements in technology across the accounting industry. Cyber-attackers are constantly implementing new methods and techniques in order to bypass a firm's cybersecurity. This causes the cybersecurity landscape to be constantly changing in order to defend against these new attacks. Through the

awareness and implementation of proper cybersecurity techniques, accounting firms will be able to minimize the risk of falling victim to a cyber-attack.

References

Keller, Nicole. “Uses and Benefits of the Framework.” *NIST*, 11 May 2020, www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework.

“SOC for Cybersecurity: Information for CPAs.” *AICPA*, 2017, www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityforcpas.html.

Nicole.keller@nist.gov. “Uses and Benefits of the Framework.” *NIST*, 11 May 2020, www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework.

Steinberg, Scott. “Cyberattacks Now Cost Companies $200,000 on Average, Putting Many out of Business.” *CNBC*, CNBC, 9 Mar. 2020, www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html.

Witts, Joel. “How To Stop Phishing Attacks: The Best Tools To Stop Pishing Scams.” *Expert Insights*, 24 Feb. 2021, expertinsights.com/insights/how-to-stop-phishing-attacks/.

Zorz, Zeljka, and September 30. “The Biggest Cyber Threats Organizations Deal with Today.” *Help Net Security*, 30 Sept. 2020, www.helpnetsecurity.com/2020/09/30/enterprise-cyberattack-trends-2020/.

Stark, Christopher. “Ransomware: Is Your Accounting Firm At Risk?” *Cpapracticeadvisor*, 22 Aug. 2016, www.cpapracticeadvisor.com/firm-management/article/12237558/ransomware-is-your-accounting-firm-at-risk.

Politzer, Malia. “Top Cyberthreats Targeting Accounting Firms.” *Journal of Accountancy*, 16 Mar. 2020, www.journalofaccountancy.com/newsletters/2020/mar/top-cyberthreats-accounting-firms.html.

Hopkins, Nick. “Deloitte Hit by Cyber-Attack Revealing Clients' Secret Emails.” *The Guardian*, Guardian News and Media, 25 Sept. 2017, www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails.

Cyware. “Deloitte Email Data Breach: Confidential Information and Documents of Clients Exposed: Cyware Hacker News.” *Cyware Labs*, Cyware, 22 Feb. 2020, cyware.com/news/deloitte-email-data-breach-confidential-information-and-documents-of-clients-exposed-971f9730.

Davis, Jessica. “Community Care Patients Sue Accounting Firm Over Data Breach.” *HealthITSecurity*, HealthITSecurity, 15 June 2020, healthitsecurity.com/news/community-care-patients-sue-accounting-firm-over-data-breach.

Shinn, Byron. “Cybersecurity: An Urgent Priority for CPA Firms.” *The Tax Adviser*, The Tax Adviser, 1 Apr. 2020, www.thetaxadviser.com/issues/2020/apr/cybersecurity-urgent-priority-cpa-firms.html.

Milkovich, Devon. “15 Alarming Cyber Security Facts and Stats.” *Cybint*, 12 Jan. 2021, www.cybintsolutions.com/cyber-security-facts-stats/.

Statista. “Topic: Deloitte.” *Statista*, 29 Jan. 2021, www.statista.com/topics/2602/deloitte/.