The Growing Threat of Ransomware: What Accountants, Their Clients, and Security Professionals Need to Know

Patrick M. Ryle[1], Robin Hicks[2], Kenneth L. Shemroske[3], Mark A. Mcknight[4], Brett L. Bueltel[5]

Abstract: Objectives This paper is designed to prepare accountants to meet the dangerous challenges posed by ransomware. **Prior Work** Business operating conditions concerning ransomware have never been more dangerous. In confronting these dangers, prevailing data protection regimes have proven frighteningly inadequate. This paper explores ransomware's potential impact, and the institutional, organizational, and cultural approaches necessary in the preparation and prevention of such attacks. **Approach** This paper presents a review of the development of the threat of ransomware outlines several steps accountants can take to prevent such incidents from occurring, and outlines steps accountants can take after a security failure in the face of a ransomware attack. This paper highlights the importance of devoted preparedness., **Results** This paper implores accountants to take the threat of ransomware seriously, to understand that cyber-attacks are unpredictable and that the time to prepare is now. **Implications** We examine post-incident mitigation considerations and the ongoing organizational, professional, reputational, and financial consequences of a successful ransomware attack. **Value** This paper's contribution provides an examination of ransomware awareness, steps that must be taken in preparation, and the costs of failure in a context unique to accounting and tax professionals.

Keywords: Cyber-security; Safeguards rule; Gramm-Leach-Bliley, Client data; Data breach

JEL Classification: K2; M48; M15

1. Opening Vignette

Upon returning to the office from a regularly scheduled client meeting, a firm manager senses a concerning change in the tenor and energy of her office environment. She witnesses the IT staff desperately moving from inoperable computer to inoperable computer, before the disheveled district manager approaches and frantically informs her that the unthinkable has happened - the firm has been targeted by an unforeseen cyber-attack, and the cyber security defenses failed to stop it. Her network is down, the systems are non-functional, and the integrity of the firm and client data has been compromised.

An on-the-spot field assessment determines that the firm has suffered a successful and novel "ransomware" attack. The attackers have not only captured company data but are requesting the

[1] Assistant Professor, Dalton State College, United States, E-mail: pryle@daltonstate.edu.
[2] Manager, Graduate Cybersecurity Degrees, United States, E-mail: rhicks34@gatech.edu.
[3] Associate Professor, PhD, University of Southern Indiana, United States, E-mail: klshemrosk@usi.edu.
[4] Professor, PhD, CFE, University of Southern Indiana, United States, Corresponding author: mamcknight@usi.edu.
[5] Associate Professor, University of Southern Indiana, United States, E-mail: blbueltel@usi.edu.

payment of a six-figure ransom sum within 24 hours to release it. If the company fails to make payment, attackers promise to publish elements of the data on the dark web and to otherwise destroy access to it permanently. In this moment of complete vulnerability, the manager not only wonders what more she could have done to prevent this doomsday scenario, but how she will inform clients about the scenario. She begins to feel even more concerned while contemplating the governmental reporting obligations while contacting her lawyer.

2. Introduction

In today's sophisticated, Internet-connected environment, one of the most impactful decisions a firm will ever make is the choice between prevention costs on the front end of a security event versus mitigation costs on the back end. The rise in ransomware attacks presents an alarming threat to the entire digitized American economy. Ever-evolving ransomware attacks have become all too common, victimizing even the most diligent and vigilant of organizations. Accountants and tax practitioners have, by no means, been exempted from this frightening trend. For instance, in 2020, the prominent accounting firm BST was victimized by an attack that illustrates just how dangerous ransomware-related security events can be. In targeting BST, the *Maze* ring of attackers accessed and obtained firm client records (Diana, 2020), including the records of health care provider Community Care. As a result, the attackers obtained medically related data of up to 170,000 patients held by Community Care (Anderson, 2020). Following this event, BSO and Community care have been targeted by class-action lawsuits for failure to take proper care in protecting client/patient data (Cropley, 2020).

The tales of caution unfortunately do not end with BST. In 2019, accounting and tax software giant Wolters Kluwer was also the victim of a high-profile ransomware attack (Fazzini, 2019). To prevent the event from spreading across its entire IT infrastructure, Wolters Kluwer was forced to shut down its entire system, including its CCH cloud-based tax division. Accountants across the United States and abroad were unable to access vital client records, tax return information, or personal information of their clients, causing delays in filing and missed deadlines (Kovacs, 2019). This event was significant enough that, in response, the IRS offered a seven-day extension to file taxes for those impacted (Cohn, 2019).

Ransomware is also not only merely an American concern. In June 2020, a Toronto accounting firm suffered a ransomware incident, and client information, including bank login credentials, was being offered for sale on a lesser-known online community referred to as the "dark web" (Solomon, 2020). Prominent Canadian accounting firm MNP was also hit with a ransomware-based cyberattack, which forced it to shut down its system and operations, closing for the week of April 17, 2020 (Abrams, 2020).

Ransomware attacks threaten the very survival of targeted firms (whether large, small, domestic, or international), presenting such organizations with a difficult road ahead. Those impacted by a ransomware attack will face life-altering business, financial and career consequences. Many firms victimized by ransomware may struggle to regain public trust, while others may not withstand the financial, regulatory, and reputational fallout.

Firms will then need to go through the unenviable task of explaining to customers that their personal, financial, and other sensitive data was stolen and/or destroyed. Casualties of ransomware attacks will be compelled to inform law enforcement and other government agencies, insurance carriers, and even

professional licensing authorities. Moreover, as ample data suggests that most thieves return data upon payment of a ransom demand, firms will also face the difficult decision of whether to pay the ransom. Even upon payment, the return of stolen data is not guaranteed and instead rests upon the honor of thieves.

As a result of the extremely sensitive nature of the data held by accounting firms, ransomware attacks present an existential threat to the entire profession. Accounting practices are businesses built on trust and confidence of the highest order, and, as a result, accountants hold a special place in client's lives. Along with this trust comes a sacred duty to take sufficient and appropriate measures to protect the ultra-sensitive data to which clients have been entrusted. It follows that protecting client data is one of the most significant of all professional responsibilities (Ryle et al., 2022).

2.1. Accountants and Ransomware

Few professional groups hold a more pressing reliance on the safety of, and continuous access to, critically sensitive data than those in accounting and auditing. These industries provide services to clients steeped in trust, confidence, and privacy. Clients require and assume as a matter of professional competence that information entrusted into the hands of another will be safely and securely obtained, transmitted, and stored.

While the threat to client confidentiality and data safety is very real, ransomware can place accountants in an almost unimaginable position of professional exposure. Victimization by such a ransomware attack can shatter public confidence, create crippling civil and criminal liabilities, and contribute to professional licensing for accounting professionals. Further, CPAs are being targeted by ransomware and other cyber-attacks more frequently because "Obtaining ... clients' tax returns, Social Security numbers, employer ID numbers, financial statements, and other sensitive data is like hitting the lottery for a hacker (Sheridan, 2015). The best path to avoid such horrific consequences is to ensure in advance that proper safeguards were designed, implemented, and maintained. The professional responsibility is clear – exercise professional due care and diligence in the face of an increasingly dangerous threat environment.

Getting a fix on ransomware statistics and data is an enormously difficult task. Failure to prepare for such an event has undoubtedly led many firms to capitulate to ransom demands quietly and out of public view. This is a double-edged sword as it does typically yield the return of encrypted data, but also provides an incentive for the attacker(s) to continue. Recent data suggests that the costs of ransomware payments are escalating rapidly, increasing by 41% from 2018 to 2019, and averaging over $190,000 by the end of the year (Popper, 2020). Add to this the fact that financial institutions and banking, government agencies, and critical infrastructure were the most targeted by hackers in 2018-2019 (Morgan, 2017), and a picture of low-risk, high-reward activity becomes clearer.

2.2. An Evolving Cyber-Threat Environment

Cybercrime is big business for both attackers and defenders - with an estimated $6 trillion cost globally in 2021 (Morgan, 2017). One factor driving cybercrime's explosive growth is its unique combination of profitability and anonymity. Successful ransomware attacks can yield substantial payments while providing cyber criminals with little chance of being caught. Proper attack attribution is difficult making the likelihood of being "brought to justice" near impossible (Katyal, 2001).

The organizational cybersecurity stakes have risen far beyond where they were just ten years ago. In the past, traditional forms of malware were much less perilous. Such threats were typically designed perhaps to simply destroy the contents of the machine where it was installed or allow the threat actor to log your keystrokes. Over time, malware adapted new capabilities and became more pernicious along the way. For example, malware became "wormable", meaning it could itself across a network without human interaction. It also developed the ability to check for antivirus before running to ensure attack success and became capable of intelligently seeking structural vulnerabilities. Finally, it has developed the ability to hold a system's data hostage or exfiltrate it in the hope of a ransom payment for its return. One particularly harmful tool of ransomware is to encrypt the endpoint or server, but also to seek out various forms of data backups and either delete them or encrypt them as well, rendering victimized entities wholly at the mercy of their assailant.

Ransomware attacks now outnumber classic security breaches as the most prevalent form of cybercrime (Francis, 2016). This is a matter of increasing importance as ransomware attacks are increasing in size, frequency, and overall destructiveness. For example, in 2021 there were 623.3 million ransomware attacks, which was an increase of 105% from 2020 (Griffiths, 2024). It should come as no surprise then that ransomware is also increasing in overall cost to the US economy, to the tune of approximately $7.5 billion in 2019 (O'Neill, 2019). Like any form of technology, ransomware will continue to evolve.

2.3. Ransom Payment Costs

The most obvious financial consequence of being victimized by ransomware derives from the ransom payment itself, should an organization choose to pay it. As ransomware criminals have tasted success, they have upped the ante, requesting larger and larger payments over time. Ransomware requests are often tailored to the size and financial resources of the target company. Moreover, some "rings" of attackers offer call centers whereby target companies can receive the assistance necessary to complete the deal, including the process of creating any required virtual currency wallet to effectuate the ransom payment (Ng, 2017). There may also be fees associated with consulting with legal advisors before and commensurate with the payment.

2.4. Post-Incident Costs

Whether or not a ransomware payment is made, the post-ransomware cleanup process can be difficult and expensive. Victimized companies need to do a complete system review and address any deficiencies found. Ransomware attacks expose institutional vulnerabilities and require a comprehensive post-mortem analysis of what went wrong and why. Organizations may commission an independent third-party forensic review evaluating what transpired, including a thorough and complete examination of the events, processes, and system vulnerabilities that made the intrusion possible. Depending upon what is found on forensic examination, organizations will then incur the cost of remediation, including additional training, programming, software, hardware, and other remediation costs to bring the system back up to acceptable standards. Next, firms may then be compelled to commission independent third-party penetration testing of the new system for its adequacy. Recovery costs are not cheap, and by one recent estimate now average over $84,000 per incident (*Coveware*, 2020), exclusive of payments to the attackers.

2.5. System Downtime Costs

System downtime leads to interruptions in operations, missed deadlines for customers and other stakeholders, out-of-pocket expenses, and lost revenue. System functionality remains impaired for an average of ten days following a successful attack, compromising an organization's ability to conduct its operations or service its clients (Davis, 2019). While downtime costs will vary depending on the size, complexity, and extent of penetration damage, what is clear is that downtime costs are substantial and rising. One recent estimate indicated such costs increased by more than 200% from 2018 to 2019, reaching an average of $141,000 (*Datto, 2020*). Costs will likely increase with organizational size, the length of the downtime, and the extent of system damage.

2.6 Collateral Damage Costs

From a cybercriminal's standpoint, ransomware attacks can be the gift that keeps on giving, providing valuable data and other resources to exploit for years to come. Successful ransomware attacks spoil not only ransomware payments but valuable firm and client data as well. Ransom payment aside, cybercriminals can profit by selling data on the dark web or by exploiting it for other nefarious purposes. As collateral damage may prove costly to clients and other impacted stakeholders, it will also expose victimized firms to secondary civil liability claims. As we have previously examined, several firms have been sued for failing to adequately protect client data.

Another collateral form of attack is through the spoils of the first ransomware attack. For example, criminals can exploit stolen password information to obtain a new attack vector for future use. This can be utilized to re-infect the companies far into the future and to enable future attacks or reconnaissance intrusions, all with little risk of ever being caught. Cybercriminals have also been widely exploiting stolen client tax information to file fraudulent tax returns. (Schlesinger and Day, 2018).

2.7. Civil Penalties, Criminal Penalties and Licensing Complications

The failure to protect client data could also create professional problems for accountants. CPAs must secure confidential client data under both the AICPA Code of Professional Conduct as well as IRC § 7216. Failure to do so could result in professional misconduct claims by licensing authorities (Cheng, *et al.*, 2019). IRC § 7216 also provides criminal penalties (including imprisonment for up to a year) for those who knowingly or recklessly disclose tax information potentially including the reckless failure to properly secure data (Rule, 2019).

Accountants possess a solemn obligation to protect non-public information from unauthorized access. Ransomware attacks resulting in such unauthorized access may spur heightened regulatory scrutiny, revealing GLBA non-compliance issues. Many CPAs and tax practitioners are classified as "financial institutions" under the GLBA's "Safeguards Rule," and as such, are required to comply with statutory and regulatory requirements to protect non-public client data (Phan & Morehead, 2020). Firms are currently required to have a written security plan in place, to designate an employee to coordinate the information security program, to assess and identify data-related risks to design measures to protect against such risks and to monitor and test the measures, to oversee external vendors, and to adapt and modify security measures over time as lessons are learned and as needs change (Ryle, Yan & Gardiner, 2021).

The FTC is authorized to enforce these requirements and failure to comply with the Safeguards Rule can result in substantial penalties (McAndrew *et al.* 2017).

This is even more significant as the FTC has proposed sweeping modernizing changes to the "Safeguards Rule." If adopted, these changes will require covered accountants to radically transform cybersecurity practices. Among the most notable of the numerous proposals is the requirement to retain a Chief Information Security Officer or CISO. Moreover, firms will be required to either conduct continuous system monitoring or conduct annual system penetration tests. As these requirements are soon to expand, firms need to take note and consult with appropriate IT and data security professionals immediately. Failure to comply with Safeguards Rule requirements could result in civil and criminal penalties (Ryle, Jie, and Gardiner, 2021).

2.8. Reputational Damage

Finally, a firm may suffer irreparable reputation damage from a publicly exposed ransomware attack. Companies that endure a significant and well-publicized data breach suffer both immediate and sustained reputational damage (Choong *et al.*, 2017). As eloquently stated by leading Global Chief Information Security Officer and Board Advisor, Société Générale IBFS, Stephane Nappo "[i]t takes 20 years to build a reputation and few minutes of cyber-incident to ruin it (Thakur, 2018)." To businesses steeped in trust and confidence (such as the accounting profession), however, reputational harm imposed by a successful ransomware attack could prove fatal to one's reputation. This loss of trust is almost certain to lead to a permanent loss of business and revenue streams.

3. Methodology

The present research utilizes a dual approach to qualitatively analyze several recent events experienced by organizations related to information security issues to provide meaningful purpose and intent toward action on the part of account professionals faced with the threat of cyber-attacks. More specifically, this paper employs a combination of grounded theory (first) and action research (second) as a means of investigating the impact and involvement of accounting professionals in the response to a ransomware attack. This qualitative approach is followed by attack response data gathering and cluster analysis to provide a framework of guidance for accounting professionals who may be faced with the impact of a ransomware attack.

3.1. Grounded Theory

Grounded theory has been used for decades as a general approach and means of analyzing qualitative data. Though there are slight variations of grounded theory as a methodology, the two main schools of thought both provide an inductive process that is aimed toward theory development (Charmaz, 2000). Charmaz (2003) notes that the use of grounded theory is based on a method consisting of flexible strategies…to construct "middle-level theories" directly from data analysis.

Grounded theory is the discovery of emerging patterns in data and is the generation of theories based on those patterns in data (Walsh, et. al., 2015). Walsh, et. al., (2015) explain that grounded theory which is positivist is much more objective and applied, and interpretive grounded theory is much more of an acknowledged interpretation, with practitioner literature falling somewhere between the two

applications of grounded theory. For the present research, the linking of the methodology to practitioner literature makes it an ideal fit given the purpose of the research. The methodology simply looks for patterns within a defined dataset to make meaningful interpretations related to those constructs and ideas. The specific stages used in grounded theory involve:

- Identifying the substantive area (area of interest).
- Collect data about the substantive area.
- Coding data into categories as collected.
- Write theoretical memos linking concepts to other concepts.
- Conduct selective coding and theoretical sampling (picking the most critical categories).
- Sort memos to find theoretical codes that best organize data.
- Read literature and integrate it with the theory.
- Write up the theory.

(Grounded Theory Online, 2022).

Grounded theory is significant for many reasons, including providing clear guidelines for conducting qualitative research, streamlining data collection and analysis, and legitimizing qualitative research as scientific inquiry (Charmaz, 2003).

3.2. Action Research

Action research is a family of research methodologies that pursue action or change and research simultaneously (Dick, 1999) "adopted by a researcher to solve an immediate problem" (FiveVidya, 2019) geared toward enacting social change (Bogdan & Biklen, 1998). Action research is conducted in situations in which the researcher will observe events and then identify an issue or problem to address. Common methods involve observations of individuals, and groups, taking field notes, etc. (FiveVidya, 2019). Bogdan & Biklen (1998) assert that action research not only seeks to solve problems but also to expose corruption, scandal, or injustice.

3.3. Attack Response Data Collection

The qualitative analysis provided here is followed by an approach to support the development of a framework that can be used by accountants who are faced with the reality of a ransomware attack.

Twenty resources were used as guidance for the development of a response framework. These sources included professional agencies well established in the field of cybersecurity, providers of cyber services, and governmental agencies or consultants which are widely used as references for cyber response mechanisms (e.g., the National Institute of Standards and Technology, the Cybersecurity, and Infrastructure Security Agency).

Each of these resources detailed activities appropriate for responding to a ransomware attack. The activities from each resource were put into a matrix. A cluster analysis was then performed by grouping like activities together and giving the clusters a name appropriately summarizing the nature

of the grouping. In this manner, a series of seven responses were identified for use in this paper. These seven activities serve as a framework that gives details relevant to accounting professionals responding to a ransomware attack.

3.4. Research Methodology Applied to the Current Case

Our methodology sought to combine grounded theory, action research, and quantitative data collection to provide a focus that could support a framework to prepare accounting professionals to deal with issues related to ransomware attacks. This approach resulted in a four-step process:

- Review relevant literature.
- Identify recent and relevant events related to ransomware attacks.
- Establish a motivation for and importance of the impact of ransomware on accounting professionals.
- Use a data-supported approach to provide a practical guidance framework (theory) for accounting professionals facing the impacts of ransomware.

4. Ransomware Response for Accounting Professionals

Based on our analysis of resources and their recommendations for response to ransomware, we developed a framework of response activity directed at the accounting professional. Each of these activities may represent activities ranging from minimal effort to extensive collaboration on the part of the accounting professional. Regardless of the extent of one's involvement, knowledge of all response activities will be beneficial such that each may be expedited by the accounting professional and impacts from a ransomware attack minimized.

The framework consists of seven response activities. The activities were given a sequence which made chronological sense to the authors and was supported by the sources that were researched. Yet, it should be noted that organizations with response teams dedicated to cyber-attack response might dictate a different sequence. Additionally, some of these activities may be carried out in parallel. The seven response activities were identified as: activate incident response structures, isolate/stop the ransomware, assess the intrusion, remove the ransomware, and repair vulnerabilities, recover data, report/communicate to key stakeholders, move forward. Each of these response activities is discussed in detail in this section.

4.1. Activate Incident Response Structures

The first activity in response to a ransomware attack may be as simple as acknowledging the attack and moving on to the following steps. In the case of an accounting professional acting alone, this could well be the case. Many organizations that have IT support entities will likely have more complex structures that should be enacted. A business continuity plan or, more specific to cybersecurity, an incident response plan (IRP) should have specific instructions that will help address many, if not all, of the following steps and should be used as a guide. In some cases, there will be an incident response team (IRT) expressly trained and knowledgeable about ransomware and many other

types of attacks. Where an accounting professional acting alone would be one end of a continuum of response activity, the other would be for the accounting professional to turn over all further response activities to an IRT. Regardless of where one lies on the continuum, it is best to be knowledgeable about the following steps as the individual can have responsibilities requiring engagement with the IRT.

4.2. Isolate/Stop the Ransomware

After consulting any incident response plan, the next step should be to isolate/stop the ransomware from doing any further damage. In many cases, it would be wise to initiate this response in parallel with the first step in this framework as it could be important to limit the extent of any damage caused by the attack.

One item of importance that was identified in this research is a word of caution against turning off an infected machine. All but one resource was firmly against this activity and even cautioned that it should be strictly avoided. Cyber-attacks may require forensic investigation techniques for one or more of the following response activities. An important factor in forensic investigations is that any impacted machines remain powered on. Volatile memory in a computer is lost when the machine is powered down. In many cases, malware or other attack remnants are resident in memory and need to be preserved to carry out a thorough investigation.

To isolate any further threat any machine that is identified as or even suspected of being impacted by ransomware should be removed from the network. This includes both wired and wireless communications and means consideration of all wireless communication forms like Wi-Fi, Bluetooth, NFC, and IR. Any network wires should be removed from the machine and any wireless communication services turned off.

While cyber-attacks are often considered ‘virtual’, physical security also plays a role. To prevent any potential further damage by way of physical access, any impacted machines should be labeled or locked in a restricted area so that they are not used by anyone not involved in the response activities.

4.3. Assess the Intrusion

After any impacted machines have been isolated, an assessment should be performed. A deep analysis might need to be turned over to a cybersecurity analyst, though there are important steps that can be taken by accounting professionals. The goals of this step are to trace an attack to its origin and make some determinations about the extent of the damage.

In an overwhelming majority of cases, ransomware attacks can be traced to emails. Either an attachment to an email containing the virus or a link in the mail directs the receiver to a web page with scripting that downloads the virus. An investigation of suspect emails and recent related actions is an important part of the assessment. Tracing the path of the email to other clients either within or external to the organization should also be considered. This information should be recorded for further analysis or turned over to others if an IRT is performing the investigation.

Ransomware works by informing the target of the infection and giving direction as to how the ransom might be paid to receive a decryption key which will restore access to the files being ‘held ransom’.

Any notes or other communications involved in this process should be captured as evidence for further investigation and further consideration in the later stages of this response framework.

All files and directories impacted by the attack should be documented. An accurate account of the extent of the damage will be critical to ensuring later steps to recover from the attack are effective.

4.4. Remove the Ransomware and Repair Vulnerabilities

After a determination has been made about the origin and extent of the attack, steps can be taken to remove the ransomware from the impacted machines and seek to repair any vulnerabilities that may have been exploited or created by the attack.

The removal of malware is generally performed using tools dedicated to such a purpose. The broader family of these tools is referred to as 'anti-malware' or even an 'internet protection suite'. These tools can be used on infected machines to identify and quarantine any infected files.

There are more robust tools available to the cybersecurity professional or anyone who desires to perform a deeper analysis which would include the forensic investigation mentioned earlier. This may be necessary if the anti-malware tools are not effective. Some of these come in the category of 'freeware' or 'shareware' and can be quite effective at identifying and eradicating threats. The only drawback for the accounting professional would be the learning curve associated with the knowledge needed to use these tools. Where an IRT may be involved, this type of analysis and removal can be turned over to the team. In the case of an accounting professional who is without such support, there are a range of consultants that provide such capabilities.

Ransomware may be a result of an email intrusion. However, there may be other vulnerabilities that allow the ransomware to infiltrate the system. One such example could be if there were no anti-malware software installed on the machine, or if there were no method or systematic approach to ensuring such software is continuously updated. This or any other vulnerability that allowed the ransomware to access the machine should be identified and resolved as a part of this step. The identity of the virus captured from earlier analysis can be referenced in one of several international data repositories of computer information threats (e.g., cve.mitre.org). These data repositories will help reference related vulnerabilities and remediations when a specific threat can be identified.

4.5. Recover Data

Data recovery should take place and is only possible after any infections have been identified and removed. Unfortunately, reinfections are common where thorough analysis was not performed and can result in starting the response approach over.

An important decision must be made at this point in the response framework as to whether the ransom should be paid as a means of recovering any lost data. The official recommendation from the FBI, or any other law enforcement agency, will be that a ransom should never be paid in this situation. There is never any guarantee that paying a ransom will produce the needed decryption key. The bad actors perpetrating such crimes are aware of the reputational aspects of their 'business'. Some may find it amusing that the most successful bad actors will provide 'customer service' with chat services, emails, or even phone numbers to ensure their decryption keys are performing as promised. They are aware

that if the word gets out that paying a ransom does not restore information, few, if any, will pay. Many will even negotiate terms of the ransom if communications are opened.

Another approach can be to attempt to crack the encryption scheme used by the ransomware. As with the cyber analysis and cyber forensic tools, there are 'freeware' and 'shareware' tools available through cybersecurity communities that can be used to attempt cracking of encryption. Sadly, cracking encryption can be time-consuming and success rates for such attempts are low.

The most reliable method of recovering data from a ransomware attack is to use data backups to restore the most recent data available. Care should be taken to ensure backups did not capture data after the ransomware infection. Information from analysis performed in prior steps of this framework will be important to making this determination. It should also be noted that this method may result in the loss of some data. Data completeness will depend on the frequency, type, and method of backup used by the accounting professional/organization.

One final option may be to recreate the data from scratch. This approach may only be practical if the extent of the infection is small and the originators of the data are available, still, it may be a viable option.

The approach taken to restore data may be a complicated one. The state of backups, the urgency of the restoration, and the technical expertise of the accounting professional and/or the IRT will all play a role amongst potentially many other factors. The next step in this framework details communications to key stakeholders which includes law enforcement. It could be advantageous to start those communications in this step. Law enforcement may have advice based on experience with ransomware or simply ransomware in general. Cyber consultants may also have relevant experience that could prove valuable in the decision-making process.

4.6. Report/Communicate to Key Stakeholders

A cyber-attack should be communicated to all key stakeholders as soon as relevant information can be put together in a way that it may be useful. Contrary to some belief, cyber-attack information should be shared. The cyber defense community is made stronger by the sharing of information. Organizations have a responsibility to their stakeholders to keep them informed. The following is a list of stakeholders that are relevant to most accounting professionals.

- **Internal employees:** This can start with a notification to other employees in the organization so that they may be aware of and vigilant for the threat.

- **IT/Security Staff:** As mentioned previously, there may be parts of the organization dedicated to such responses. If they had not been notified before this stage, they should be notified now.

- **Customers:** If the attack impacted customer data in any way, they should also be notified of what had happened and what had been done to correct the incident. Further investigations may be needed to determine if the attack did anything other than to encrypt data. Some ransomware attacks will take extra steps to copy some or all files to another location for distribution on the dark web.

- **Cyber Sharing Community:** The database mentioned in section 4.4 is maintained by a non-profit, global consortium dedicated to protecting informational resources. This information is shared freely for the benefit of all. While Mitre (mitre.org) is possibly the largest of these, there are many information-sharing organizations around the world dedicated to the same purpose. Information shared

with these organizations betters response capabilities for all and should be considered when attack information is being communicated.

- **Law Enforcement:** Cyber-attacks are illegal. If law enforcement had not been contacted in prior steps, they should be notified at this stage for similar purposes to other stakeholders. Law enforcement will also make use of any attack information to update their knowledge bases. They may also help track down attackers and prevent further attacks.

- **Cyber Insurance Agencies:** Cyber insurance is an option (or even necessity) for organizations' business continuity. In some cases, policy or law can dictate that it is mandatory depending on the nature of the information being retained by an organization. In the previous step in this framework, there were options discussed for recovering data that was lost in an attack. It may be important to involve cyber insurance agencies in that decision-making process. If that hadn't been done prior, it would be important to contact the agency at this time to recoup any costs that are covered.

4.7. Move Forward

When an attack has been found and eradicated, vulnerabilities have been repaired, data has been restored, and the incident has been communicated, it is time to consider any actions necessary to move forward. As is common in project management, a look back over how the incident was handled for discussion and/or documentation regarding lessons learned is appropriate. Any outstanding action items should be dealt with. This can be an important time to address any shortcomings in the incident response procedure regardless of whether the responsibilities lie with an individual, team, or people across several teams.

A review of how the process went using the framework presented here could yield valuable documentation for future activities in response to cyber incidents. Some important questions to address include the following:

- Was there adequate technical expertise available to respond to this incident or should a more robust IRT be considered?
- How quickly were impacted systems identified and isolated?
- Are access rights, technical resources, or other abilities necessary to respond quickly to a cyber-attack?
- Are there purchases to be made for tools, service level agreements, or other contracts that will improve response to cyber-attacks?
- Should data backup tools and processes be updated or improved in some manner?
- Is a list of key contacts for stakeholder communications created and maintained?

While this list of questions is not comprehensive, it is a good start to addressing a look back over the response framework and considering how to better position the individual accountant or the organization to move forward with more confidence should another cyber-attack manifest.

5. Recommendations for Good Cyber Hygiene

The framework discussed in this paper can be a tool for aiding accounting professionals when responding to a ransomware attack. Yet, in cybersecurity, prevention is always preferred to response. It is important to evaluate business operations and resources and ensure that there is at least some minimal level of a cybersecurity perimeter that aids in protecting valuable information assets. To this end, the following are considerations that can aid in determining the level of cybersecurity that exists and may inform an individual or an organization on the next steps toward creating or updating a cybersecurity perimeter.

5.1. Conduct a Risk Assessment

As a foundational measure, firms should conduct a comprehensive organizational risk assessment. This will constitute a foundational step in the design of any comprehensive security program by returning valuable information for use in system design. Such an assessment should include an examination of one's current security infrastructure, practices, and procedures, and an evaluation of this against potential threats.

Policies and laws may dictate these types of assessments happen regularly. Certain policies and laws (e.g., PCI-DSS, GLBA, SARBOX, etc.…) will have specific requirements that must be met and documented in assessment reports. Audits may be performed internally or externally depending on the enforcement agency involved.

5.2. Implement Basic Security Controls

Firms should ensure that appropriate, cost-effective basic security measures are in place and are being followed by the enterprise. The controls presented below are what we consider standard practice and should be considered regardless of the outcome of the threat and vulnerability assessments conducted previously.

a. *Develop an Information Security Incident Response Plan:* Firms should develop, implement, and employ an organizational security incident response plan. After adoption, the firm should conduct incident response training for all personnel, perhaps including mock "live fire" exercises to improve organization response, dexterity, and preparedness.

b. *Regularly Back Up Data:* Firms should regularly back up data and be sure to validate those backups. A common practice is to duplicate backups offsite.

c. *Utilize Strong Network Boundary and Endpoint Protections:* Firms should utilize strong network and endpoint protections, including network firewalls, web application firewalls, intrusion detection/prevention systems, and next-generation antivirus products where possible.

d. *Require Multifactor Authentication:* An easily implementable measure with big security returns can be the implementation of and requirement for multifactor authentications for all remote access to corporate systems over the internet, including webmail and VPN.

e. *Apply All Vendor-Provided Updates Packages:* Firms regularly implement software and firmware updates as they become available.

f. *Restrict Physical and Logical Access to the Company Network:* Methods and routes of access to the organizational network including wall jacks where one might plug in a data cable and wireless access points must be identified, limited, or selectively eliminated. Encryption should be verified on all wireless communications.

g. *Reset Default Settings and Passwords:* Firms should reset all settings and passwords before deploying new devices on a network. At a minimum, all administrator credentials should be changed or removed.

h. *Implement and Enforce Complex Password Requirements:* Firms should employ complex and mandatory password requirements, which helps prevent password-related intrusions.

5.3. Appoint a Chief Information Security Officer (CISO)

In a measure that many small firms may have overlooked, every organization deserves a designated and capable chief information security officer (CISO). Events happen on an instantaneous basis. Firms require qualified professionals who can assist, at a moment's notice, with any misfortune that may occur. Moreover, hiring a CISO may soon be required of many firms due to the proposed and pending changes to the "Safeguards Rule," which is discussed in-depth below.

5.4. Create a Data Tiering System

Organizations should engage in a review and assessment of all firm and client data categories and sensitivities. Upon this review, firms should identify data with a high risk of loss and a high damage magnitude if lost. For clients in the banking and healthcare industries, a firm may possess extremely sensitive information. The release of such information could create devastating consequences for both the firm and the client. Firms should deploy limited firm resources to place extra protective measures around these data sets to help protect against loss. By contrast, data with a low loss or low likelihood of loss profile may not be deserving of such protections.

5.5. Adopt a Data Minimization Posture

Firms should audit existing data acquisition practices to minimize data acquisition and retention. Firms should acquire and retain only as much information as is necessary for the task at hand. When finished with the data, firms should employ a policy of immediately and permanently deleting unnecessary information. Finally, information should only be kept if it is needed for business purposes or required by law. Records are costly to store and increase breach exposure for firms and clients. Streamlining the acquisition and retention of records will reduce both costs.

5.6. Train Employees–But Do Not Depend on Training Alone

Firms should set a tone that promotes data security from the top of the organization and regularly reinforce the importance of information security practices with all staff. Training should not only be conducted during employee onboarding but should continue for the duration of employment. Awareness training is available from a multitude of reputable vendors for a nominal fee and typically has one of the higher rates of return among all security controls (Schultz, 2019).

5.7. Encrypt All Sensitive Data

Companies should utilize encryptions for all sensitive data so that exfiltrated data cannot be exploited without the necessary decryption keys. Further, data should be encrypted with industry-standard encryption protocols and private keys should be properly safeguarded since the theft of these keys renders encryption useless.

5.8. Monitor Logs Regularly

All computing devices can retain logs of the activities that occur on them. Resources should be dedicated to monitoring logs and configuring alerts from all critical infrastructure which signify the possibility of an attack. There are products for purchase or as freeware/shareware which can aid in this process.

5.9. Assemble, Empower, and Authorize an Incident Response Team

Organizations should proactively establish an incident response team (IRT). This IRT should convene at least once annually to review the Incident Response and Business Continuity plans, participate in tabletop exercises, and ensure all stakeholders agree on how to proceed in situations such as these with the information available to them at that time.

5.10. Establish an Offline Emergency Response Kit

If a successful ransomware attack is launched against an organization, it could take down an entire network and all or most electronic access. For this reason, it is important to maintain a list of procedures, steps, and key contacts in an offline location, ideally in print format. The list of key contacts should include the name and telephone number of:

1. All members of the incident response team
2. The local FBI field office
3. State Police
4. Internet service provider security department, and
5. Support contacts for vendors whose products the company deploys.

5.11. Consider Cybersecurity Insurance

Cyber threats continue to morph and increase in complexity and even the most prepared organizations may fall victim to threat actors. For incidents with a lower likelihood of occurrence but higher impact, consider cybersecurity insurance. To protect against crippling legal liability resulting from a ransomware attack, accountants should consider procuring liability insurance covering cyber extortion and third-party liability coverage extending to others (like passengers) deriving from cyberattacks (Raver, 2019). Policies can vary in coverage and complexity and CPAs should consider the size and nature of their practice as well as the volume of personal information possessed, conduct a thorough threat assessment, employ appropriate precautionary measures, and then insure accordingly.

5.12. Engage in Working Groups with Other Organizations

Having a strong network of security colleagues, particularly from other companies within the same vertical space, can be the difference between success and catastrophic failure. Partnering with other industry leaders and even competitors to share threat information, best practice information, and emerging methodologies can help firms stay up to date with what is most important and threatening to clients, enabling affected parties to act accordingly. Many industries have working groups devoted to cybersecurity best practices designed to support this effort and many industry-agnostic groups are covering a broader threat landscape, such as ISSA International, ISC^2, and ISACA.

Many of the measures and steps we have outlined are reasonable and affordable for any organization to adopt and employ. The importance of taking proper precautionary matters cannot be overstated and may prevent certain claims for lack of proper care, negligence, or recklessness from bring successfully alleged against the firm and its executives down the road.

6. Conclusions and Limitations

Accountants and other financial services professionals operate in dangerous times. To counter an ever-expanding universe of threats, accountants must be both proactive and vigilant. Firms must understand that a ransomware attack – or one of a litany of other malware attacks - could come at any time day or night. The next opened email, the next visited website, or the next failure to prevent a targeted network penetration could prove fatal to a firm and career-ending for its leaders. Firms should therefore prepare as if an attack is imminent.

This paper identified a framework that may be used to respond to a ransomware attack. While it was developed specifically for the context of ransomware, it could also prove useful for other types of cyber-attacks.

Further discussed was the importance of good cyber hygiene which can position an accounting professional or an organization to be better protected against all types of potential cyber-attacks. What is considered appropriate in each organization or for everyone depends on the particulars of any given situation (Bose, 2019), including the nature of threats being faced, the nature of the data held, and security processes and procedures in place. Risk tolerance, or the level of risk a firm is willing to tolerate to achieve its goals will often be highly influenced by the nature and character of data in possession (Dev & Rao, 2018) and, in turn, affect the protections each employs.

It should be noted that no cybersecurity or data protection strategy is 100% secure from threats. The response framework and general security recommendations given in this paper can help meet a commitment to maintaining a rigorous system security plan that helps ensure the safety of client data. Simple measures such as the effective utilization of security controls, regular internal audits, and continuous monitoring will not only help protect accountants but help address concerns of data confidentiality, integrity, security, and reliability.

This research referenced twenty prominent and credible resources in the cyber community when the response framework was developed. Since the technology used and the nature of cyber-attacks is constantly changing, it is not unreasonable to assume additions or changes to this framework may be necessary in the future. Additional resources may also be started or identified with credible contributions. The recommendations in this paper should be considered a base to be improved upon.

References

Abrams, L. (2020). *Leading accounting firm MNP hit with cyberattack.* Retrieved from https://www.bleepingcomputer.com/news/security/leading-accounting-firm-mnp-hit-with-cyberattack/ (accessed 13 August 2020).

ACA Global (2021). *Ransomware 101 Part 3: How to Respond to a Ransomware Attack.* Retrieved from https://www.acaglobal.com/insights/ransomware-101-part-3-how-respond-ransomware-attack (accessed 20 June 2022).

Anderson, E. (2020). *January report identified BST as hacking victim.* Retrieved from https://www.timesunion.com/business/article/Computer-breach-exposes-some-Community-Care-15067744.php (accessed 9 September 2020).

Balaji, N. (2021). *Ransomware Attack Response and Mitigation Checklist.* Retrieved from https://gbhackers.com/ransomware-checklist-mitigation/ (accessed 21 June 2022).

Bisson, D. (2017). *How to respond to a ransomware infection.* Retrieved from https://grahamcluley.com/how-to-respond-to-a-ransomware-infection/ (accessed 21 June 2022).

BlackPanda (2022). *How to Respond to Ransomware.* Retrieved from https://www.blackpanda.com/dfir-fundamentals/how-to-respond-to-ransomware (accessed 21 June 2022).

Bogdan, R. C. & Biklen, S. K. (1998). *Qualitative research for education: An introduction to theory and methods.* Needham Heights, MA: Allyn & Bacon.

Bose, R. (2019). *How can airlines protect their customers and data from evolving cyberthreats?* Retrieved from https://securityintelligence.com/posts/how-can-airlines-protect-their-customers-and-data-from-evolving-cyberthreats/ (accessed 7 June 2020).

Cawthra, J. et.al. (2020). *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events.* Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-26.pdf (accessed 20 June 2022).

Charmaz, K. (2000). *Grounded theory: Objectivist and constructivist methods.* In N. K. Denzin & Y. S. Lincoln (Eds.), Handbook of qualitative research (2nd ed., pp. 509-536). Thousand Oaks, CA: Sage.

Charmaz, K. (2003). *Grounded theory*. In the SAGE Encyclopedia of social science research methods. Thousand Oaks, CA: Sage.

Cheng, C.; Flasher, R. & Higgins, J. P. (2019). *Accounting firm data breaches: One state's records.* Retrieved from https://www.journalofaccountancy.com/issues/2019/jun/accounting-firm-data-breaches.html (accessed 7 June 2020).

Choong, P.; Hutton, E.; Richardson, P. S. & Rinaldo, V. (2017). *Protecting the brand: Evaluating the cost of security breach from a marketer's perspective.* Retrieved from https://www.articlegateway.com/index.php/JMDC/article/view/1644/1561 (accessed 8 January 2021).

CISA (2022). *Ransomware Response Checklist.* Retrieved from https://www.cisa.gov/stopransomware/ive-been-hit-ransomware (accessed 21 June 2022).

Cohn, M. (2019). *IRS offers guidance to CCH users on tax extensions after outage.* Retrieved from https://www.accountingtoday.com/news/irs-offers-guidance-to-wolters-kluwer-users-on-tax-extensions-after-cch-outage (accessed 9 August 2020).

Coveware, (2020). *Ransomware costs double in Q4 as Ryuk, Sodinokibi proliferate.* Retrieved from https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate (accessed 9 August 2020).

Cropley, J. (2020). *Class-action lawsuits sought over community care physicians data breach.* Retrieved from https://dailygazette.com/2020/06/17/class-action-lawsuits-sought-over-community-care-physicians-data-breach/ (accessed 11 August 2020).

Datto (2020). *Global state of the channel ransomware report.* Retrieved from https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf (accessed 8 January 2024).

Davis, J. (2019). *Ransomware costs on the rise, causes nearly 10 days of downtime.* Retrieved from https://healthitsecurity.com/news/ransomware-costs-on-the-rise-causes-nearly-10-days-of-downtime (accessed 7 June 2020).

Dev, A. & Rao, V. (2018). *Quantification of cybersecurity risk.* Retrieved from https://rmajournal.org/rmajournal/april_2018/MobilePagedArticle.action?articleId=1364305#articleId1364305 (accessed 8 January 2021).

Diana, C. (2020). *Another class action suit filed over BST, community care ransomware attack.* Retrieved from https://www.bizjournals.com/albany/news/2020/08/05/bst-community-care-ransomware-lawsuit.html (accessed 9 September 2020).

Dick, B. (1999). What is action research? Retrieved from http://www.scu.edu.au/schools/gcm/ar/whatisar.htm (accessed 17 May 2022).

Dtonomy (2020). *6 Critical Steps for Ransomware Incident Response.* Retrieved from https://www.dtonomy.com/6-critical-steps-for-ransomware-incident-response/ (accessed 20 June 2022).

Edmondson, J. (2021). *Responding to a Ransomware Attack: The crucial initial steps businesses must take.* Retrieved from https://www.businesstechweekly.com/cybersecurity/data-security/respond-to-ransomware-attack/ (accessed 21 June 2022).

Fazzini, K. (2019). *A malware attack against accounting software giant Wolters Kluwer is causing a 'quiet panic' at accounting firms.* Retrieved from https://www.cnbc.com/2019/05/08/wolters-kluwer-accounting-giant-hit-by-malware-causing-quiet-panic.html (accessed 7 September 2020).

FiveVidya (2019). *Action research vs. case study: Know the key difference between two qualitative research methods.* Retrieved from https://www.fivevidya.com/blog/action-research-vs-case-study-know-the-key-difference-between-two-qualitative-research-methods/#:~:text=Action%20research%20is%20a%20type,by%20improvising%20their%20current%20practices. (accessed 28 May 2022).

Francis, R. (2016). *The history of ransomware.* Retrieved from https://www.csoonline.com/article/3095956/the-history-of-ransomware.html (accessed 7 June 2020).

Griffiths, C. (2024). The latest 2023 ransomware statistics. Retrieved from https://aag-it.com/the-latest-ransomware-statistics/ (accessed January 8, 2024).

Grounded Theory Online (2022). *How do you do grounded theory?* Retrieved from https://www.groundedtheoryonline.com/what-is-grounded-theory/ (accessed 16 March 2022).

Insider (2021). *If your business is the victim of a ransomware attack, here are the 6 immediate steps to take.* Retrieved from https://www.businessinsider.com/sc/how-businesses-should-respond-to-ransomware-attacks-2021-3 (accessed 20 June 2022).

Katyal, N. K. (2001). Criminal law in cyberspace. *149 University of Pennsylvania Law Review*, pp. 1074-1075.

Kime, C. (2021). *How to Recover from a Ransomware Attack.* Retrieved from https://www.esecurityplanet.com/threats/how-to-recover-from-a-ransomware-attack/ (accessed 20 June 2022).

Kovacs, E. (2019). *Information services giant Wolters Kluwer hit by malware attack.* Retrieved from https://www.securityweek.com/information-services-giant-wolters-kluwer-hit-malware-attack (accessed 7 September 2020).

Long, P. (2017). *Respond to ransomware in three steps: secure, assess, recover.* Retrieved from https://www.networkworld.com/article/3192175/respond-to-ransomware-in-three-steps-secure-assess-recover.html (accessed 21 June 2022).

MagMutual (2022). *Immediate Response to a Ransomware Attack.* Retrieved from https://www.magmutual.com/learning/article/immediate-response-ransomware-attack/ (accessed 20 June 2022).

Mcafee (2022). *How to respond to a ransomware infection.* Retrieved from https://kc.mcafee.com/corporate/index?page=content&id=KB89805 (accessed 20 June 2022).

McAndrew, E. J.; Phan, K. & Sargsian, Z. A. (2017). *FTC settles GLBA enforcement action against TaxSlayer stemming from 2015 data breach.* Retrieved from https://www.natlawreview.com/article/ftc-settles-glba-enforcement-action-against-taxslayer-stemming-2015-data-breach (accessed 7 June 2020).

Morgan, S. (2017). *Cybercrime damages $6 trillion by 2021.* Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (accessed 7 June 2020).

Ng, A. (2017). *Malware now comes with customer service.* Retrieved from https://www.cnet.com/news/ransomware-goes-pro-customer-service-google-25-million-black-hat/ (accessed 7 June 2020).

O'Neill, P. H. (2020). *Ransomware may have cost the US more than $7.5 billion in 2019.* Retrieved from https://www.technologyreview.com/2020/01/02/131035/ransomware-may-have-cost-the-us-more-than-75-billion-in-2019/ (accessed 9 August 2020).

PCProfessional (2021). *How to Respond to Ransomware and Malware Cyberattacks.* Retrieved from https://www.pcprofessional.com/2021/02/08/how-to-respond-to-ransomware-and-malware-cyberattacks/ (accessed 20 June 2022).

Phan, K. & Morehead, K. (2020). *FTC holds workshop on GLBA safeguards rule.* Consumer Finance Monitor. Retrieved from https://www.consumerfinancemonitor.com/2020/07/20/ftc-holds-workshop-on-glba-safeguards-rule/ (accessed 17 September 2021).

Popper, N. (2020). *Ransomware attacks grow, crippling cities and businesses.* Retrieved from https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html (accessed 7 June 2020).

ProvenData (2021). *Top 6 Ransomware Incident Response Actions.* Retrieved from https://www.provendatarecovery.com/blog/top-6-ransomware-incident-response-actions/ (accessed 22 June 2022).

Raver, C. M. (2019). *A ransomware attack could devastate your company. Will your insurance cover it?* Retrieved from https://www.natlawreview.com/article/ransomware-attack-could-devastate-your-company-will-your-insurance-cover-it (accessed 6 June 2020).

Rule, C. (2019). *The confidentiality of a client's tax return information.* Retrieved from https://www.cpajournal.com/2019/11/05/the-confidentiality-of-a-clients-tax-return-information/ (accessed 5 July 2020).

Ryle, P.M.; Al-wreikat, A.; Bartley, E.; McKnight, M.A. & Bueltel, B.L. (2022). Countering identity theft and strengthening data security practices across the tax preparer community. *The Contemporary Tax Journal*, 11(1), pp. 6 – 17. DOI: https://doi.org/10.31979/2381-3679.2022.110103

Ryle, P.M.; Jie, K.Y. & Gardiner, L. R. (2021). Gramm-Leach-Bliley gets a systems upgrade: What the FTC's proposed safeguards rule changes mean for small and medium American financial institutions. *The EDP Audit, Control, and Security Newsletter*, Retrieved from https://www.tandfonline.com/doi/abs/10.1080/07366981.2021.1911387 (accessed September 16, 2021).

SANS Security Awareness (2017). *Passwords.* Retrieved from https://www.sans.org/security-awareness-training/ouch-newsletter/2017/passphrases (accessed 7 June 2020).

Schlesinger, J. & Day, A. (2018). *Cybercriminals now targeting tax pros to cash in on fraudulent returns.* Retrieved from https://www.justice.gov/tax/stolen-identity-refund-fraud (accessed 7 June 2020).

Schultz, T. (2019) *The ROI of security awareness training.* Retrieved from https://www.infosecinstitute.com/blog/the-roi-of-security-awareness-training/ (accessed 5 July 2020).

Scott, J. & Spaniel, D. (2016). *The ICIT Ransomware Report.* Retrieved from https://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report.pdf (accessed 20 June 2022).

Sheridan, B. (2015). *Cyber liability: A growing concern for CPA firms.* Retrieved from https://www.macpa.org/cyber-liability-a-growing-concern-for-cpa-firms/#0 (accessed 7 June 2020).

Silhouette Creatives (2020). *Steps to Respond to a Ransomware Attack.* Retrieved from https://www.towerwatchtech.com/steps-to-respond-to-a-ransomware-attack/ (accessed 20 June 2022).

Solomon, H. (2020). *Toronto accounting firm hit by ransomware.* Retrieved from https://www.itworldcanada.com/article/toronto-accounting-firm-hit-by-ransomware/432049 (accessed 11 August 2020).

TechSolve. (2022). *Responding to Ransomware Attacks.* Retrieved from https://www.techsolve.org/responding-to-ransomware-attacks/ (accessed 22 June 2022).

Thakur, K. (2018). Test your cybersecurity knowledge. Retrieved from https://www.njcu.edu/about/blog/2018/08/final-exam (accessed 11 August 2020).

Truman, C. & Mercer-Myers, C. (2019). *How to respond to a ransomware attack.* Retrieved from https://www.cio.com/article/221850/how-to-respond-to-a-ransomware-attack.html (accessed 20 June 2022).

Violina, B. (2021). *How to Survive a Ransomware Attack.* Retrieved from https://www.cfo.com/technology/2021/10/how-to-survive-a-ransomware-attack/ (accessed 20 June 2022).

Walsh, I.; Holton, J. A.; Bailyn, L.; Fernandez, W.; Levina, N. & Glaser, B. (2015). What Grounded Theory is…a critically reflective conversation among scholars. *Organizational Research Methods,* 18(4), pp. 581-599.

Whitney, L. (2020). *Honeypot reveals tactics used by cybercriminals to deploy ransomware.* Retrieved from https://www.techrepublic.com/article/honeypot-reveals-tactics-used-by-cybercriminals-to-deploy-ransomware/ (accessed 4 July 2020).