FRAUD RISKS ASSOCIATED WITH REMOTE WORK ENVIRONMENTS AND ROLE OF FORENSIC ACCOUNTANTS

Research Project for Emerging Issues/Advanced Topics Course

Master of Forensic Accounting Program University of Toronto

Prepared by Sarah Dandia

June 19, 2022

For Prof. Leonard Brooks

Table of Contents

ACKNOWLEDGMENTS

The author wishes to acknowledge suggestions made by Erica Pimentel, PhD, CPA, Assistant Professor, Smith School of Business at Queen's University during the research for this report.

1.0 INTRODUCTION AND OBJECTIVES

When COVID 19 was declared a Global Pandemic in 2020, millions were instructed to work from home indefinitely. As reported by Statistics Canada, between April 2020 to June 2021, 30% of employees between the age of 15 to 64 who worked during the Labour Force Survey week had performed most of their hours from home. This change represented a significant increase in employees working from home compared to 2016, when only 4% of employees worked from home[1].

Organizations transitioning to remote work arrangements faced several challenges relating to infrastructure, adaptability, and productivity within a short period. Many organizations successfully innovated and adapted to these rapidly changing circumstances, but the changing landscape exposed these organizations to increased existing and novel fraud risks.

As businesses were investing in new technologies and systems that would accommodate work-from-home arrangements, they were left helpless to foster the security requirements, and fraudsters were quick to take advantage of the situation. According to PwC's Global Economic Crime and Fraud Survey report 2022, 46% of the surveyed organizations reported fraud or economic crime since the onset of Pandemic[2].

[1] Statistics Canada. (2021, August 4). Working from home during the COVID-19 pandemic, April 2020 to June 2021. Retrieved from https://www150.statcan.gc.ca/n1/daily-quotidien/210804/dq210804b-eng.htm

[2] PricewaterhouseCoopers. (2022). PwC's Global Economic Crime and Fraud survey 2022. Retrieved from https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

Remote work arrangements have caused employees to work in less secure home networks, giving rise to cyber frauds such as phishing attacks, ransomware and data and identity theft. Remote work has also instigated a shift in consumer behaviour, causing an increase in online buying and virtual transactions. TransUnion reported a 40 % increase in the use of online transactions in the first four months of 2021 compared to the last four months of 2020, during which fraud attempts against financial services companies increased by 218%[3].

While working from home was a temporary response to the Pandemic, this transition might be a permanent feature of the future work model. Several surveys over two years have suggested that remote work is to stay at least in some capacity. As we can see, with the Pandemic restrictions lifting, most organizations are adopting a hybrid work model, allowing employees to work remotely and in person.

While hybrid work models become the norm in society, businesses will need assistance from industry experts to combat the increase in fraud associated with remote work arrangements. For example, forensic experts will not only have to find preventative measures to reduce fraud caused by remote work but also recognize the advanced tools and techniques fraudsters apply to take advantage of organizational vulnerabilities. In addition, conducting remote investigations will require Investigators to learn new skills and techniques and be prepared to deal with the challenges of digitization needed for a remote workspace.

[3] TransUnion. (2021). Digital Fraud in 2021. Retrieved from https://www.transunion.ca/blog/fraud-trends-Q2-2021

My motivation for writing this report was to explore the evolving fraud risks associated with remote work and the challenges that IFA's might anticipate in the future under a remote work arrangement.

This research report will be divided into three sections: ·

- The first section will overview the emerging fraud risks associated with the shift to a remote work environment.
- The second section will focus on the challenges IFA's face in identifying and investigating fraud emerging from remote work environments. This section will also discuss how Forensic Investigators will assist organizations in mitigating the impact of fraud associated directly or indirectly with remote working.
- The third and last section will focus on the skills required by IFA's to conduct investigations remotely.

2.0 METHODOLOGY

The method adopted for writing this report was based on qualitative research and reading of articles, surveys, and information published by government agencies, including the Canadian Anti-Fraud Centre, Statistics Canada, and others, and analysis from professional websites such as CPA Canada and Association of Certified Fraud Examiners. Other sources include company reports, articles, and publications.
Finally, an Assistant Professor from Queen's University, whose recent work involves the impact of remote work arrangements on audit practices, was interviewed to understand if IFA's will be exposed to similar challenges as auditors in the face of technological disruptions. A copy of the questions provided to the interviewee in advance can be found in **Appendix B**.

The detailed list of specific documents reviewed and relied upon for purposes of preparing this report are outlined in the attached bibliography.

3.0 SCOPE LIMITATIONS

The research conducted to support this report has various limitations, which are discussed below:

The report has used various statistics to showcase the importance of discussed issues. Most of the statistics used in this report are based on surveys conducted in the U.S., some are based on surveys conducted in Canada, and a few are based on survey reports from other countries. Likely, fraud risks and the role of an IFA's in the remote workspace are different in various countries, which could present an opportunity for study for future research. In addition, most of the information relied upon to support the findings in this report is limited to two years of data. Remote work is a relatively new topic subject to ongoing debate since the onset of the Pandemic. Therefore, the trends observed in this report may change as further research is conducted in this area. Furthermore, this report is not meant to be a complete review of all the risks associated with the remote work environment but instead an opportunity to touch on some key fraud risks related to remote work and encourage IFA's to learn more about emerging fraud risks and remote investigation techniques.

4.0 BACKGROUND

4.1 The History of Remote Work

Remote work, also known as "teleworking"[4], is a working model that allows individuals to work at locations outside the traditional offices. Work-from-home arrangements have existed for hundreds of years, but it was not until recently that remote work became popular due to technological advances.

The 1950s- The world's first electronic digital computer inventions happened. These technological innovations lay the groundwork for the personal computer and the opportunity to work from home.

The 1970s – Before the days of Skype and Zoom calls, a NASA engineer named Jack Nilles laid the foundation for modern remote working when he coined the term "telecommuting" in 1973[5]. Soaring gasoline prices caused by the OPEC oil embargo made commuting more expensive. The work from home policies adopted in the 1970's allowed people to work from home or other locations such as libraries and coffee shops occasionally, expecting them to return to the office periodically. In 1979 five IBM employees were allowed to work from home. By 1983, the count rose to 2000[6].

[4] Reynolds.W.B, Bibby.A. The Complete History of Working From Home. Retrieved from https://www.flexjobs.com/blog/post/complete-history-of-working-from-home/

[5] Butler.H. The History of Remote Work: How It Became What We Know Today. Crossover. Retrieved from https://www.crossover.com/perspective/the-history-of-remote-work

[6] Ibid

2000's – The adoption of work from home increased in the 2000's due to the advance in personal computers, the Internet, email, broadband connectivity, laptops, cell phones, and cloud computing.

Pre-COVID – Working from home was already popular before Covid-19 was announced as a global Pandemic in March 2020. Before the Pandemic, many companies had allowed more employees to work from home, including prominent corporations such as Yahoo and IBM[7].

4.2 The Future of Remote Work

The outbreak of Covid-19 in November 2019 prompted many employers to shift to a working model that allowed employees to work remotely. Due to advancements in technology and the Internet, most companies successfully adapted to this new norm. As reflected earlier, remote work environments already existed before the Pandemic; however, the Pandemic worked as a catalyst encouraging a rapid and large-scale transition to remote work.

Organizations have recognized several benefits associated with remote work arrangements. According to Global Workplace Analytics nearly six out of ten[8] employers identified cost savings as a significant benefit to remote working. This report also indicates that over two-thirds of employers reported increased productivity among their employees when working remotely. An increase in productivity, reduced real estate costs,

[7] Choudhary. P. (2020). Our Work from Anywhere Future. Harvard Business Review. Retrieved from https://hbr.org/2020/11/our-work-from-anywhere-future

[8] Global Workplace Analytics. (2022). Cost and Benefits of Agile Work Startegies for Companies. Retrieved from https://globalworkplaceanalytics.com/resources/costs-benefits#toggle-id-4

flexibility, and the ability to maintain a work-life balance are benefits organizations will consider when adopting work from home as a permanent solution. Many tech giants have already made working from home a permanent solution. Twitter Inc. and PwC[9] are a few companies that are giving employees the option to work virtually forever.

According to a McKinsey survey in June 2020, 15% of executives surveyed amid the pandemic said at least one-tenth of their employees could work remotely two or more days a week going forward, almost double the 8% of respondents who expressed that intention before COVID-19[10].

An OECD survey reported that managers expect around 60% of their workforce to do more of their work from home. Relatedly, as of August 2020, about 60% of Canadian employers expected a portion of their workforce to perform some work from home after the Pandemic[11]. According to Statistics Canada, businesses expected to offer at least some of their employees the opportunity to telework when the COVID 19 pandemic is over in Canada increased from 34% to 59% between May and August 2020[12].

Employees have also benefited from this new workspace. Flexible work schedules, work-life balance, and fewer commuting hours are reasons employees would want to

[9] Ren.H. (2022, February 15). In 10 Years, 'Remote Work' Will Simply Be 'Work'. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2022-02-15/in-10-years-remote-work-will-simply-be-work

[10] Lund.S., Cheng.W., Dua.A., Smet.A.D., Robinson.O., Sanghvi.S. (2020, September 23). What 800 executives envision for the post pandemic workforce. Retrieved from https://www.mckinsey.com/featured-insights/future-of-work/what-800-executives-envision-for-the-postpandemic-workforce

[11] Mehdi.T, Morissette.R. (2021, October 27). Working from home in Canada: What have we learned so far? Retrieved from https://www150.statcan.gc.ca/n1/pub/36-28-0001/2021010/article/00001-eng.htm

[12] Statistics Canada. (2021, April 1). Study: Working from home: Productivity and preferences. Retrieved from https://www150.statcan.gc.ca/n1/daily-quotidien/210401/dq210401b-eng.htm

continue with this model permanently. The OECD survey also reported that 90%[13] of workers expressed a preference for doing more of their work from home in the future. Another report from Statistics Canada in 2021 indicated that 80% of new teleworkers would like to work at least half of their hours from home once the Pandemic is over and only 15% would prefer to work all of their hours from home after the Pandemic[14].

Employees consider working from home a perk; with the costs and time associated with commuting, employees are even willing to accept jobs with lower pay if offered the option to work from home. For example, in a survey conducted by the National Bureau of Research, respondents are willing to accept pay cuts of 7 percent[15], on average, if given the option to work from home a few days per week after the Pandemic.

Just within a few months of the Pandemic, many employees started quitting their jobs, awakening to their strong bargaining power. According to the U.S. Bureau of Labour Statistics, 4.5 million employees quit their jobs in November 2021[16]. Employees are realizing several benefits associated with remote work, and several studies conducted over the past two years suggest that employees would not want to work in an office full-time. If employers do not evolve with the needs of their employees, they risk losing their

[13] Ibid

[14] Statistics Canada. (2021, April 1). Study: Working from home: Productivity and preferences. Retrieved from https://www150.statcan.gc.ca/n1/daily-quotidien/210401/dq210401b-eng.htm

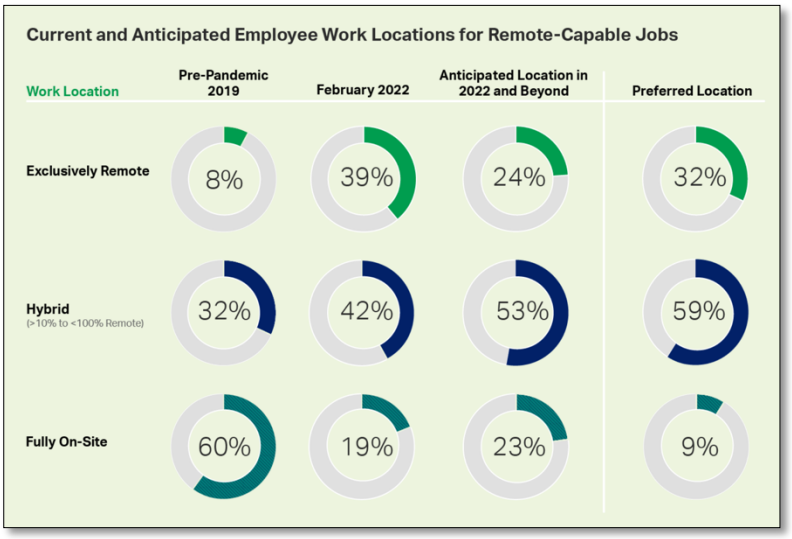
[15] Barrero,J., N.Bloom and S.Davis (2020),Why Working From Home Will Stick http://dx.doi.org/10.2139/ssrn.3741644

[16] U.S. Bureau of Labor Statistics. (2022, January 6). Number of quits at all-time high in November 2021. Retrieved from https://www.bls.gov/opub/ted/2022/number-of-quits-at-all-time-high-in-november-2021.htm

staff during the era of "Great Resignation"[17]. Therefore, most organizations are adjusting their practices to accommodate the changing needs of their employees, adopting a hybrid model that allows employees to split time between the office and home.

A survey conducted by Gallup indicated that 53% employees are expected to work in a hybrid work environment post Pandemic.18.

Figure 1 – Current and Anticipated Employee Work Locations for Remote-Capable Jobs



Source: Gallup Workplace, March 15, 2022. The Future of Hybrid Work: 5 Key Questions Answered with Data

These results were also illustrated in PwC's Remote work survey, which indicated that 68% of executives believe that people should be in the office at least three days a week and would not be returning to their Pre-Pandemic work model[19].

[17] Fontinelle. A. (2022, May 5). The Great Resignation. Retrieved from https://www.investopedia.com/the-great-resignation-5199074

[18] Wigert.B. (2022. March 15). The Future of Hybrid Work: 5 Key Questions Answered With Data. Retrieved from https://www.gallup.com/workplace/390632/future-hybrid-work-key-questions-answered-data.aspx

[19] PwC. (2021, January 12). PwC's Remote Work Survey 2021. Retrieved from https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

Although the hybrid working model has many advantages, the increased reliance on digital platforms arising from this model will pose new security threats to organizations, increasing the risk of existing frauds and giving rise to novel forms of fraud.

4.3 Remote Work and Fraud

The Pandemic has changed the way businesses operate. The two factors that significantly contribute to the increasing fraud risks are changes in business operations (including allowing employees to work remotely) and changes in consumer behaviour (Shift to virtual/retail transactions, online buying).

When COVID-19 was announced as a global Pandemic in 2020, work from home increased substantially in Canada and many other industrialized countries. This changing landscape required businesses to implement new internal controls, policies, and processes. Unfortunately, businesses were unprepared to deal with the technological challenges of these reformations and soon became the target of fraud perpetration.

According to PwC's Global Economic Crime and Fraud Survey report 2022, 46% of the surveyed organizations reported fraud or economic crime in the last 24 months[20]. In another survey conducted by ACFE in collaboration with Grant Thornton in 2020, 51% of organizations uncovered more fraud since the onset of the Pandemic[21].

[20] PricewaterhouseCoopers. (2022). Global Economic Crime and Fraud Survey. Retrieved from https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC%E2%80%99s-Global-Economic-Crime-and-Fraud-Survey-2022.pdf

[21] Association of Certified Fraud Examiners., Grant Thornton. (2020). Strengthen your fraud defenses. Preparing for the post-pandemic fraud landscape. Retrieved from https://www.grantthornton.ca/insights/strengthen-your-fraud-defenses/

Fraud patterns are also evolving; the new environment has created new opportunities for internal and external parties to perpetrate fraud against the organization. For example, Ravelin's Online Merchant Fraud and Payments survey has confirmed new forms of fraud emerging post-COVID. According to the study, 62% of respondents reported emerging new fraud types[22]. Of course, remote work may not be the only cause of these unknown fraud risks. Still, cloud computing and weak security networks are some of the factors associated with remote work contributing to the evolving fraud risks.

Digitization has required companies to hold all relevant and critical information online, which has allowed employees to work remotely but also provides an opportunity for fraudsters to gain access to all necessary information of the organization. Once access is achieved, the data can be used to either directly steal significant funds from the company or indirectly through impersonation or other acts. In addition, technological advancements have caused fraud attacks to become increasingly complex over time, and fraudsters identify creative methods to achieve the most effective results with less effort and investment. Most fraudsters aim to achieve higher financial gains while targeting fewer individuals/organizations. A benchmark data report from ACI worldwide indicated that the average transaction value of attempted fraud increased by 4.7%, while overall occurrences decreased by 3.2%[23].

[22] Ravelin. (2022). Online Merchant Perspectives. Fraud And Payments Survey. Retrieved from https://www.ravelin.com/blog/online-merchant-perspectives-fraud-payments-survey-2022

[23] ACI Worlwide. (2021, February). Pandemic – Driven Patterns of eCommerce Fraud. Retrieved from https://www.aciworldwide.com/wp-content/uploads/2021/04/pandemic-driven-patterns-of-ecommerce-fraud-article.pdf

The Canadian Anti-fraud Center also observed similar results; as of August 31, the Canadian Anti-Fraud Centre reported the impact of fraud in 2021 at $144 million lost, up from $106 million in 2020. However, the number of victims dropped to 36,334 from 42,182[24] (fewer victims with higher returns). As per the Canadian Anti-fraud Center, the total amount lost to fraud in the first three months of 2022 has been reported to be $125M.

Figure 2 – The Impact of Fraud so far this year

Source: Canadian Anti-Fraud Centre, March 15, 2022. The impact of fraud so far this year

The remote work setting has allowed fraudsters to perpetrate fraud schemes that are low in risk but provide higher pay-outs. For example, cyber fraud involves sophisticated attacks and high returns with minimal risk of being caught. Similar online fraud schemes are expected to increase with the rise in virtual activity. According to the ACFE Global

[24] Canadian Anti Fraud Centre. (2022). The Impact of Fraud so Far this Year. https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

Survey report 2020, some of the fraud risks expected to increase post-pandemic are cyberfraud, social engineering, data theft, identity crime, payments fraud, fraud by vendors or sellers, and others[25].

The Pandemic has opened a new landscape for fraud; remote employees allow hackers to access the organization's crucial information through their unsafe home networks. If organizations do not take prompt action and measures, fraudsters can take advantage of operational weaknesses and misappropriate the Company's assets leading to significant losses.

4.4 Internal Controls and Fraud Risks

Internal controls are policies and procedures implemented by an organization to ensure adequate financial reporting, safeguard company assets, ensure compliance with rules and regulations and protect the organization from fraud.

Poor internal controls can lead to severe consequences for organizations, including loss of company assets and damage to reputation. Internal controls currently implemented by organizations are not designed to detect and prevent fraud in a full-time virtual environment. When a new control is implemented and not tested for efficiency, it may allow fraudsters to override the control and defraud the organization. Shift to a remote work environment has changed the way businesses operate; these changes have required management to design and implement new controls to accommodate the new work environment. Since most organizations were rushed to implement new controls, they

[25] Association of Fraud Examiners. (2020). The Report to The Nations. Global Study on Occupation Fraud and Abuse. Retrieved from https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf

were not given the due time needed to test the effectiveness and security of the updated controls and processes, leaving the organization exposed to increased fraud risks. As per the ACFE 2022 report to the nation, nearly half of the cases reported were likely due to either lack of internal controls (29%) or due to override of existing controls (20%)[26].

The shift to remote work has set a new challenge for management to design controls that will allow the organization to operate remotely; specifically, digital approvals have increased the risk of fraud which needs to be mitigated by organizations. These new controls have not only increased the risk of existing fraud schemes but have also introduced the opportunity for fraudsters to perpetrate new fraud schemes. Some internal control challenges faced by organizations will include:

- Employees can manipulate supporting documents used to prepare financial statements digitally.
- Difficulty in maintaining segregation of duties, employees can work in collusion.
- Lack of in-person interaction with senior leadership makes it difficult to maintain ethical standards.
- Key approvers working from home may not show the same level of diligence in reviewing documents as they would if they were in the office.
- Employees may be working in shared accommodation where others can access and view sensitive data.
- Employees may have or adopt irresponsible social media use habits[27].

[26] Association of Fraud Examiners. (2022). Occupational Fraud 2022. Retrieved from https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

[27] Perachio.G, Sexton.R. (2020, June 12). COVID-19 implications: internal fraud. Retrieved from https://www.ey.com/en_uk/disrupting-financial-crime/financial-crime/covid-19-implications-internal-fraud

4.5 Industries Most Affected by Fraud

Banking, public sector, and manufacturing are some of the industries that were the most successful in transitioning to remote work. According to a recent survey by Crowe 56% of the banking industry's respondents rated their transition to remote work as excellent, followed by 53% of public sector respondents and 37% by manufacturing and distribution[28]. Most of the employees in these industries are considered to be knowledge workers who can work independently and perform a significant amount of their work without being at the office. For example, most employees working in the banking sector are staff who work behind their computers and most likely have laptops available for remote work. In addition, the administrative staff of the public sector and manufacturing industry could also shift off-site, making it convenient for businesses in these industries to move their knowledge workers to remote work. In addition, online communication channels, online banking, cloud computing, e-commerce, and online customer service are some factors that have made the transition into remote working for these industries relatively easy.

Some of these industries experienced an increase in fraud more than others due to their massive and quick shift to a virtual presence. While having an online presence has many benefits such as flexibility, efficiencies and cost-savings, there are also inherent fraud risks and cybersecurity concerns due to technological deficiencies. According to the 2021

[28] Walk-Morris.T. (2020, August 27). These Industries Are Thriving With A Remote Workforce. Forbes. Retrieved from https://www.forbes.com/sites/crowe/2020/08/27/these-industries-are-thriving-with-a-remote-workforce/?sh=120e2cfe6587

Global Threat Intelligence Report, attacks against manufacturing increased from 7% last year to 22%, healthcare increased from 7% to 17%, and finance is up from 15% to 23%. Attackers continue to focus on these industries, with the combined percentage of attacks against the top three targeted industries being 62% in 2020.

Figure 3 – Percent of attacks against the top three industries in 2018, 2019 and 2020

	2018	2019	2020
Percent of attacks focusing on the top three industries	46%	51%	62%

Source: NTT, 2021 Global Threat Intelligence Report

Finance emerged as the most attacked industry, on the strength of a 50% increase in attack volume. Manufacturing jumped from the fifth most targeted in 2019 to the second most targeted in 2020[29].

As a result of the COVID -19 Pandemic, many consumers have shifted to the use of digital financial services. In a TransUnion-commissioned late September 2020 survey, 40% of consumers with financial accounts were reported to use digital platforms more frequently since the onset of the Pandemic, and 60% of consumers said the majority of their financial transactions are conducted through mobile applications[30]. Increased mobile banking usage has also contributed to more attacks, studies of U.S. financial data indicate

[29] IBM Security. (2022). X-Force Threat Intelligence Index. Retrieved from https://www.key4biz.it/wp-content/uploads/2021/05/2021-Global-Threat-Intelligence-Report-full-report.pdf

[30] Transunion. (2021, June 3). Suspected Financial Services Digital Fraud Attempts Rise Nearly 150% Worldwide As Prevalence of Digital Transactions Increase. Retrieved from https://www.transunion.ca/blog/fraud-trends-Q2-2021

a 50 percent surge in mobile banking since 2020. In addition, studies indicate that 36 percent of Americans plan to use mobile tools to conduct banking activities, and 20 percent plan to visit branch locations less often. As the public increases its use of mobile banking apps, partially due to increased time at home, the FBI anticipates cyber actors will exploit these platforms[31].

Shifting to remote work has intensified the phishing threat level for financial service providers. IBM's report notes that the average total cost of a data breach in the financial services sector in 2020 was $5.85 million[32]. Considerable data breaches often lead to harmful media exposure, hurting brand reputation, and eventually leading to customers' loss of trust and confidence. Other factors include legal fees, insurance premiums, ransomware payments, and crisis management costs.

Government sector has seen a significant increase in data breaches. These attacks are on government databases to obtain strategic information. for example, Russian hackers breached US defense contractors and stole military and communication infrastructure data from 2020–2022[33].

Manufacturing ranked as the second most-attacked industry in 2020, up from eighth place in 2019 and retail ranked as the fourth most attacked[34]. With the growing use of

[31] Federal Bureau of Investigation. (2020. June 10). Increased Use of Mobile Banking Apps Could Lead to Exploitation. Retrieved from Internet Crime Complaint Center (IC3) | Increased Use of Mobile Banking Apps Could Lead to Exploitation

[32] IBM Security. (2021). Cost of a Data Breach Report 2021. Retrieved from https://www.ibm.com/downloads/cas/ADLMYLAZ

[33] Ekran. (2022, May 5). 5 Industries Most at Risk of Data Breaches. Retrieved from https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches

[34] Ibid

smartphones and mobile devices and internet services, e-commerce has emerged as a major shopping platform in the world. Fraudsters have taken notice of this transformation and are using complex techniques to take advantage of security vulnerabilities embedded within these industries. 83% of top 30 US retailers have online vulnerabilities, posing cybersecurity threats, including retailers such as Amazon, Walmart and Costco[35].

Some industries are more susceptible to fraud than others due to employees having direct access to the organization's assets. For example, financial institutions provide employees with direct access to cash. Therefore, when employee banking credentials are hacked, the hacker has direct access to the assets associated with the business. For example, the Accounts Payable (AP), authorized to process payments for the business, may have confidential banking details of the Company stored on their computer. If the AP supervisor has weak security networks, it would be convenient for the fraudster to perpetrate phishing or malware attacks against the user and obtain access to the Company's banking details. The same applies in the manufacturing industry. For example, employees working at warehouses have direct access to inventory; with most employees working remotely, there is less security and oversight over such individuals, which provides them with an opportunity to misappropriate Company's assets.

[35] Security. (2020, December 10). 83% of top US retailers have online vulnerabilities, posing cybersecurity threats. Retrieved from https://www.securitymagazine.com/articles/94137-of-top-30-us-retailers-have-online-vulnerabilities-posing-cybersecurity-threats

5.0 DETAILED FINDINGS AND ANALYSIS

The "Fraud Triangle" developed by criminologist Donald R. Cressey is a visualization of the three conditions that must co-exist for the perpetration of fraud: (a) Pressure, (b) opportunity, and (c) the ability to rationalize or justify wrongful actions[36].

Changes in business operations and processes during COVID shaped a landscape that contained all three elements of fraud: tremendous pressure to maintain break-even earnings, rationalization of behaviors such as enhanced risk-taking and unethical decision making, and significant changes in internal controls providing opportunities to commit fraud. In addition, the shift to a remote work environment was an essential factor that created a gap in the Company's internal control structure. Since fraudsters are always looking for ways to take advantage of difficult situations, this new landscape presented them with the perfect platform to perpetrate fraud.

Although many organizations have reported a significant increase in fraud risks during COVID, remote work cannot be considered the only cause of this increase. For example, the Government offered relief fraud schemes, and supply chain disruption fraud are a few of the schemes that were unique to the COVID 19 crisis and unrelated to remote working. In the ACFE report to the nations, survey respondents cited shift to remote work as a significant factor that contributed to the fraud cases investigated (a contributing factor in 32% of the cases) However, 62%[37] of the fraud cases were unrelated to remote working.

[36] Whistleblower Info Center. (2021, June 23). What is the Fraud Triangle?. Retrieved from https://whistleblowerinfocenter.com/resources/blog/what-is-the-fraud-triangle/

[37] Association of Fraud Examiners. (2022). Occupational Fraud 2022. Retrieved from https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

However, suppose organizations continue to support hybrid work models, allowing employees to continue working remotely in some capacity. In that case, some of the fraud risks that emerged during the Pandemic will continue to exist and evolve over the years.

6.0 FRAUD RISKS ASSOCIATED WITH REMOTE WORK ENVIRONMENT

6.1 Policy Abuse Fraud

Policy abuse fraud is a scheme that surged post-COVID and has presented significant challenges to e-commerce businesses. Policy abuse fraud is when customers take unfair advantage of business policies for personal gain. Promotion abuse fraud, return abuse fraud and items not received fraud are a few of the policy abuse frauds that have surfaced in the past few years.

Promo Abuse and Refund Abuse

Promo abuse is taking advantage of the Company's sign-up bonuses, referral bonuses, discount codes and vouchers. Fraudsters take advantage of sign-up bonuses and referrals by creating multiple accounts. Refund abuse occurs when the excessive use of the company’s return policy becomes unprofitable to the Company.

Recent Statistics on Promo Abuse and Refund Abuse Fraud

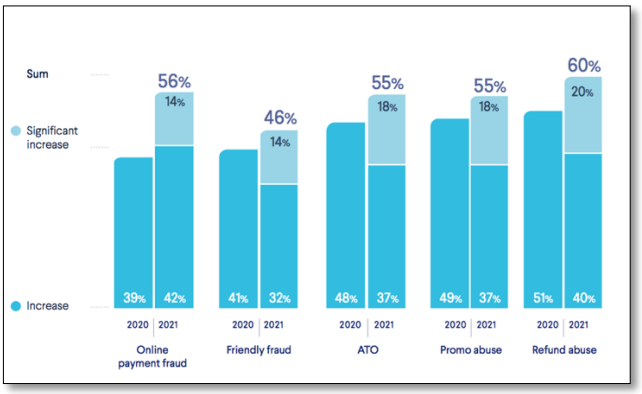
According to the Online Merchant Fraud and Payments survey conducted by Ravelin, 49% of e-commerce businesses have experienced a rise in promo abuse, and 51% have experienced a rise in refund abuse since mid-2020. This survey was carried out using a

panel of 1700 global fraud professionals[38]. PYMNTS' research reveals that policy abuse costs retailers with more than $100 million in revenue in the United States as much as $89 billion per year[39].

A similar survey was conducted in September 2021 as a collaboration between PYMNTS and Forter; according to the survey, PYMNTS finds that 73 percent of eCommerce companies have experienced promotion abuse over the past 12 months, making it the most common type of known customer fraud. This fraud was followed by INR abuse (50 percent) and return abuse (44 percent)[40]

Merchant fraud has been rising due to the digitization of businesses and the rapid shift to e-commerce. In the survey conducted by Ravelin, it was reported that online payment fraud and promotion and refund abuse were the top two frauds observed post-COVID[41].

Figure 4 – Increase in Fraud Activity



Source: Ravelin, 2022 Online Merchant Perspectives, Fraud & Payments Survey 2022

[38] Ravelin. (2022). Online Merchant Perspectives. Fraud And Payments Survey. Retrieved from https://www.ravelin.com/blog/online-merchant-perspectives-fraud-payments-survey-2022

[39] PYMNTS Beyond eCommerce Fraud. (2021. November). How Retailers Can Prevent Customer Policy Abuse. Retrieved from https://www.thehive-network.com/wp-content/uploads/2021/12/PYMNTS-Beyond-eCommerce-Fraud-November-2021.pdf

[40] Ibid

[41] Ibid

Mairtin O'Riada, Chief Intelligence Officer at Ravelin[42], when asked about Promo abuse and refund abuse fraud, states

> "One way we've seen promo abuse happening a lot is through the creation of multiple accounts, so a customer repeatedly receives a free trial. Multi-accounting ranges from something as basic as a customer logging out of one account and signing into another, to fraudsters creating fresh I.P. addresses or synthetic I.D.s. We've also seen promotion abuse evolve into more organized reselling schemes, where fraudsters take advantage of product promos to amass merchandise to sell at a higher price. Where refund abuse is concerned, we've noticed a considerable rise in the trend of 'wardrobing,' where someone orders an item of clothing, wears it once to take pictures for social media, and then returns the item. Merchants have a tricky balance to strike here, though. Make returns policies lenient, and this kind of thing may keep happening. But making return policies stricter might scare off customers, as 83% of shoppers will only buy from platforms with return policies they like."

Shift to online channels has made it convenient and less time-consuming for customers engage in online purchasing. GWI found that 46% of people surveyed in 2020 believe that they will be doing more online shopping even after the pandemic ends[43]. With the

[42] Ibid

[43] Smulders.S. (2021, August 4). How the Pandemic has changed the online sales Landscape. Retrieved from https://www.forbes.com/sites/forbesbusinesscouncil/2021/08/04/how-the-pandemic-has-changed-the-online-sales-landscape/?sh=3074b1718362

convenience of online buying, consumers may continue taking advantage of product promotions and refunds.

As Scott Buchanan, chief marketing officer at Forter pointed out during an interview with FashionUnited at NRF Big Show[44]:

> "Policy abuses are increasing, partly because that pandemic has us all shop more from the comforts of home," According to Scott Buchanan Policy abuse fraud and account takeover will continue to rise in 2022.

Recent Events on Policy Abuse

Students in the U.K. stung Amazon for hundreds of thousands of pounds after discovering a glitch that meant a one-off discount code to be used repeatedly. The promo code was designed as a one-time introductory offer to attract customers; however, some students soon realized a glitch in the system. The code was re-usable, allowing them to make purchases worth thousands of pounds for nothing[45].

To take advantage of Uber's referral promotion, an individual was caught posting his uber code on the reddit site to gain referrals. The specific individual was able to obtain 2,500 or so referrals from reddit, and by signing up so many people he was able to secure $50,000 in credit[46].

---

[44] Rodriguez.G.A. (2022. January 29). From policy abuse to friendly fraud: Retailers face billions in revenue loss. Retrieved from https://fashionunited.com/news/business/from-policy-abuse-to-friendly-fraud-retailers-face-billions-in-revenue-loss/2022012945450

[45] Roberts.J. (2019. October 27). Broke students cash in after discovering 'Amazon coucher glitch'. Retrieved from https://metro.co.uk/2019/10/27/broke-students-cash-discovering-amazon-voucher-glitch-10993142/

[46] Kosoff.M. (2015. January 5). How one 24-year old got $50,000 in Free Uber Rides By Duping Uber's Promo-Code System. Retrieved from https://www.businessinsider.in/tech/How-One-24-Year-Old-Got-50000-In-Free-Uber-Rides-By-Duping-Ubers-Promo-Code-System/articleshow/45767241.cms

Promotions and return policies are important tools businesses use to attract and retain customers and differentiate themselves from competitors. However, Policy abuse fraudsters have become increasingly savvy and are developing new methods and techniques to deceive retail businesses and take advantage of these policies. In addition, policy abuse frauds are complex and more difficult to measure, assess and control. This complexity will present an ongoing challenge for retailers as more and more consumers are shifting to online buying as the primary channel.

6.2 Cybercrime

Cyber fraud is considered a crime or fraud carried out online, using a digital platform, mobile application, or network of computer systems. In an interview with INSIDER, billionaire businessman and philanthropist Warren Buffet calls "cybercrime the number one problem with mankind and cyberattacks a bigger threat to humanity than nuclear weapons"[47].

Recent Statistics on Cybercrime

According to a survey report from Ponemon Institute in 2020, seventy-one percent[48] of respondents surveyed were concerned that remote workers are putting the organization at risk for a data breach. To deal with the Government imposed restrictions, employees shifted to remote work, which meant that employees often used their personal devices for work purposes. Employees, when working from home, are also accessing customer data

[47] Oyedele.A. (2017. May 6). Buffet: This is 'the number one problem with mankind'. Retrieved from https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5

[48] Ponemon Institute. (2020). Cybersecurity in the Remote Work Era. Retrieved from https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf

and confidential financial information of the Company through their home networks. The work-provided device is not the only device connected to that network; according to a study by Forrester, remote workers have an average of eight devices[49] connecting to their home network. Due to a lack of visibility over home networks and connected devices, the company data is exposed to a high risk of cyber-attacks. As per Check Point Software's 2022 Security Report, cyber-attacks against organizations worldwide increased by an average of 50% in 2021, compared to 2020[50], suggesting that cyber attackers are taking advantage of the world's sudden and increased shift to the virtual mode of work.

According to Statistics Canada just over one-third (36%) of those reporting at least one cyber security incident experienced a loss due to the incident. Among those who experienced a loss, the most common was a loss of time (87%), followed by loss of data (13%) or financial loss (13%)[51]. Information loss and business disruption caused by these attacks can lead to significant costs for businesses. Cybersecurity Ventures say cyber fraud or Internet fraud has already reached $ 6 trillion in global damage in 2021. This figure is projected to rise to $ 10.5 trillion annually by 2025[52].

Cybercrime has always existed, but the massive shift to remote work has exposed sensitive business information to security vulnerabilities. In addition, remote work and

[49] Forrester. (2021). Beyond Boundaries: The Future of Cybersecurity in the World of Work. Retrieved from https://static.tenable.com/marketing/whitepapers/Forrester-Beyond_Boundaries_The_Future_of_Cybersecurity_in_the_New_World_Of_Work.pdf

[50] Check Point. (2022). Security report: Global Cyber Pandemic's Magnitude Revealed. Retrieved from https://www.checkpoint.com/press/2022/check-point-softwares-2022-security-report-global-cyber-pandemics-magnitude-revealed/

[51] Statistics Canada. (2020. October 14). Canadians spend more money and time online during pandemic and over two-fifths report a cyber incident. Retrieved from https://www150.statcan.gc.ca/n1/en/daily-quotidien/201014/dq201014a-eng.pdf?st=O3x9Cw1x

[52] Calif.S. (2020. November 13). Cybercrime to Cost the World $10.5 Trillion Annually By 2025. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

business transactions have caused an increase in the enactment of complex cybercrimes such as social engineering, phishing attacks, and ransomware attacks. Sensitive business information has become exposed to security vulnerabilities which have caused a rise in these crimes. According to a Global Risk Report by Ponemon institute sixty percent[53] of respondents say their organizations experienced a cyberattack, the most frequent attacks involved credential theft (56 percent of respondents) and phishing/social engineering (48 percent of respondents). According to the 2021 data breach report by Identity Theft Resource Center, Phishing, ransomware and malware were the top three cyberattacks reported in 2020 and 2021.

Figure 5 – Attack Vector Trends

ATTACK VECTOR TRENDS	2021	2020	2019
Cyberattacks	**1,613**	**878**	**928**
Phishing/Smishing/BEC	537	383	490
Ransomware	321	158	83
Malware	139	104	112
Non-secured Cloud Environment	23	51	15
Credential Stuffing	14	17	3
Unpatched software flaw	4	3	3
Zero Day Attack	4	1	n/a
Other - not specified	436	161	222
NA	106	n/a	n/a
Human & System Errors	**179**	**152**	**231**
Failure to configure cloud security	54	57	56
Correspondence (email/letter)	66	55	89
Misconfigured firewall	13	4	4
Lost device or document	12	5	19
Other - not specified	34	31	63
Physical Attacks	**51**	**78**	**118**
Document Theft	9	15	19
Device Theft	17	30	57
Improper Disposal	5	11	14
Skimming Device	1	5	4
Other - not specified	19	17	24
Unknown	**12**	**n/a**	**2**

Source: Identity Theft Resource Center, 2021 Data Breach Annual Report[54]

[53] Ibid

[54] Identity Theft Resource Center. (2021). Annual Data Breach Report. Retrieved from https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/

Since the start of the internet age, cybercrime attacks have grown considerably. In the past few years, an increase in online activity and a vast shift toward working from home have enabled many more opportunities for a criminal to launch cyber-attacks. With advanced tools and technologies, these attacks have become more sophisticated. Artificial Intelligence, machine learning and blockchain technologies are being used by cybercriminals to speed up attacks, resulting in cyber-attacks becoming impactful and far more invasive. In addition, the shift to remote employment has resulted in employees working from home using insecure personal phones and computers. These operational changes pose security risks to businesses, and cyber criminals constantly look to exploit these organizational vulnerabilities for personal gain. Identity theft, phishing attacks, and ransomware are some of the most common cybercrime attacks that have become increasingly popular in the past few years.

6.3 Identity Theft

Identity theft is the act of fraudulently obtaining another person's personal or financial information to use their identity for financial gains, such as making unauthorized transactions or purchases.

Fraudsters are taking advantage of the recent increase in remote work arrangements by impersonating legitimate business correspondence. Fraudsters pose as coworkers or authorized officials of the organizations, emailing employees using a fake email account or an official-looking business account. The email may include a link by clicking on which the employee will give access to fraudsters' business credentials, allowing them to open lines of credit and file an illegal tax return.

Personal devices are often used for work purposes, and since many individuals have insecure settings, these devices are more likely than business devices to encounter hacking attacks.

Recent Statistics on Identity Theft

With the increase in online transactions, it has become convenient for hackers to access personal or business banking information. Fraudsters can use this information to rack up millions from the victim while the loss remains unknown to the victim for months. According to a 2021 research report from Javelin, the average financial loss associated with identity theft is more than $13 billion[55].

According to a US-based Identity Theft Resource Center (ITRC) report, the first three quarters of 2021 there was a 17% increase in the number of businesses experiencing data breaches. These breaches are one of the prime sources of identity theft[56].Overall, FTC complaints jumped 46% from 2019 to 2020 and identity theft was reported to be the main reason for FTC complaints, accounting for 29.39% of all cases[57]. In addition, Transunion Canada reported a rise in digital I.D. fraud attempts by 218% since the outbreak of the COVID-19 Pandemic[58].

[55] Javelin (2021). 2021 Identity Fraud Study. Shifting Angles. Retrieved from https://javelinstrategy.com/content/2021-identity-fraud-report-shifting-angles-identity-fraud

[56] Identity Theft Resource Center. (2021). Annual Data Breach Report. Retrieved from https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/

[57] Federal Trade Commission. (2022, February 22). New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021. Retrieved from https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0

[58] Transunion. Financial Services Digital Fraud Attempts in Canada Rise 218%. Retrieved from https://www.transunion.ca/blog/fraud-trends-Q2-2021

Financial identity theft is a common type of identity theft, where the fraudster uses the victim's identity to obtain credit, loan, services or other financial benefits. Other sources also indicate that identity thefts have increased sharply, both globally and in the U.S. specifically. For example, according to figures released by the Aite Group, 47% of U.S. citizens experienced financial identity theft in 2021[59].

Credit Card Fraud

Credit card fraud is a form of identity theft in which an individual acquires someone else's credit card details and uses that information to make unauthorized purchases or borrow money without the intent to repay it.

Recent Statistics on Credit Card Fraud

Corporate credit cards are issued to employees to pay for authorized business expenses. Due to the recent shift to WFH (Work From Home), employees spend a significant amount of time at home and conduct most of their financial transactions, whether work or personal related, through their home networks. As a result, individuals may disclose personal or credit card information without verifying the source, providing a gateway for hackers to download malware in the system and obtain credit card information. Account takeovers are a standard method used by cyber attackers, in which the attacker first changes the victim's address on file. Subsequently, reports the card stolen to obtain a new card and make fraudulent purchases. The 2022 IBM Global Financial Impact report has found that consumers have moved exclusively to credit card and digital payments, costing

[59] Giact. (2021, March). U.S. Identity Theft: The Stark Reality. Retrieved from https://giact.com/identity/us-identity-theft-the-stark-reality-report/

American consumers $265 per year in fraudulent financial charges made by unauthorized third parties[60].

IBM studied data breaches in more than 500 companies worldwide, including 26 based in Canada, between May 2020 and March 2021 and found Canada ranking in the global top three for data breach costs, with the average incident costing around $6.75 million. The most common method behind data breaches was stolen credentials, accounting for 20 percent of attacks[61]. Additionally, electronic databases containing credit cards may be hacked, releasing customers' credit card information, and putting the security of many accounts at risk. Stolen credit card information can lead to loss of consumer confidence, damage to reputation, financial costs, legal costs, and other severe consequences for the organization.

The company-issued credit cards are also at the risk of being used for unauthorized purposes. For example, to accommodate WFH, many organizations updated their expense policies, where expenses such as basic office supplies, utilities, and office furniture are permitted to make the home office comfortable. Unfortunately, as a result, many employees may take advantage of these amended policies and swipe employer-provided credit cards for expenses not considered necessary.

Identity theft and credit card fraud has existed before COVID-19 but has become prevalent in recent years due to the rapid shift to digitization. Individuals are spending

[60] IBM. (2022, February). 2022 IBM Global Financial Fraud Impact Report. Retrieved from https://filecache.mediaroom.com/mr5mr_ibmnewsroom/193031/MC%20%2B%20IBM%20Financial%20Fraud%20Study%20-%20Global%20Report%20Updated%203.8.22.pdf

[61] Ibid

most of their time online whether it is through mobile phones or their computers, tasks that were once conducted in person are now being conducted online through the internet. An increase in online facilities such as online shopping, online banking, and work from home has exposed individuals to identity fraud. Identity thieves may hack the devices used for conducting online activities, for example many individuals engage in online banking through their mobile phones, making it very convenient for the identity thief to hack the device and steal the individual's personal credentials – bank account number, name, date of birth. The hacker can use this information to either create a new account, or transfer funds from existing account or borrow large amounts of money. Once data, including personal, banking and other private information, has been wrongfully accessed, the fraudster can exploit this information and cause significant losses to the individual or organization.

6.4 Phishing

Phishing is a cyberattack in which the fraudster impersonates as a legitimate representative of an authentic institute and uses phone, email or text to entice the victim into providing personal or confidential information including passwords, credit card information, and social security numbers. This information is then used to access accounts or systems, often leading to identity theft or significant financial loss.

The most common type of data being compromised in a Phishing attack is:

- Credentials (Passwords, Usernames, etc.)
- Personal (Banking Information, Social security number, Name, Date of Birth)

2021 Tessian research found Microsoft, ADP, Amazon, Adobe Sign and Zoom as some of the most commonly impersonated brands in phishing attacks[62]. Similarly, IBM's X-Force Threat Intelligence Index 2022 report revealed that the most phished brands in 2021 were Microsoft, Apple, and Google[63].

Recent Statistics on Phishing Attacks

As per Statistics Canada, on October 14, 2020, just over 4 in 10 Canadians (42%) experienced at least one type of cyber security incident since the Pandemic, including phishing attacks, malware, fraud and hacked accounts[64]. Moreover, in 2021, research from IBM confirmed this trend, citing a two-percentage-point rise in phishing attacks between 2019 and 2020, partly driven by COVID-19 and supply chain uncertainty[65].

Organizations have shifted to online platforms for purposes of work communication more than ever. Email and text messages have become the primary modes of communication due to the lack of in person interactions under remote work. This drastic shift has left individuals and businesses more vulnerable than ever to a wide variety of cyberthreats. Fraudsters have been taking advantage of the increased use of email and text messages, hackers impersonate as an authorized official of the organization and send emails to employees with the intention to obtain employees credentials. Some of the common

[62] IT Security News. (2022. March 4). The most impersonated brands in phishing attacks. Retrieved from https://www.itsecuritynews.info/the-most-impersonated-brands-in-phishing-attacks/

[63] IBM Security. (2022). X-Force Threat Intelligence Index 2022. Retrieved from https://www.ibm.com/downloads/cas/ADLMYLAZ

[64] Statistics Canada. (2020. October 14). Canadians spend more money and time online during pandemic and over two-fifths report a cyber incident. Retrieved from https://www150.statcan.gc.ca/n1/en/daily-quotidien/201014/dq201014a-eng.pdf?st=O3x9Cw1x

[65] Rosenthal.M. (2022, January 12). Must-know Phishing Statistics: Updated 2022. Retrieved from https://www.tessian.com/blog/phishing-statistics-2020/

subject lines used that can entice employees to fall victim to these emails include "password check required immediately", "Reminder: Important Security Upgrade Required" and "Remote Work Policy Update". A common technique used by fraudsters is email phishing attacks, in which an email is sent to the user informing them that there has been a compromise to their account and requires them to respond immediately by clicking on a provided link. CISCO's 2021 Cybersecurity threat trends report suggests that at least one person clicked a phishing link in around 86%[66] of organizations. Clicking on a phishing link will lead to the system being infected by viruses including malware and spyware. Once these viruses are installed, the fraudster can easily extract the users sensitive and confidential information.

Just over one-third of respondents (34%) received phishing attacks since the start of the Pandemic, a specific type of spam targeting individuals to defraud the recipient.[67]. The APWG also noted 316,747 attacks in December 2021, which was the highest monthly total in APWG's reporting history[68].

Recent Events on Phishing Attacks

The Cofense Phishing Defense Center (PDC) observed a phishing campaign in which the attacker by acting as the Chief Information Officer of the organization attempts to gather login credentials from employees. By pretending to be an executive, the fraudster sends an email

[66] Cisco. (2021). Cyber security threat trends: Phishing, crypto top the list. Retrieved from https://learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

[67] Statistics Canada. (2020, October 4). Canadian spend more money and time online during pandemic and over two-fifths report a cyber incident. Retrieved from https://www150.statcan.gc.ca/n1/daily-quotidien/201014/dq201014a-eng.htm

[68] APWG. (2021). Phishing Activity Trends Report. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q3_2021.pdf?_ga=2.195350636.1174400344.16544610612146370

with a newsletter attached explaining the new precautions and changes to the Company's business operations relative to the Pandemic. To access the newsletter attached in the email, the employee must enter user credentials[69]

In February 2020, Lookout Phishing A.I. discovered a campaign that used SMS messaging to target customers to fake websites of well-known banks in Canada and the U.S., including Scotiabank, CIBC, HSBC, Chase and others. The campaign was designed to capture users' banking and login information[70].

The sudden shift to a remote work environment left many organizations without the time and other resources to take appropriate security measures. Employees were not equipped with appropriate security tools on work-issued devices, allowing fraudsters to ramp up their attacks and make most of these vulnerabilities.

When working from home, employees are using less secure networks than networks used in the office, presenting a significant threat to the organization’s confidential information. 65% of employers allow their employees to access company applications from unmanaged personal devices[71].

In addition, employees are using personal devices for work purposes and work devices for personal activities; this mixing of personal and work devices poses a significant threat

[69] NetSec.News. (2019, July 22). Phishing Campaign Targets Administrator Credentials with Office Alerts. Retrieved from https://www.netsec.news/phishing-campaign-targets-administrator-credentials-with-office-alerts/

[70] Pressley.A. (2020. July 22). Lookout’s 2020 Mobile Phishing report shows 37% sequential increase in first quarter of 2020. Retrieved from https://www.intelligentcio.com/north-america/2020/07/22/lookouts-2020-mobile-phishing-report-shows-37-sequential-increase-in-first-quarter-of-2020/#

[71] Bitglass. (2020). Remote Workforce Security Report. Retrieved from https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY20Q2RemoteWorkforceReport%282%29.pdf?aliId=eyJpIjoiM3JOXC8yWENvbk8yZ2tyUE8iLCJ0IjoienhMa3IwWVFCNXVDVXpYaEVGZTdGUT09In0%253D

to organizations. For example, suppose an employee's credentials are compromised on their device, the hacker may access the organization's confidential and sensitive information if the personal device is being used for work-related activities. Similarly, when employees are browsing social media platforms on work devices, they are providing an opportunity to attackers to hack work devices by accidentally clicking on malicious links sent to their social media pages. Phishing attacks will become more and more sophisticated due to social engineering and other advanced technologies; organizations will have to invest in technologies such as spam filters and web filters and educate and train employees to limit these attacks.

Business email compromise and Vendor Email Compromise

A business email compromise is a type of targeted scam in which an attacker impersonates an authorized official of the organization with the intent of defrauding or extracting sensitive data from the Company or its partners.

Business and vendor email compromises are common phishing scams that have become prevalent in recent years. In BEC, the fraudster impersonates someone of authority in the organization to obtain sensitive information from the Company or defraud the Company. Even before the recent push to a remote workforce, organizations had started shifting to cloud-based emails, which is one of the primary reasons BEC has been thriving.

Recent Statistics on Business Email Compromise

A typical BEC attack begins by identifying its target; the scammer is often seeking individuals authorized to make payments on behalf of the organization or have access to

private and confidential information of the organization. Once the victim is identified, the BEC scammer takes over the online identity of the victim's immediate supervisor and uses tactics such as urgency, persuasion, and authority to obtain information from the victim. If the victim is authorized to make payments, the hacker can also persuade the victim to process payments to a fraudulent account; these payments are often for significant dollar amounts. According to IBM, BEC costs businesses an average of $5.01 million per breach[72]. Followed by a report from APWGA, indicating that the average amount requested during wire transfer BEC attacks was $48,000 in Q3, 2020[73].

Vendor email compromise is a similar technique used by cybercriminals. In such schemes the criminal takes over the account of a legitimate vendor, by registering a domain name that appears relatively similar to the legitimate vendor and then sends emails requesting payment information changes. Once the account information is updated, payments are forwarded to the fraudulent account. In early November 2019, Agari Cyber Intelligence Division predicted that vendor email compromise (VEC) would pose a significant threat to companies in 12-18 months[74]. Agari also reported that in Q3, scammers requested funds in the form of gift cards in 71 percent of BEC attacks. They requested payroll diversions in 6 percent of attacks, in 14 percent, they requested direct bank transfers[75].

[72] IBM. (2021. December 1). Costs of a Data Breach. Retrieved from https://www.ibm.com/security/data-breach

[73] Ibid

[74] Agari Cyber Intelligence Division. (2019). Email Fraud & Identity Deception Trends. Retrieved from https://www.agari.com/cyber-intelligence-research/e-books/q4-2019-report.pdf

[75] Ibid

Recent Events of Business Email Compromise and Vendor Email Compromise

In March, a French pharmaceutical company got tricked into transferring $7.25 million to a supposed hand sanitizer and protective masks supplier. After the money was transferred, the supplier suddenly disappeared, and the items were never received. The "Supplier"[76] was a Singapore-based fraudster that had spoofed the identity of a legitimate company and had begun advertising fast delivery of supplies.

Remote workers rely heavily on email and other online communication channels. For example, when working in person, employees can walk to the office of their co-workers to verify instructions. However, since these facilities are not available when working remotely, employees must take a few extra steps such as phone calls, texts, or follow-up emails. Unfortunately, due to a lack of oversight, workers might sometimes skip these steps and become targets to BEC attacks.

BEC attacks are hard to detect because they don't use malware or malicious URLs; instead, these attacks rely on impersonation and other social engineering techniques. Rather than exploiting software and weak security flaws, these attacks take advantage of human nature. These emails are designed to impersonate someone the individual's trust and trick them into sending personal and confidential information to hackers. For example, the fraudster may impersonate an authorized official of the organization and ask the victim to provide confidential company information. However, due to communication barriers under remote working, the victim may fail to verify the authenticity of the

[76] Deichler.A. (2020. April 14). BEC Scams Poised to Surge in Coronavirus Crisis. Retrieved from https://www.afponline.org/ideas-inspiration/topics/articles/Details/bec-scams-poised-to-surge-in-coronavirus-crisis

request and may end up providing confidential information to the fraudster. **Appendix** D demonstrates a VEC attack.

6.5 Ransomware

"Ransomware is malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattacks place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files[77]."

Ransomware attacks have exploded in recent years, and several factors have contributed to the increase in these attacks. However, one of the most critical factors responsible for the exponential growth of ransomware attacks is the shift to remote work. The most commonly used tools for remote access are virtual remote networks (VPN) and remote desktop protocol (RDP). RDP allows users to access their desktop computers over the Internet, and VPN enables users to access shared network resources outside the company firewall. These tools allow the organization to shift employees to remote workspaces; for example, RDP quickly allows users to easily transition as they will get the same desktop experience at the office. The way companies work, and employees connect to enterprise networks is rapidly changing, and these legacy solutions are struggling to keep up with the modern security needs. Ransomware fraudsters are attacking vulnerable VPN devices, and several security breaches have originated due to security flaws in these systems.

[77] Check Point. (2022). Security report: *Global Cyber Pandemic's Magnitude Revealed*. Retrieved from https://www.checkpoint.com/press/2022/check-point-softwares-2022-security-report-global-cyber-pandemics-magnitude-revealed/

According to Forbes. Ransomware attacks have spread like wildfire due to the surge of remote workers, increasing by 92.7% in 2021 compared to 2020[78].

Recent Statistics on Ransomware

Connecting through insecure home networks, use of weak passwords and lack of cybersecurity training to remote workers are some of the reasons why cyber-attacks have surged in the past two years. In 2021, the largest ransomware payout was made by an insurance company at $40 million, setting a world record[79].

Once the attacker obtains access to company information through either phishing attacks or other method, they focus on identifying and extracting valuable information from the users system. A common technique used by attackers is to completely lock off the user from the system, and access is only given when a specified amount of ransom is paid to the hacker. Inability to access user files and programs can lead to significant financial losses to the organization. The average downtime a company experiences after a ransomware attack is 21 days[80]. In a report by Antivirus firm Emsisoft it was indicated that the average requested fee increased from about $5,000 in 2018 to about $200,000 in 2021[81]. Some businesses quickly identify the attack right away. However, many

[78] Schiappa.D. (2019. October 18). The Rise of Targeted Ransomware Attacks. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/10/18/the-rise-of-targeted-ransomware-attacks/?sh=456c01c15048

[79] Chnag.B. (2021. May 22). One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack. Retrieved from https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5

[80] Johnson.J. (2021. November 10). Length of impact after a ransomware attack Q1 2020- Q3 2021. Retrieved https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/

[81] National Security Institute. (2022). The Growing Ransomware Wave. Retrieved from https://www.nsi.org/2021/02/15/employee-cyber-security-awareness-ransomware-wave/

organizations fail to identify the infection for days or weeks and incur significant losses, including legal damages and fines, ransom payments, damage to reputation etc.

Appendix C demonstrates the stages of a ransomware attack.

Recent Events On Ransomware

On May 7, 2021, Colonial Pipeline, an American oil pipeline system that supplies gasoline to the U.S., suffered a ransomware cyberattack. This attack caused huge gas shortages for several days, and forced the Company to take some systems offline. The Colonial Pipeline Company eventually resolved the attack at a net cost of around $2.1 million to the Company. This attack has now been attributed to a virtual private network breach; an encrypted connection commonly used by remote employees to connect to a company system[82].

Kia Motors America in February suffered a ransomware attack carried out by the Doppel Paymer gang, which demanded $20 million to not leak stolen data. Once data was stolen from the organization, the gang threatened to release the information in two-to-three weeks if the Company did not negotiate with them.[83].

The sudden increase in internet usage for almost everything, including health, finances, work, etc. has allowed attackers to focus on vulnerable systems such as outdated firewalls and servers. Similarly, as organizations move toward hybrid work models, vulnerabilities

[82] Kelly.S. (2021). Colonical Pipeline Contacted Local FBI Offices Prosecutors After Attack – Company. Retrieved https://money.usnews.com/investing/news/articles/2021-06-07/colonial-pipeline-contacted-local-fbi-offices-prosecutors-after-attack-company

[83] Hacknotice. (2021, February 16). Kia Motors America suffers ransomware attack, $20 million ransom. Retrieved from https://hacknotice.com/2021/02/16/kia-motors-america-suffers-ransomware-attack-20-million-ransom-bleepingcomputer/

embedded with cloud usage and storage are coming to light. Attackers are constantly refining their methods. Since the first ransomware attack in 1989[84], the complexity of ransomware attacks has grown exponentially. However, employees working from home lack the necessary tools, including anti-ransomware software, spam filters, offline backups and other tools to protect the organization from ransomware attacks.

6.6 Data Theft and Time Theft

Data Theft

Data theft is the act of stealing confidential or private digital information stored on computers, servers, or electronic devices for the purpose of personally benefiting from it. Ineffective or weak passwords, system vulnerabilities, unsafe networks, compromised downloads and insider threats are a few reasons why organizations are being exposed to data threats.

Employees working from home are unsupervised and accessing the Company's information through unsecured networks, which is one of the prime reason's organizations have become vulnerable to data theft. Organizations with sensitive and confidential customer information, such as the healthcare and finance industries, can lead to severe consequences, including financial losses, damage to reputation, and legal consequences. In addition, when an employee is logging into the computer's network, the information available on the system is also becoming exposed to family members, room partners and others living with the employee if not logged out properly by the employee.

[84] Groot.D.J. (2022, April 4). A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time. Retrieved from https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#:~:text=The%20first%20known%20attack%20was,through%20the%20use%20of%20a

Employees may require strong passwords to login into systems. However, most employees do not have secure networks, allowing fraudsters to hack systems and access sensitive company and client information.

COVID 19 has given a significant boost to digitalization, and as businesses are becoming increasingly digital, data theft, amongst other cybercrimes, is also accelerating. Most businesses still do not have the right infrastructure and policies to protect businesses from these malicious attacks. Data theft attacks are not always from individuals outside the organization; instead, any individual who has access to the Company's networks and data, including employees, consultants or others, can be a target of these threats. Organizations exposes to data theft face severe consequences, including financial losses, legal fees, brand depreciation and loss of customers.

Time Theft

Working from home provides employees with the flexibility of not travelling to the office and the comfort of working within their home offices. However, employers are also concerned about how the employees work when they cannot physically see them. In addition, employers are concerned about whether employees are working for the number of hours they are committed to working.

Working from home can give rise to certain malpractices, eventually causing the organization to lose money. Time theft can be one of the most common causes organizations lose money. When employees claim for the time they have not worked, they are causing the organization to pay for services the businesses did not receive, which leads to a complete loss for the organization.

Recent Statistics on Time Theft

Time theft can result in big losses for organizations. For example, the American Society of Employers estimates that 20% of every dollar earned by a U.S. company is lost to employee time theft[85].

The APA reports that time theft can cost companies up to 7 percent of their gross annual payroll. In other words, a business that pays out $1 million in annual payroll could be losing up to $70,000 each year due to "stolen" time[86].

A study from the staffing firm revealed that mobile devices are the biggest distraction during the workday. Specifically, workers waste 56 minutes per day, or nearly five hours a week, using their mobile devices for non-work activities[87].

Common Types of Time Theft

- Using Personal Email and Cell Phone**:** Since employees are not physically being monitored, employees can spend a lot of work time checking personal email, sending text messages, chatting on different social media platforms, engaging in online shopping and playing games online.

[85] Jones.D. (2019, January 17). The True Cost of Time Theft. Retrieved from https://www.mytotalretail.com/article/the-true-cost-of-time-theft/

[86] Czerwonka.E. (2021, December 17). Prevent Time Theft With an Online Time Clock System. Retrieved from https://buddypunch.com/blog/prevent-time-theft-online-time-clock-system/#:~:text=Furthermore%2C%20the%20APA%20estimates%20that,taking%20extended%20breaks%20and%20lunches

[87] Uzialko.A. (2020. March 17). How Much Time Are Your Employees Wasting on Their Phones. Retrieved from https://www.businessnewsdaily.com/10102-mobile-device-employee-distraction.html

- Extended Breaks and Lunches: Some people steal employers' time by extending their mealtimes and breaks. For instance, a 30-minute break may be prolonged to 45 minutes, especially in companies that do not clock out after lunch breaks.
- Running Personal Errands**:** Employees might opt to take care of their errands during office hours. For instance, some people run their side business, make private phone calls, or attend personal appointments while on the clock.
- Running Personal Business on Work Time: A recent report from the Wall Street Journal[88] indicated employees taking on multiple jobs, toggling between Slack accounts and work calendars, and using excuses like WiFi issues to balance responsibilities and earn higher income by doing so.

Recent Events Related to Time Theft Fraud

Franklin Andrews was a senior analyst and policy advisor in the federal Department of Citizenship, he was terminated when it was discovered that he had been spending 50 to 100 percent of his workday using the internet for personal vs work purposes, Andrews accepted that amount of time he was using the internet during work hours was excessive and inappropriate. The Ministry terminated him for these actions because such excessive and inappropriate misuse of his work time and work equipment amounted to time theft[89].

The recent shift to remote work has accelerated the digital transformation of many organizations and has increased the reliance on unsafe home networks. As a consequence,

[88] Kelly.J. (2021, August 15). The Remote Trend of Working Two Jobs At the Same Time Without Both Companies Knowing. Retrieved from https://www.forbes.com/sites/jackkelly/2021/08/15/the-remote-trend-of-working-two-jobs-at-the-same-time-without-both-companies-knowing/?sh=6938dde217f3

[89] bakertilly. (2011, November 7). Employee Internet Use as “Time Theft?”. Retrieved from https://www.bakertilly.ca/en/btc/publications/employee-internet-use-as-time-theft

we are witnessing a significant rise in ransomware, data theft, phishing and other cyber-crimes. Company networks only allow trusted devices to connect and have stronger protections in place, but when organizations had to quickly enable their employees to work remotely, lack of strong security and weak wi-fi networks left the door open for hackers to access company data and networks. When everyone is connecting through one network it is easy for the organization to monitor that one network as compared to now when IT professional are dealing with thousands of networks. Erica Pimentel in an interview stated:

> "The massive internal control issue becomes when client employees are doing their work from home and there is cybersecurity risk. It is really easy when one is at office, you login to your computer servers and they have complete control over the physical environment and the network environment, all of a sudden all these employees are working from home that have a whole new dimension to all these unknown characters that are maybe accessing the company's physical files or the electronic files"

Post COVID many employees have noticed an increase in fraudulent emails and have been exposed to phishing and ransom ware attempts. Inadequate cyber and data security controls at home networks increases the risk of becoming the target of these attacks. Larger organizations would have some preparedness for these attacks, however mid to small size organizations have been most affected because they were to switch to the virtual world overnight without much preparation. Many of these organizations do not

have IT security teams who have the expertise to effectively manage cybersecurity risks and provide ongoing training for the rest of the team.

A common technique used by cyber attackers is to impersonate an official from the organization and send emails to employees containing infected links or attachments. Once the employee clicks on that link the hacker has access to the employee's credentials and can use that information to further exploit the organization. On some occasions the fraudster may also impersonate the supplier and direct Accounts Payable to change vendor details, so future payments are directed towards the fraudsters account. In an office it is quite simple to check if a colleague has sent a request or a specific email by walking over to their desk and asking if they've sent the message or ask any questions for that matter. Lack of fluidity in communication in a virtual environment has increased the opportunities for hackers to exploit system vulnerabilities.

Many employees are also using personal devices to get their word done from home. This presents an additional challenge for organizations as many individuals do not have their software's updated and maybe accessing confidential work files through a system that has no firewall protection. These employees may also decide to leave the organization while holding these confidential files on personal devices exposing vulnerable corporate information to hackers.

As companies evolve and adapt to technology, there is a higher demand for forensic accounting for fraud quantification and prevention. Furthermore, the Hybrid workplace model and other significant operational changes have created the perfect conditions for fraudsters to perpetrate fraud. For example, Organizations may require assistance from

IFA's to provide training material that would assist employees in taking preventive measures when working from home. IFA's expertise will also be required in identifying and investigating fraud schemes emerging due to WFH. Therefore, it is expected that the role of Forensic Investigators will become more prominent than ever, as reported by Market Research Future the global forensic accounting markets overall valuation post pandemic is expected to be 8.85 billion by 2025. The growth is expected to occur at a pace of 8.2% CAGR due to the development of the new dynamism, making active development in the market's growth, mainly from 2018-to 2025[90].

7.0 CHALLENGES FACED BY IFA'S DUE TO REMOTE WORK ARRANGEMENTS

As many employees have shifted to remote work, IFA's are conducting most investigations remotely. IFA's are required to conduct a thorough investigation while facing the challenges of privacy, confidentiality, security and technology that comes with remote work. Some of these challenges are addressed below.

7.1 Lack of Human Contact

Conducting witness interviews is an integral part of forensic investigations. IFA's are often required to conduct witness interviews to extract critical information concerning the investigation allegation. With most employees working in hybrid work models, face-to-face interviews have been migrated to Zoom and other online meeting platforms, and

[90] GlobelNewswire. (2021, October 28). Forensic Accounting Market Expected to Hit USD 8.85 Billion, at a CAGR of 8.2% by 2025 – Report by Market Research Future. Retrieved from https://www.globenewswire.com/en/news-release/2021/10/28/2323077/0/en/Forensic-Accounting-Market-Expected-to-Hit-USD-8-85-Billion-at-a-CAGR-of-8-2-by-2025-Report-by-Market-Research-Future-MRFR.html

interaction is challenging in meetings conducted through these platforms. Online meetings seem to be a reasonable solution to remote work environments, but they can never fully replace the benefits of face-to-face meetings.

Adam Hanover, CPA/CFF, J.D., managing director of restructuring and dispute resolution at CohnReznick LLP, in an interview, stated:

> "The lack of human contact is challenging. Sometimes, you need to be in the room with an individual to sense whether he or she is hiding something. A personal connection with someone who may or may not be an adversary is of utmost importance in our line of work."[91]

In-person interviews also allow the IFA to read non-verbal cues better, including posture and hand movements which may indicate signs of nervousness. Interviews conducted virtually only allow the interviewer to observe facial expressions, making it difficult for the interviewer to know if the interviewee is hiding something. Lack of human contact in virtual interviews makes it challenging to read the interviewee's body language and can make it difficult to remain engaged in the discussion.

[91] Wiesenfeld.J. (2020, October 5). COVID-19 challenges to forensic accounting. Retrieved from https://www.journalofaccountancy.com/newsletters/2020/oct/coronavirus-challenges-forensic-accounting.html

7.2 Stay Up-to-date on Emerging Fraud Risks

According to the PWC 2022 Global Fraud Survey report, 70%[92] of the respondents encountering fraud have experienced new incidents of fraud as a result of the disruption caused by COVID- 19.

The Pandemic has changed the way businesses operate by forcing more activity into online channels. As businesses cope with these operational changes, fraudsters are looking to exploit this confusion and target individuals and organizations with various scams, including new fraud forms that might not have existed prior to the Pandemic. In the earlier section of this report, it was represented that there has been an observed increase in phishing and ransomware. These fraud schemes entail more sophisticated attempts to trick people into sharing sensitive information. In addition, fraudsters are modifying their efforts to keep up with organizations' changing environment to digitization; therefore, IFA's must keep updated with new fraud schemes types and learn to tackle these novel forms of fraud. In an interview with Erica Pimentel, when asked about challenges faced by IFA's in a remote work environment, she stated

> "Forensic Investigators must ensure that their knowledge is up-to-date, to at least be conversant with these systems. They must also understand the limits of their expertise and recognize when an expert in the subject matter should be brought in. The challenge is that the difference in knowledge between

[92] PricewaterhouseCoopers. (2022). Protecting the perimeter: The rise of external fraud (PwC's Global Economic Crime and Fraud Survey 2022). Retrieved from https://www.pwc.com/lt/en/about/news/fraudsters-target-tech-two-thirds-experienced-draud-in-past-2-years.html

> the Investigator and expert at times is so much that the Investigator can no longer supervise the expert. The accepted standard require that the Investigator is sufficiently competent in the subject matter that they are supervising to be able to challenge the assumptions made by the expert. Therefore, the goal is to upscale enough not to necessarily become experts but enough to at least supervise the experts that they will engage"

Forensic Investigators must also understand the opportunity for fraud to identify which fraud schemes an individual can commit. To achieve this, Forensic Investigators should understand the new fraud schemes and familiarize themselves with the changing operational and control environment of organizations.

7.3 Remote Data Collection

The Investigator would meet with the client to understand the known sources where evidence would be collected. However, prior to the Pandemic, the sources would be limited to devices provided by the employer in most cases. Post-Pandemic data collection activities are no longer limited to devices available on site. Earlier, electronic evidence was collected mainly from three primary sources: computers, email and file servers. Now work is primarily saved on the cloud, and employees are also using mobile devices extensively when working from home. Therefore, Forensic Investigators are now required to not only limit their search to the primary sources identified above but should also review other areas, including the cloud and mobile devices.

When conducting a thorough investigation, the Investigator is required to interview the employer and different employees to identify the possible locations where the suspect

may be hiding information. Searching devices provided by the Company are considered less challenging, as it is considered property of the Company. However, obtaining access to a personal device may be more of a challenge.

Working from home has blurred the lines between professional and personal boundaries. Mobile devices and personal laptops are being used for work purposes, and employer-provided devices are being used for personal purposes. When collecting evidence, forensic Investigators may be required to review the personal devices of the suspect if it is determined that such devices are being used for work purposes. Several methods can be used to capture data stored on these devices, including the traditional method of having these devices confiscated and sent to a digital forensic specialist to create a forensic image of the device. Also, advanced methods allow the digital forensic specialist to take control of a system remotely and create a "live" image of the relevant files. Instant messaging is often used between suspect parties for communication purposes; these platforms allow users to delete/erase messages instantly once the message is read or delivered to the recipient. For example, to gather evidence from a mobile messaging application such as Whatsapp, the Investigator may require decrypting the WhatsApp database.

However, whatever method is selected, the evidence collected will only be valuable to the court if the right legal standards are followed when seizing and reviewing these devices. The IFA must understand that personal devices may store private and confidential information. If the Investigator is handling personal data, they are bound by the privacy act not to disclose such information and to take necessary measures to maintain the confidentiality of such information. In Canada, two significant laws govern the collection

of electronic evidence, including the Personal Information Protection and Electronic Documents Act and the Privacy Act. In addition, the Investigator must understand and comply with the laws of the state and jurisdiction where the investigation is being conducted.

7.4 Privacy and Confidentiality Concerns Due to Remote Interviews

According to the Standard Practices "IFA practitioners should establish appropriate control and management procedures to safeguard the confidentiality, integrity and preservation of all documents and other material that come into their possession or are created during an IFA engagement"[93]

Confidentiality may be compromised when an interview is conducted in a remote environment. The interviewer and interviewee may not have a private space when working from home, and sensitive and private information may be disclosed in the presence of others. During remote interviews, it would be impossible for the Investigator to know if there is an individual unrelated to the investigation present in the room. Someone in the room could also coach the interviewee or record the interview. Therefore, to the best of their ability, the interviewer must ensure that the interview is being conducted in a private room setting away from family, friends or any outsiders.

Information being releases to third parties will pose legal consequences for the Investigator and can also be detrimental to the investigation and taint the investigation's

[93] The Canadian Institute of Chartered Accountants. (2006, November). The Standard Practices for Investigative and Forensic Accounting Engagements. Retrieved from https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/forensic-and-investigative-accounting/publications/standard-practices-investigative-forensic-accounting-engagements

effectiveness and credibility. In addition, the client would not want unnecessary rumours spreading about internal investigations, as negative news can damage the organization's reputation. Under these circumstances, a company has considerably less control over who else, unbeknownst to the Company, might be present during the interview or meeting.

Interviews being conducted on teams or Zoom can also create the risk of mistakenly sharing private or confidential information on screen, especially when documents are being shared with witnesses to conduct the investigation.

If interviews are being recorded, there is a risk of the videos being released to third parties. Therefore, the Investigator must ensure that access to any recording is only limited to those involved in performing the investigation.

7.5 Technological Challenges Due to Remote Interviews

Remote interviews rely heavily on technology, and so many things can go wrong with a video interview; connection problems can cause delays or frozen video. In addition, if the Investigator is disconnected from the Internet, it may take some time to regain connection, which would take away from the time scheduled for the interview, which can result in relevant questions not being asked.

The interviewer or interviewee could have audio issues, where unclear audio can lead to miscommunication. In such cases, the Investigator might be required to ask the same question several times, which can be frustrating for both the interviewer and interviewee.

The interviewee can leave the meeting when a critical question is being asked to the suspect, claiming that they had connectivity issues or could intentionally delay returning to the call. Hence, they have enough time to prepare for the response.

Screen sharing is also a feature allowed by most videoconferencing apps, including teams and Zoom. The Investigator may want to share documents with the interviewee before asking any questions; in such situations, if the interviewee is unable to view the screen/document, this can impact the entire interview process. This impact is because most of the questions are built around the documents collected during evidence-gathering. Therefore, using technology to conduct an interview can be a struggle for both the Investigator and the interviewee.

7.6 Authenticity and Completeness of Documents Collected

The admission of electronic documents is governed by s.31.1 to 31.8 of the Canada Evidence Act and traditional rules of admissibility.

31.1 "Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be

31.2 (1) The best evidence rule in respect of an electronic document is satisfied

- **(a)** on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or
- **(b)** if an evidentiary presumption established under section 31.4 applies.[94]. "

[94] Canada Evidence Act. (2022, June) Authentication of electronic documents. Retrieved from https://laws-lois.justice.gc.ca/eng/acts/c-5/fulltext.html

When working remotely, accessing physical documents of the organization may pose a critical challenge; not all organizations have all relevant documents digitized. Therefore, organizations need to facilitate this new workspace and create digital versions of their documents, including processes such as scanning physical documents. In addition, such documents sent electronically to the Investigator may pose several challenges for the Investigator, one of them being the ability to verify the authenticity and completeness of documents provided. During an interview conducted with Erica Pimentel, she stated:

> "When you rely on electronic evidence that you don't yourself access from the system the risk is always there even if it's remote. Take that to another level when you are not even at the clients site. Now you are seeing the world through the lens of what your client want you to see. From a forensic accountant perspective that becomes even more difficult because you are looking for what's not there, for what's not reported, for what's' missing but now you can only see what the client wants you to see which introduces a completely new dimension. One of the things clients can do is to give access to the system directly, creating an account for them so they can get the information they want. It's important to understand, test and validate the IT controls over all the electronic evidence that is received. We also need to understand if all investigations can be done remotely, or in some cases the risk is too high and we cannot rely on the documents that client is providing, and being in person at the clients site in such cases would be necessary"

These documents could be part of the electronic records presented as evidence to the court. To support the admissibility and weight of electronic evidence as documentary evidence, the Investigator must ensure that these records can be proven or presumed to be reliable, accurate, and authentic.

Authentic in electronic evidence gathering ensures that the evidence is the exact evidence and comes from the right source. There is a risk that the electronic documents provided are either encrypted, overwritten or partially overwritten, therefore making it a challenge for the Investigator to ensure that the documents are not tampered with and that the client has followed due diligence when sending these documents.

The Electronic Records as Documentary Evidence Standards guide developing policies, procedures, processes and documentation that support the continuing reliability, accuracy and authenticity of electronic records to a) ensure that electronic records can reliably support decisions ; b) support the admissibility and the weight of electronic records in legal proceedings; and c) protect the capability of electronic records to effectively document an organization's decisions, actions, and transactions and to hold accountable those who are responsible for them[95].

When dealing with electronic evidence, the IFA must be familiar with the Canadian Evidence Act and the Electronic Records as Documentary Evidence Standards.

[95] Ibid

7.7 Collecting and Reviewing Electronic Evidence

Collection of evidence remotely during the Pandemic has become the most viable and cost-beneficial solution; however, collecting and reviewing digital evidence presents several challenges for Forensic Investigators, including:

- Technology Challenges: Operating systems and application software are undergoing rapid changes. Older versions do not support new software, and various new software is being introduced to the market. As a result, forensic Investigators may be required to update their software or even install the specific software or tool used to create the document on hand.
- Resource Challenges: The Internet has facilitated the flow of communication, and such easiness of communication has increased the volume of data stored online. Large volumes of data are provided to Forensic Investigators, which creates difficulty in identifying original and relevant data. This difficulty also requires the Investigator to go through all the collected data, which may take more time and a bigger team; if time is a limiting factor, it becomes further challenging for the Investigator.
- Legal Challenges: An individual might store private or confidential information on the system they use for work purposes. The Investigator, while investigating, might come across information related to the allegation but is not allowed to use that information against the suspect due to privacy issues. Therefore, forensic Investigators need to know the laws and statutes that govern electronic evidence collection.

- Anti-Forensic Challenges: When dealing with digital evidence, Anti-Forensic has become a significant challenge for Forensic Investigators.

  "Anti-forensics is the process of disrupting or impeding a forensic investigation. This is done by negatively affecting the quality, quantity, or integrity of evidence[96]."
- If an attacker uses anti-forensic techniques to cover up fraudulent activities before evidence is collected, the time and cost of the investigation can increase drastically. Some standard anti-forensic techniques used are hiding and deleting relevant data, digital attacks on forensic Investigators, and creating fake evidence.

Accessing and reviewing data and evidence remotely, conducting interviews through Zoom or other platforms, preserving confidentiality, and verifying electronic evidence's authenticity and reliability are some challenges that forensic Investigators have encountered due to remote work. Investigators are continuously seeking solutions to mitigate the impact of these challenges. However, Forensic Investigators must be mindful that not all investigations can be conducted remotely. If the engagement requires the Investigator to visit the client's premises or interview suspects in person, the client should be informed before taking on the engagement.

8.0 REMOTE WORK AND DIGITIZATION

When the Pandemic hit in 2020, organizations quickly invested in new digital capabilities to outlive the Government imposed stay-at-home restrictions. Remote work, supply chain disruptions and consumers' shift to online channels posed several challenges, which

[96] Herd.A. (2021, June 12). Anti-Forensic. Retrieved from https://hack.technoherder.com/anti-forensic-techniques/

required businesses to accelerate their adoption of digital technologies. Virtual collaboration software such as zoom and teams, cloud-based office systems, mobile technology, automated machinery, and A.I. applications were some digital tools organizations invested in smoothly running their business operations. Over 60%[97] of firms have adopted new technologies or management practices since the Pandemic, while a third have invested in new digital capabilities. Covid-19 accelerated or prompted this adoption.

Digitization has changed the way businesses operate. For example, customer interactions with businesses have become online, and individuals within organizations do not communicate through traditional methods. Therefore, organizations' implementation of digital technologies was a necessary action to function efficiently and effectively during the Pandemic.

With the changing landscape around how employees continue to work in future, organizations will continue investing in digital technologies to streamline workflows and improve productivity. This era of digitization will provide opportunities for both fraud perpetrators and Forensic Investigators. Fraudsters will use advanced technology tools to perpetrate fraud, and Investigators will use advanced technologies such A.I. and Machine learning to discover fraud. However, the advancement of digitization will also present several challenges to Fraud Investigators requiring them to learn new skills and techniques that would allow them to defeat fraud perpetrators.

[97] Valero.A, Riom.C. (2020, September). The Business Response to Covid-19: the CEP-CBI survey on technology adoption. Paper No.009. Retrieved from The London School of Economics and Political Science https://cep.lse.ac.uk/pubs/download/cepcovid-19-009.pdf

Recent developments, such as cloud solutions, virtual communications and remote working, means that Forensic Investigators must look outside the traditional methods of conducting investigations and acquire skills and learn new techniques that will prepare them to deal with challenges associated with digitization.

9.0 SKILLS NEEDED BY IFA'S TO DEAL WITH REMOTE WORK CHALLENGES

9.1 Data Mining

The changing landscape has resulted in organizations digitizing all their information, eventually resulting in large volumes of data. The excessive electronic information available is a challenge to forensic Investigators. Most forensic accounting engagements are time-sensitive, and when litigation is involved, forensic Investigators are more likely to meet specific deadlines. When large amounts of electronic data are presented to Forensic Investigators, it may take them several weeks or even months to identify and analyze relevant information. In such cases, data mining tools can be valuable by allowing forensic Investigators to extract valuable information from large data sets without spending time reviewing each document provided. With the use of data mining tools, Forensic Investigators can promptly and systematically analyze a vast amount of data to produce useful information.

Email is a common means of communication in organizations. When organizations have shifted to remote work with less in-person interaction, individuals have likely shifted to communication through emails or other instant messaging platforms. Email is accepted as legal evidence; however, manually analyzing large volumes of email can be tedious and

not cost-effective. Learning data mining tools can be handy to Forensic Investigators, as it allows them to gather relevant information efficiently and cost-effectively.

9.2 Mobile Forensics

Due to the extensive use of mobile devices, critical evidence is likely stored in these devices. Mobile devices refer to any handheld electronic device that can quickly move from one location to another and encompass gadgets such as mobile phones, smartphones, and tablets. Due to the advancement of smartphones, mobile devices can be used for work purposes, for example, to check emails, review documents and presentation files, to call and text work colleagues. Digital relevant information may be stored on these devices, and the Investigator must ensure to acquire every piece of information that may be relevant to the investigation. Forensic Investigators must know about the mobile operating systems to collect evidence through mobile devices. Most mobile phones are running iOS or Android; knowledge of these two mobile operating systems will allow the Investigator to explore many mobile devices. Forensic Investigators must also be familiar with the procedures to be followed when retrieving data from these devices. Finally, the Investigator must ensure the integrity of the information being extracted from mobile devices; the evidence is not admissible in court if the information is compromised during collection.

9.3 E-Discovery Tools

The advancement of technology has made it important for all organizations to store their information electronically. Having a robust mechanism that can identify, collect and preserve and present relevant information is becoming extremely important. “E-

Discovery is the process in which electronic data is sought, located, secured, reviewed and produced for use as evidence in a civil or criminal lawsuit[98]". During this procedure, data is brought to a single location so that Investigators can view it. E-discovery tools allow users to reduce the volume of data which has the potential to enhance the investigation significantly. Often, a document is duplicated; for example, an email that is CC"d, in such cases e-discovery tools can identify and remove duplicated documents, reducing the volume of data available for the user to review. Keyword searching can also be used, where a single key term is searched, or multiple searches are combined by words "AND", "OR" "Not"[99]. Once the data is collected, the documents are manually reviewed to determine their relevance to the investigation. There are several e-discovery tools available. Logikcull, Everlaw, Nuix, and Relativity are a few to name. Logikcull is an e-discovery tool that narrows the actual data set by date range, document type, email type, and other available filters. Forensic Investigators must learn how to use these e-discovery tools and store, search, and review data through these tools.

9.4 Artificial Intelligence

The amount of data that must be analyzed is increasing, but its nature and how you interpret it are constantly changing. Since A.I. is becoming widely available to more and more people, the potential of the technology to be used for malicious purposes also increases significantly. An understanding of the technology is necessary to counter these attacks and be prepared for forensic challenges regarding crimes committed with A.I.

[98] Lawton.D, Stacey.R, Dodd.G. (2014. September). eDiscovery in digital forensic investigations. Retrieved https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf

[99] Ibid

Artificial intelligence can mimic the problem-solving and decision-making capabilities of the human with use of computers and machine learning. Data entry and analysis are integral to the forensic accounting profession and artificial intelligence can use machine learning to identity trends in data and patterns in data and can exponentially increase data analyzing practices.

New fraud schemes have emerged, and fraudsters have become extremely sophisticated in their attacks because of advances in technology. Forensic Investigators can improve the efficiency of their investigations by utilization of these A.I. platforms. Forensic Investigators should understand how these technologies can be used to support their findings and how evidence gathered through A.I. techniques can be presented to the court.

Machine learning is a further evolution of artificial intelligence and can be useful to forensic Investigators especially in preventing cybercrime. For example, programs are being created that identify trends in cybercrime and, based on analysis of these trends machine learning can assist Investigators in being prepared for the cybercriminals next step.

Tools such as Encase can be used, allowing examiners to automate common tasks, complete comprehensive searches, identify relevant items, and create compelling reports faster than ever before[100].

[100] Guidance Software. EnCase Forensic Transform your Investigations. Retrieved from https://www.ibm.com/topics/what-is-blockchain

During a forensic audit/investigation, auditors focus on transactions susceptible to fraud or an area identified as fraudulent. With advanced A.I. and machine learning techniques, dissecting financial data to identify spending patterns and high-risk transactions for CPA for review has become much less time-consuming when compared to the traditional manual sampling methodology used by auditors. As a result, it has now become business imperative to adopt sophisticated I.T. infrastructure, A.I. platforms, and tools not to enable accounting firms to improve efficiencies of their audits and investigations to detect fraudulent activity when internal controls fail.

Key benefits of incorporating AI into forensic Audits

- A.I. platforms can process and analyze massive amounts of data in a significantly reduced timeline, thereby saving staff time and engagements timeline
- NLP (Natural Language Processing) in A.I. can help identify key terms and performance indicators within contracts, administrative documents, and financial reports. In addition, machine Learning can detect anomalies or inconsistencies in data sets with fewer human interactions, thereby reducing the risks of human errors through clerical analysis.
- A.I. techniques can process the massive amount of data enabling AI-powered platforms to summarize the massive amount of data into user-friendly visuals to illustrate findings and support auditors in faster decision making. This process allows for more accurate, timely, and understandable data analytics.

9.5 Blockchain Technology

Blockchain technology is method to pass information from one person to the other safely and fully automated in real time. As a database, a blockchain stores information electronically in digital format.

Various organizations use blockchain technology to streamline transactions and reduce costs, but most importantly, to protect businesses from online crimes. A report by the World Economic Forum suggests that 10% of global GDP will be stored on blockchain-related technology by 2025, which implies that the way transactions are recorded and communicated will completely transform between now and then[101].

With digitization under the changing landscape, digital payments have become a daily necessity and carry the risk of information theft during the transaction process. In addition, many financial institutions and individuals have lost significant funds due to the insecure systems of banks and other financial institutions. Blockchain technology is a decentralized public ledger, allowing all participants to have visibility over the transactions and making it almost impossible to tamper with any information stored on the blockchain.

As more and more organizations are implementing blockchain technologies in their existing systems, Forensic Investigators need to be aware of the potential impact this may have on their investigations. Additionally, Investigators must understand the nature of the technology and its potential risks and controls. Cryptocurrencies are becoming typical,

[101] World Economic Forum. (2015). Deep Shift, Technology Tipping Points and Societal Impact. Retrieved from https://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

and Investigators must be able to investigate suspicious crypto transactions just as effectively as they do for traditional currencies.

Blockchain technologies can also be relevant to Forensic Investigators when reviewing digital evidence. Transparency of how digital evidence is produced, accessed or modified will enhance the reliability of the digital evidence chain of custody. The blockchain's properties prevent disputing the chain of custody of digital evidence during a judicial procedure, a common challenge for many law enforcement agencies and forensic Investigators. Blockchain technology can improve digital evidence management in multiple ways, as the blockchain tracks every movement enabling a comprehensive view of transactions since origination. Once data is stored on the blockchain, it cannot be changed or reversed except with the blockchain participants agreement. This is an independent proof that digital evidence was created at a specific time and has not been changed since then.

9.6 Social Engineering

"Social engineering is a form of fraud that exploits vulnerabilities in human decision-making. Rather than hacking or otherwise directly stealing, scammers who use social engineering manipulate individuals into transferring money or divulging company secrets"[102].

[102] KnowBe4. Define Social Engineering. Retrieved from https://www.knowbe4.com/what-is-social-engineering/

A common social engineering scheme is when individuals receive a fraudulent email from their financial institution asking to click on a link. Because the email appears to be a legitimate email from the institute, the individual may follow the directions and provide personal information. Perpetrators use this personal information to empty checking and saving accounts, steal other credentials, and apply for loans. Some common social engineering techniques that exist include

- Hackers impersonate an individual with authority within the organization. For example, fraud perpetrators may request the employee to process payments or disclose confidential information about the organization.
- They are sending emails to employees that offer them access to new information. These emails include a link by clicking on which the hacker can access the employee's system.
- A commonly used social engineering technique offers the victim an incentive that motivates the individual to reveal sensitive or private information.
- A classic social engineering move is to offer something very tempting that motivates the victim to reveal some information or take some action. For example, a company offering customers a reward for writing a product review requires the customer to input personal information.

Social engineering techniques can include many forms, including phishing, email hacking, pretexting, and identity theft. The significant rise in social engineering attacks may require organizations to seek assistance from Forensics Investigators. Therefore, forensic Investigators must stay informed about recent developments in social

engineering techniques to assist organizations in reducing the risks associated with social engineering and prevent these attacks from succeeding.

9.7 Remote Interview Tools and Techniques

To conduct interviews remotely, the Investigator should be familiar with the technology used to conduct the interview; understanding the application will prevent the Investigator from undue anxiety and allow for a free-flowing, lively interaction. Once the platform is decided, the Investigator should ensure that all involved have the same updated version of the software required to conduct the call. The software selected should be secure and have end-to-end encryption. A technical trial run of the video conferencing platform should be performed, and the Investigator should ensure that the computer camera, microphone, and internet connection are working correctly. The Investigator should also prepare a pre-interview script in advance and ensure consistent messaging is given to all interviewees to avoid confusion.

It is likely that confidential information might be shared during interviews. Therefore the Investigator should ensure that the interviewee is alone in the room and is not recording the interview. A written consent form should be obtained from the interviewee where the interviewee agrees not to record the interview. Preservation of confidentiality must be ensured throughout the remote investigation.

The interviewee should be informed in advance and asked for consent if the interview is being recorded. During the interview, the witness may disclose personal information; therefore, it should be securely stored and protected to prevent misuse or unauthorized access if the discussion is recorded.

It may be necessary for the interviewee to be shown documents as part of the interview. Any such documents should be clearly numbered for ease of reference. The software can allow screen-sharing to show interviewees relevant documents or provide them in a view-only format, preventing downloading, printing, editing, or sharing with others. Interviewees should be reminded not to copy any documents shown to them, and their confirmation should be obtained, ideally in writing (e.g., by email) before the interview. It is impossible to prevent all risks of the interviewee copying documents, e.g., taking photos or screenshots.

As with all investigations, not all interviewees will be willing to cooperate. For example, interviewees could end the virtual interview or fake technical difficulties to avoid answering questions. They could also communicate with others during the interview to get their stories straight, for example, have someone pass them notes with responses. Forensic Investigators must be familiar with these challenges and be prepared in advance if faced with such issues.

10.0 CONCLUSION

Since the beginning of the Pandemic, remote work arrangements have given rise to a significant increase in fraud attacks. An increase in productivity, savings from real estate costs, and higher satisfaction among employees are some factors which remote work has become a success. However, businesses have also been negatively impacted due to fraudulent activities arising out of this new workspace. There has been an increase in reported cases of common fraud methods, but experts have also noticed new forms of

fraud. Some of these new forms of fraud are directly related to working from home, such as time theft.

Most organizations will continue enforcing a hybrid work model, partially allowing employees to work from home. However, as organizations are updating their technologies to accommodate work-from-home arrangements, fraudsters at the same time are also becoming more sophisticated with their attacks, which is resulting in a significant increase in cybercrimes.

To mitigate the impact of these fraudulent activities, organizations are hiring experts for procuring consulting services about fraud prevention. Forensic Investigators have a crucial role in assisting these organizations in establishing preventative measures to reduce fraud risks and providing expertise in investigating fraudulent activities. Forensic Investigators can also help organizations prepare against emerging fraud schemes by providing anti-fraud training and consulting services.

The massive shift towards remote work has not only been a challenge for companies but also for forensic Investigators. For example, forensic investigators must adapt to new investigation methods as remote work limits their access to specific data and prevents them from collecting all the evidence.

The forensic Investigators will play a significant role in combatting these frauds and reducing the risks, regardless of their challenges. In the coming years, more companies will have to work closely with the experts to minimize the impact of fraud and prepare them for the upcoming threat caused due to a further shift of employees working from home. In addition, fraud perpetrators use cybercrime, social engineering, and artificial

intelligence to take advantage of the ongoing operational changes businesses are experiencing. As a result, forensic Investigators, now more than ever, are required to expand their knowledge and skills to deal with the challenges that the new work landscape has presented to the world.

Appendix A

Abbreviations

ACFE –	Association of Certified Fraud Examiners
APA –	American Payroll Association
APWG –	Anti Phishing Work Group
BEC –	Business Email Compromise
CAGR –	Compound Annual Growth Rate
FBI –	Federal Bureau of Investigation
FTC –	Federal Trade Commission
GWI –	Global Web Index
IBM –	Internal Business Machine Corporation
IFA –	Investigative and Forensic Accountant
INR –	Item Not Received
OECD –	The Organization for Economic Co-operation & Development
OPEC –	The Organization of Petroleum Exporting Countries
RDP –	Remote Desktop Protocol
VEC –	Vendor Email Compromise
VPN –	Virtual Remote Network

Appendix B

Interview Questions

Date of Interview: June 3, 2022

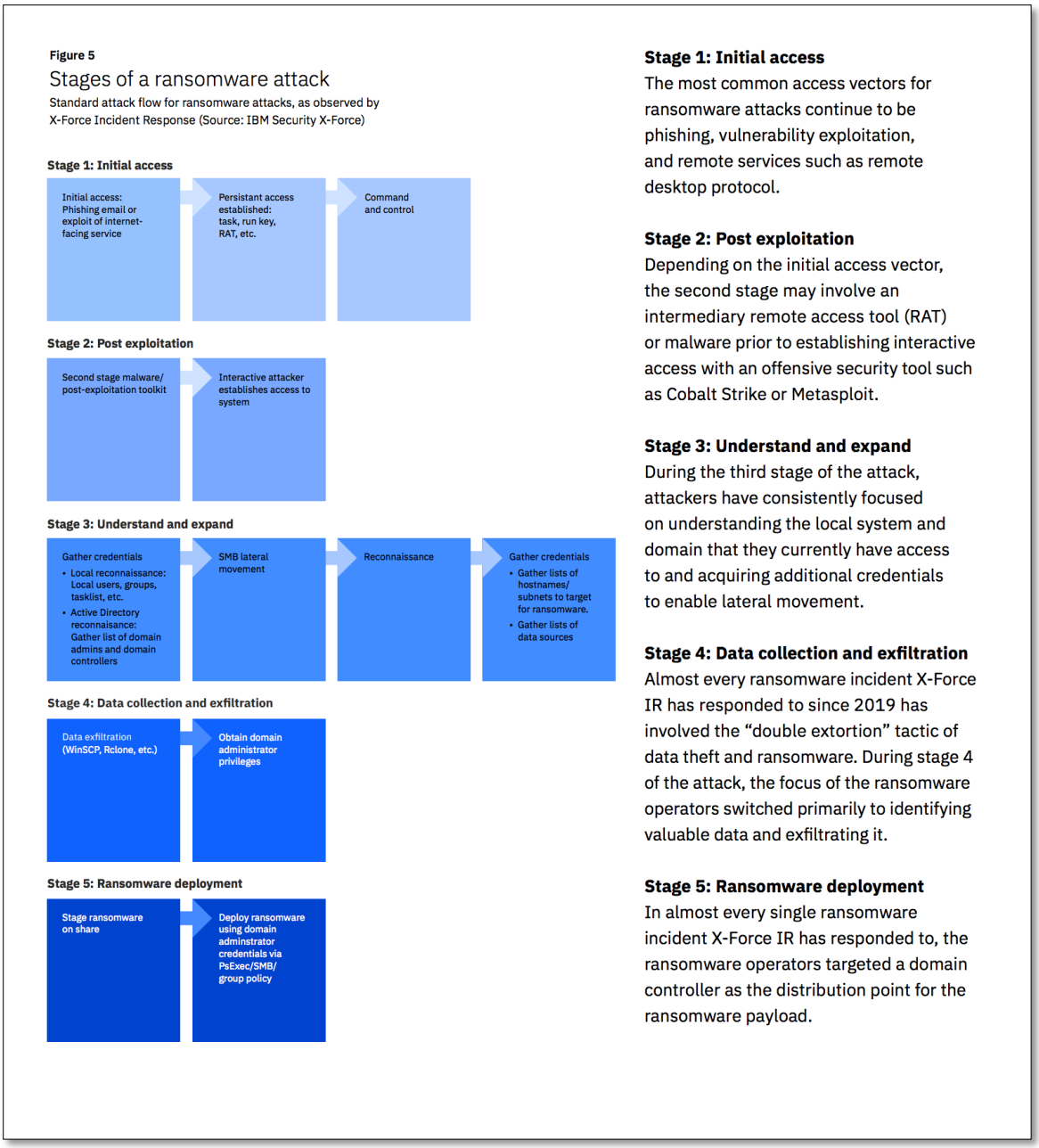
1. Please provide your full name
2. What is your current role, and does your recent research work entail?
3. The title of my research project is Fraud Risks Associated with Remote Work and the Challenges Faced by Forensic Investigators, but most of my questions are directed at challenges faced by the audit profession because I believe that similar challenges will befall forensic Investigators. Do you agree with my assumption, and if not, why not?
4. Some of your research work explores how technological disruption impacts the ways in which auditors engage with their work, can you please tell me more about that?
5. How can auditors prepare for the challenges of emerging technologies?

Interview Questions – (Cont.)

6. Will auditors have less on-site, face-to-face work with clients at client premises in the future? If so, how will the role of auditors and the practice of auditing be affected?
7. How will audit risks be changed by less face-to-face work with clients, and by less daily contact with colleagues due to increased working at home?
8. What are some of the challenges from blockchain technology that you foresee for auditors?
9. Do you foresee any important challenges facing forensic Investigators that auditors will not face in the future? If so, what are they?

Appendix C

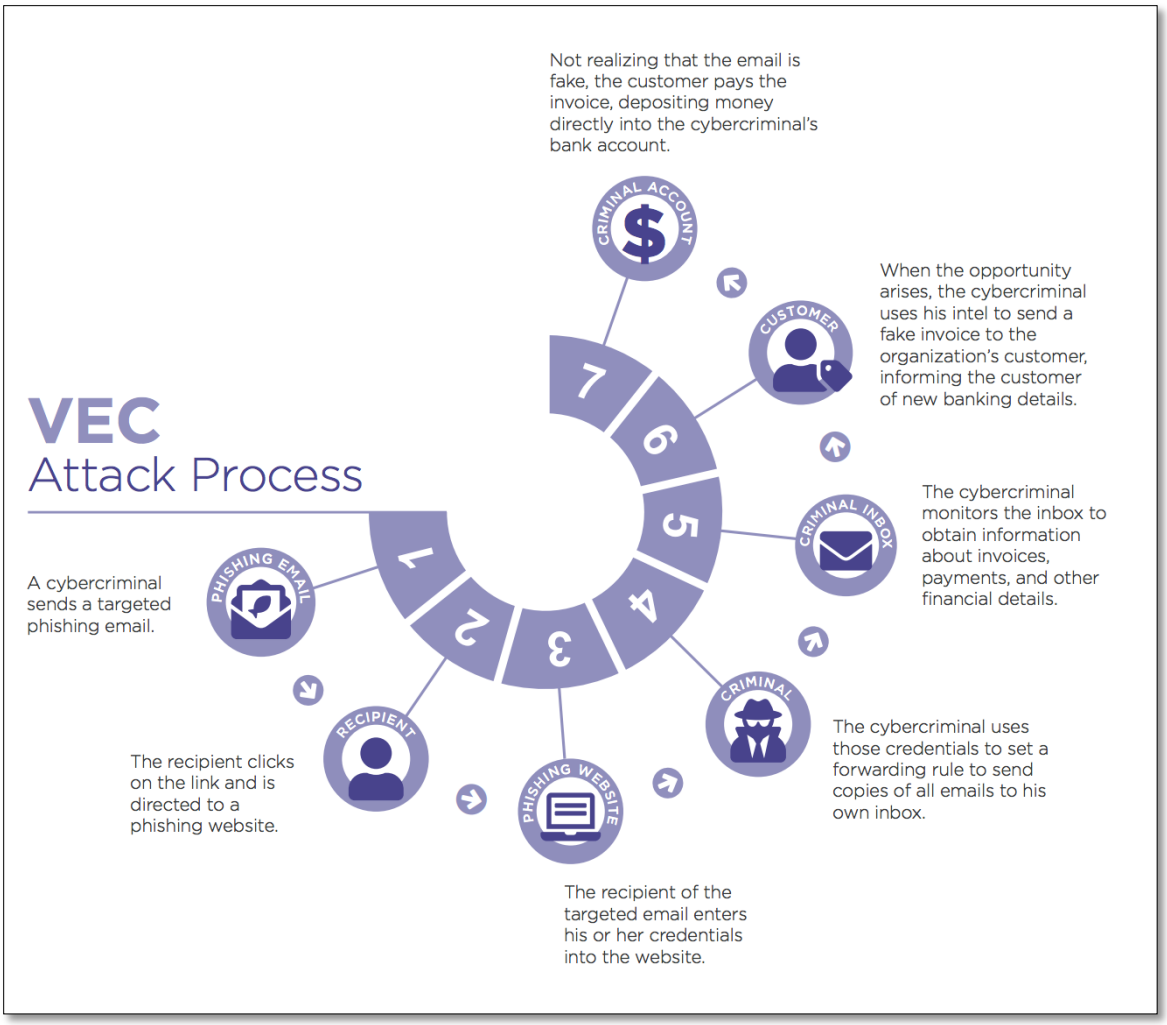
Stages of a Ransomware Attack



Source: Stages of a ransomware attack retrieved from IBM Security; Global Threat Intelligence Report

Appendix D

Stages of a Vendor Email Compromise Attack



Source: Anatomy of a Compromised Account. Retrieved from Agari Cyber Intelligence Division

Bibliography

ACI Worlwide. (2021, February). *Pandemic-Driven Patterns of eCommerce Fraud.* Retrieved from aciworldwide.com: https://www.aciworldwide.com/wp-content/uploads/2021/04/pandemic-driven-patterns-of-ecommerce-fraud-article.pdf

Adeshina, A. (2020). *How Blockchain Technology Can Prevent Fraud.* Retrieved from Blockchain Council: https://www.blockchain-council.org/blockchain/how-blockchain-technology-can-prevent-fraud/

Agari Cyber Intelligence Division. (2019). *Email Fraud & Identity Deception Trends.* Retrieved from agari.com: Agari Cyber Intelligence Division. (2019). Email Fraud & Identity Deception Trends. Retrieved from https://www.agari.com/cyber-intelligence-research/e-books/q4-2019-report.pdf

APWG. (2021). *Phishing Activity Trends report.* Retrieved from APWG: https://docs.apwg.org/reports/apwg_trends_report_q3_2021.pdf?_ga=2.195350636.1174400344.1654461061-2146370929.1654461061&_gl=1*r32f5t*_ga*MjE0NjM3MDkyOS4xNjU0NDYxMDYx*_ga_55RF0RHXSR*MTY1NDQ2MTA2MS4xLjAuMTY1NDQ2MTA2MS4w

Association of Certified Fraud Examiners., Grant Thornton. (2020). *Strengthen your fraud defenses*. Preparing for the post-pandemic fraud landscape. Retrieved from https://www.grantthornton.ca/insights/strengthen-your-fraud-defenses/ -

Association of Fraud Examiners. (2020). *The Report to The Nations. Global Study on Occupation Fraud and Abuse*. Retrieved from https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf

Association of Fraud Examiners. (2022). *Occupational Fraud 2022*. Retrieved from https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf –

Bakertilly. (2011, November 7). *Employee Internet Use as "Time Theft?"*. Retrieved from https://www.bakertilly.ca/en/btc/publications/employee-internet-use-as-time-theft

Barrero,J., N.Bloom and S.Davis (2020),*Why Working From Home Will Stick* http://dx.doi.org/10.2139/ssrn.3741644

Bitglass. (2020). *Remote Workforce Security Report*. Retrieved from https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY20Q2RemoteWorkforceReport%282%29.pdf?aliId=eyJpIjoiM3JOXC8yWENvbk8yZ2tyUE8iLCJ0IjoienhMa3IwWVFCNXVDVXpYaEVGZTdGUT09In0%253D

Butler.H. *The History of Remote Work: How It Became What We Know Today*. Crossover. Retrieved from https://www.crossover.com/perspective/the-history-of-remote-work

Calif.S. (2020. November 13). *Cybercrime to Cost the World $10.5 Trillion Annually By 2025*. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Canadian Anti Fraud Centre. (2022). *The Impact of Fraud so Far this Year*. https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

Canada Evidence Act. (2022, June) Authentication of electronic documents. Retrieved from https://laws-lois.justice.gc.ca/eng/acts/c-5/fulltext.html

Castrillon.C. (2020. December 27). *This is the Future of Remote Work in 2021*. Forbes Magazine. Retrieved from https://www.forbes.com/sites/carolinecastrillon/2021/12/27/this-is-the-future-of-remote-work-in-2021/?sh=3446cb8f1e1d

Chnag.B. (2021. May 22). *One of the biggest US insurance companies reportedly paid hackers $40 million ransom after a cyberattack*. Retrieved from https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5

Check Point. (2022). Security report: *Global Cyber Pandemic's Magnitude Revealed*. Retrieved from https://www.checkpoint.com/press/2022/check-point-softwares-2022-security-report-global-cyber-pandemics-magnitude-revealed/

Choudhary. P. (2020). *Our Work from Anywhere Future. Harvard Business Review*. Retrieved from https://hbr.org/2020/11/our-work-from-anywhere-future

Cisco. (2021). *Cyber security threat trends: Phishing, crypto top the list*. Retrieved from https://learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

Criscuolo, C., P. Gal, T. Leidecker, F. Losma, and G. Nicoletti. (2021). *Telework after COVID-19: Survey evidence from managers and workers on implications for productivity and well-being*. OECD Global Forum on Productivity.

Czerwonka.E. (2021, December 17). *Prevent Time Theft With an Online Time Clock System*. Retrieved from https://buddypunch.com/blog/prevent-time-theft-online-time-clock-system/#:~:text=Furthermore%2C%20the%20APA%20estimates%20that,taking%20extended%20breaks%20and%20lunches

Deichler.A. (2020. April 14). *BEC Scams Poised to Surge in Coronavirus Crisis*. Retrieved from https://www.afponline.org/ideas-inspiration/topics/articles/Details/bec-scams-poised-to-surge-in-coronavirus-crisis

Ekran. (2022, May 5). *5 Industries Most at Risk of Data Breaches*. Retrieved from https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches

Federal Bureau of Investigation. (2020. June 10). I*ncreased Use of Mobile Banking Apps Could Lead to Exploitation*. Retrieved from Internet Crime Complaint Center (IC3) | Increased Use of Mobile Banking Apps Could Lead to Exploitation

Federal Trade Commission. (2022, February 22). *New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021*. Retrieved from https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0

Forrester. (2021). Beyond Boundaries: *The Future of Cybersecurity in the World of Work.* Retrieved from https://static.tenable.com/marketing/whitepapers/Forrester-Beyond_Boundaries_The_Future_of_Cybersecurity_in_the_New_World_Of_Work.pdf

Global Workplace Analytics. (2022). *Cost and Benefits of Agile Work Strategies for Companies.* Retrieved from https://globalworkplaceanalytics.com/resources/costs-benefits#toggle-id-4 –

Giact. (2021, March). *U.S. Identity Theft: The Stark Reality*. Retrieved from https://giact.com/identity/us-identity-theft-the-stark-reality-report/

GlobelNewswire. (2021, October 28). *Forensic Accounting Market Expected to Hit USD 8.85 Billion, at a CAGR of 8.2% by 2025 – Report by Market Research Future*. Retrieved from https://www.globenewswire.com/en/news-release/2021/10/28/2323077/0/en/Forensic-Accounting-Market-Expected-to-Hit-USD-8-85-Billion-at-a-CAGR-of-8-2-by-2025-Report-by-Market-Research-Future-MRFR.html -

Groot.D.J. (2022, April 4). *A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time*. Retrieved from https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time#:~:text=The%20first%20known%20attack%20was,through%20the%20use%20of%20a

Guidance Software. *EnCase Forensic Transform your Investigations*. Retrieved from https://www.ibm.com/topics/what-is-blockchain

Hacknotice. (2021, February 16). *Kia Motors America suffers ransomware attack, $20 million ransom*. Retrieved from https://hacknotice.com/2021/02/16/kia-motors-america-suffers-ransomware-attack-20-million-ransom-bleepingcomputer/

Herd.A. (2021, June 12). *Anti-Forensic*. Retrieved from https://hack.technoherder.com/anti-forensic-techniques/

IBM. (2021. December 1). *Costs of a Data Breach*. Retrieved from https://www.ibm.com/security/data-breach

IBM Security. (2022). *X-Force Threat Intelligence Index*. Retrieved from https://www.key4biz.it/wp-content/uploads/2021/05/2021-Global-Threat-Intelligence-Report-full-report.pdf

Identity Theft Resource Center. (2021). *Annual Data Breach Report*. Retrieved from https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/

IT Security News. (2022. March 4). *The most impersonated brands in phishing attacks.* Retrieved from https://www.itsecuritynews.info/the-most-impersonated-brands-in-phishing-attacks/

Javelin (2021). *2021 Identity Fraud Study. Shifting Angles*. Retrieved from https://javelinstrategy.com/content/2021-identity-fraud-report-shifting-angles-identity-fraud

Johnson.J. (2021. November 10). *Length of impact after a ransomware attack Q1 2020-Q3 2021*. Retrieved https://www.statista.com/statistics/1275029/length-of-downtime-after-ransomware-attack/

Jones.D. (2019, January 17). *The True Cost of Time Theft*. Retrieved from https://www.mytotalretail.com/article/the-true-cost-of-time-theft/

Kelly.J. (2021, August 15). *The Remote Trend of Working Two Jobs At the Same Time Without Both Companies Knowing*. Retrieved from

https://www.forbes.com/sites/jackkelly/2021/08/15/the-remote-trend-of-working-two-jobs-at-the-same-time-without-both-companies-knowing/?sh=6938dde217f3

Kelly.S. (2021). *Colonical Pipeline Contacted Local FBI Offices Prosecutors After Attack – Company*. Retrieved https://money.usnews.com/investing/news/articles/2021-06-07/colonial-pipeline-contacted-local-fbi-offices-prosecutors-after-attack-company

Kosoff.M. (2015. January 5). *How one 24-year old got $50,000 in Free Uber Rides By Duping Uber's Promo-Code System*. Retrieved from https://www.businessinsider.in/tech/How-One-24-Year-Old-Got-50000-In-Free-Uber-Rides-By-Duping-Ubers-Promo-Code-System/articleshow/45767241.cms

KnowBe4. *Define Social Engineering*. Retrieved from https://www.knowbe4.com/what-is-social-engineering/

Lederer, E. M. (2020, May 23). *Top UN Official warns malicious emails on rise in pandemic.* Retrieved from abc News: abc News. (2020. May 23). Top UN official warns malicious emails on rise in pandemic. Retrieved from https://abcnews.go.com/Technology/wireStory/top-official-warns-malicious-emails-rise-pandemic-70846787

Lawton.D, Stacey.R, Dodd.G. (2014. September). *eDiscovery in digital forensic investigations.* Retrieved https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf

Lund.S., Cheng.W., Dua.A., Smet.A.D., Robinson.O., Sanghvi.S. (2020, September 23). *What 800 executives envision for the post pandemic workforce*. Retrieved from https://www.mckinsey.com/featured-insights/future-of-work/what-800-executives-envision-for-the-postpandemic-workforce

National Security Institute. (2022). *The Growing Ransomware Wave*. Retrieved from https://www.nsi.org/2021/02/15/employee-cyber-security-awareness-ransomware-wave/

NetSec.News. (2019, July 22). *Phishing Campaign Targets Administrator Credentials with Office Alerts*. Retrieved from https://www.netsec.news/phishing-campaign-targets-administrator-credentials-with-office-alerts/

Oyedele.A. (2017. May 6). *Buffet: This is 'the number one problem with mankind'*. Retrieved from https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5

Perachio.G, Sexton.R. (2020, June 12). *COVID-19 implications: internal fraud*. Retrieved from https://www.ey.com/en_uk/disrupting-financial-crime/financial-crime/covid-19-implications-internal-fraud

Pressley.A. (2020. July 22). *Lookout's 2020 Mobile Phishing report shows 37% sequential increase in first quarter of 2020*. Retrieved from https://www.intelligentcio.com/north-america/2020/07/22/lookouts-2020-mobile-phishing-report-shows-37-sequential-increase-in-first-quarter-of-2020/#

PricewaterhouseCoopers. (2022). *Global Economic Crime and Fraud Survey*. Retrieved from https://www.pwc.com/gx/en/forensics/gecsm-2022/pdf/PwC%E2%80%99s-Global-Economic-Crime-and-Fraud-Survey-2022.pdf

Ponemon Institute. (2020). *Cybersecurity in the Remote Work Era*. Retrieved from https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf

PYMNTS Beyond eCommerce Fraud. (2021. November). *How Retailers Can Prevent Customer Policy Abuse*. Retrieved from https://www.thehive-network.com/wp-content/uploads/2021/12/PYMNTS-Beyond-eCommerce-Fraud-November-2021.pdf

Ravelin. (2022). *Online Merchant Perspectives. Fraud And Payments Survey*. Retrieved from https://www.ravelin.com/blog/online-merchant-perspectives-fraud-payments-survey-2022

Ren.H. (2022, February 15). *In 10 Years, 'Remote Work' Will Simply Be 'Work'*. Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2022-02-15/in-10-years-remote-work-will-simply-be-work

Reynolds.W.B, Bibby.A. *The Complete History of Working From Home*. Retrieved from https://www.flexjobs.com/blog/post/complete-history-of-working-from-home/

Rosenthal.M. (2022, January 12). *Must-know Phishing Statistics: Updated 2022*. Retrieved from https://www.tessian.com/blog/phishing-statistics-2020/

Roberts.J. (2019. October 27). *Broke students cash in after discovering 'Amazon coucher glitch'*. Retrieved from https://metro.co.uk/2019/10/27/broke-students-cash-discovering-amazon-voucher-glitch-10993142/

Rodriguez.G.A. (2022. January 29). *From policy abuse to friendly fraud: Retailers face billions in revenue loss*. Retrieved from https://fashionunited.com/news/business/from-policy-abuse-to-friendly-fraud-retailers-face-billions-in-revenue-loss/2022012945450

Schiappa.D. (2019. October 18). *The Rise of Targeted Ransomware Attacks*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/10/18/the-rise-of-targeted-ransomware-attacks/?sh=456c01c15048

Security. (2020, December 10). *83% of top US retailers have online vulnerabilities, posing cybersecurity threats*. Retrieved from https://www.securitymagazine.com/articles/94137-of-top-30-us-retailers-have-online-vulnerabilities-posing-cybersecurity-threats

Smulders.S. (2021, August 4). *How the Pandemic has changed the online sales Landscape*. Retrieved from https://www.forbes.com/sites/forbesbusinesscouncil/2021/08/04/how-the-pandemic-has-changed-the-online-sales-landscape/?sh=3074b1718362

The Canadian Institute of Chartered Accountants. (2006, November). The Standard Practices for Investigative and Forensic Accounting Engagements. Retrieved from https://www.cpacanada.ca/en/business-and-accounting-resources/other-general-business-topics/forensic-and-investigative-accounting/publications/standard-practices-investigative-forensic-accounting-engagements

Statistics Canada. (2020, October 4). *Canadian spend more money and time online during pandemic and over two-fifths report a cyber incident*. Retrieved from https://www150.statcan.gc.ca/n1/daily-quotidien/201014/dq201014a-eng.htm

Statistics Canada. (2021, April 1). *Study: Working from home: Productivity and preferences*. Retrieved from https://www150.statcan.gc.ca/n1/daily-quotidien/210401/dq210401b-eng.htm

TransUnion. (2021). *Digital Fraud in 2021*. Retrieved from https://www.transunion.ca/blog/fraud-trends-Q2-2021

U.S. Bureau of Labor Statistics. (2022, January 6). *Number of quits at all-time high in November 2021*. Retrieved from https://www.bls.gov/opub/ted/2022/number-of-quits-at-all-time-high-in-november-2021.htm

Uzialko.A. (2020. March 17). *How Much Time Are Your Employees Wasting on Their Phones*. Retrieved from https://www.businessnewsdaily.com/10102-mobile-device-employee-distraction.html

Valero.A, Riom.C. (2020, September). *The Business Response to Covid-19: the CEP-CBI survey on technology adoption*. Paper No.009. Retrieved from The London School of Economics and Political Science https://cep.lse.ac.uk/pubs/download/cepcovid-19-009.pdf

Wigert.B. (2022. March 15). *The Future of Hybrid Work: 5 Key Questions Answered With Data.* Retrieved from https://www.gallup.com/workplace/390632/future-hybrid-work-key-questions-answered-data.aspx

Willis Towers Watson . (2020. March 5). *North American companies take steps to protect employees from coronavirus epidemic*. Retrieved from https://www.bnnbloomberg.ca/bmo-says-80-of-employees-may-switch-to-blended-home-office-work-1.1431569

Walk-Morris.T. (2020, August 27). *These Industries Are Thriving With A Remote Workforce.* Forbes. Retrieved from https://www.forbes.com/sites/crowe/2020/08/27/these-industries-are-thriving-with-a-remote-workforce/?sh=120e2cfe6587

Whistleblower Info Center. (2021, June 23). *What is the Fraud Triangle?.* Retrieved from https://whistleblowerinfocenter.com/resources/blog/what-is-the-fraud-triangle/

Wiesenfeld.J. (2020, October 5). *COVID-19 challenges to forensic accounting*. Retrieved from https://www.journalofaccountancy.com/newsletters/2020/oct/coronavirus-challenges-forensic-accounting.html

World Economic Forum. (2015). *Deep Shift, Technology Tipping Points and Societal Impact*. Retrieved from https://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf