12-2021

Working from home in the age of COVID-19 and beyond: The Risks, and Benefits to Corporate Information Technology Infrastructure

Jon Nordos

Working from home in the age of COVID-19 and beyond: The Risks, and Benefits to Corporate Information Technology Infrastructure

by

Jon Nordos

A starred paper

Submitted to the Graduate Faculty of

St. Cloud State University

In Partial Fulfillment of Requirements

For the Degree of

Master of Science

In Information Assurance

December, 2021

Starred Paper Committee:
Mark Schmidt, Chairperson
Lynn Collen
Erich Rice

Abstract

In 2020 the COVID-19 viral pandemic circled the globe and impacted the population of the world. Workers who typically commuted to an office were forced to work from home. Faced with concerns such as where they would physically do their work, to who would watch their children during the workday (as schools shut down) societal challenges we have never seen before became a new reality. In a matter of months, infrastructure needs shifted as millions of people no longer commuted to work. Information technology infrastructure, as well as power, internet, and roadway infrastructures all needed to adjust to changes in demand. With many of these changes looking to become permanent, the global information technology security landscape is scrambling to keep up. This paper will discuss the impacts of COVID-19 on many aspects of life, and the impacts they have on information technology security.

Acknowledgements

I would like to thank my committee members Mark Schmidt, Lynn Collen, and Erich Rice. Both as mentors on this final research project, and as professors in several classes, I appreciate all you have taught me.

But most of all, I would like to thank my wife and children. Without my wife Suzanne's sacrifices, and my children's patience, I would not have been able to further my education.

Table of Contents

Chapter Page

List of Tables

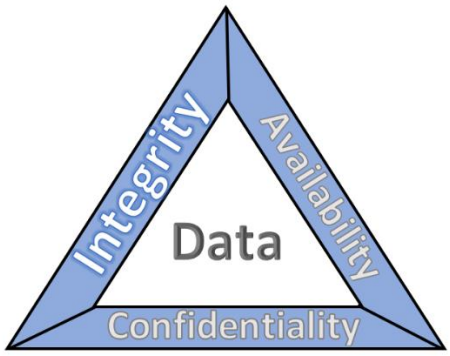
List of Figures

Chapter I: Introduction

According to the National Institute of Standards and Technology (called NIST going forward), the United States based organization that sets technology standards for the United States government, the core goal of information assurance and security is to ensure that information technology systems maintain *Confidentiality*, *Integrity*, and *Availability*. NIST calls this the CIA Triad (Cawthra et al., 2020).

Figure 1

CIA Triad



Note. A representation of the NIST CIA Triad (Cawthra et al., 2020)

Prior to the COVID-19 pandemic of 2020, organizations could focus their finite information technology (called I.T. going forward) security resources on on-premises technology infrastructure. As the pandemic progressed, many in society were asked to quarantine at home. This meant that workers that had the capability of working from home, began doing so. The focus of organizations I.T. staff around the globe had to shift their lines of defense in a short amount of time.

Problem Statement

Prior to 2020, most organizations had the procedural and technological capabilities that would allow *some* employees to work from home. Few organizations, however, had the processes, procedures, and equipment for *most* of their staff to work from home. This paper aims to discuss the risks and benefits to corporate information technology infrastructure as employees working in access-controlled offices, shifted to working from home.

Nature and Significance of the Problem

Late in 2019, COVID-19 began to circulate around the globe. Many in society were concerned with the virus, but few could imagine how quickly our daily lives would change. Using the American State of Minnesota as an example, the governmental response to the pandemic quickly changed how many Minnesotans went about their workday, ate their meals, received their education, and shopped for everyday items. According to an article by Minnesota Public Radio (MPR News Staff, 2021) the timelines of the governmental response to the COVID-19 pandemic are demonstrated in the following table.

Table 1

COVID-19 Timelines

Date	Incident
March 6th, 2020	1st case of COVID-19 reported in Minnesota
March 11th, 2020	The World Health Organization declares COVID-19 a pandemic
March 13th, 2020	The Governor of Minnesota declares a 'Peacetime Emergency'
March 15th, 2020	All schools in Minnesota are asked to close and are given a few days to do so
March 16th, 2020	All bars and restaurants are to shift to 'takeout only'
March 19th, 2020	Minnesota reports their first COVID-19 death
March 25th, 2020	The Minnesota Governor orders all non-essential personnel to stay home

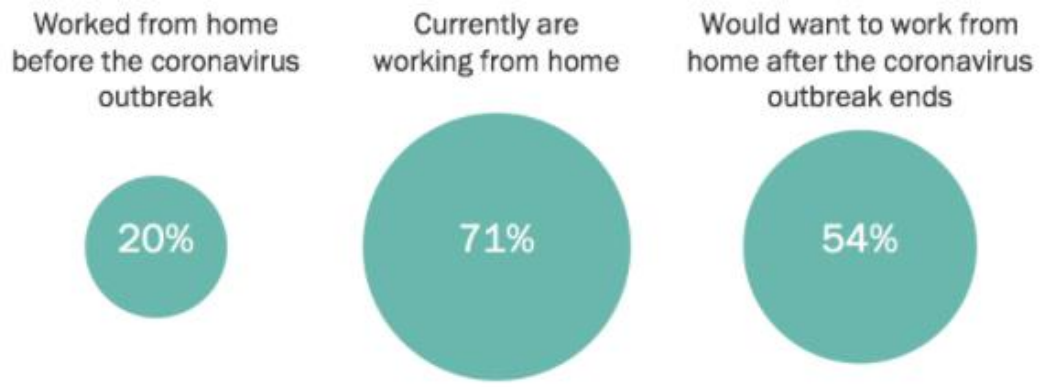
Note. A table representing COVID-19 timelines

As the table shows, there were 19 days from the first reported case of COVID-19 in Minnesota, to an almost complete lockdown of the state. Minnesota, a state with 5.7 million people (America Counts Staff, 2021) and 18 companies listed on Fortune magazine's top 500 list, (Niepow, 2021) staying at home impacted tens of thousands of workers. These workers, many who had been commuting to an office daily were forced to work from home as the state locked down.

According to Pew Research (Parker et al., 2020) prior to the pandemic, around 20% of American workers who could work from home, were working from home on a regular basis. That percentage jumped to over 70% as the pandemic progressed.

Figure 2

Working from home by the numbers



Note. A representation of the % of people working from home (Parker et al., 2020)

With millions of people working from home over the past year and a half we have seen impacts on almost every aspect of our lives. From a global I.T. security standpoint, many organizations have seen substantial increases in cyber threats and alerts. Cisco, a manufacturer of networking equipment, surveyed 3,196 customers around the globe (Future of Secure Remote Work Report, 2021). They reported that most respondents have seen 25% or higher increases in cyber threats or alerts. The graphics below show that this trend is seen across multiple industries.

Figure 3

Increases in Cyber Threats by Industry

Note. A representation of industries seeing increases in cyber threats (Future of Secure Remote Work Report, 2021)

Figure 4

Increases in Cyber Threats by Industry

Note. A representation of industries seeing increases in cyber threats (Future of Secure Remote Work Report, 2021)

As the number of threats has increased, so too have the challenges to I.T. staff everywhere. According to the Cisco report, 97% of American companies responding to their survey indicated they made systemic changes to support remote workers. 57% indicated they believe spending on cyber security will increase in the future.

Objective of the Research

The object of this study is to explore the challenges, risks, and benefits to organizations as the “work from home” models continue to evolve in the time of COVID-19 and beyond. The research will include discussions on operational and personnel impacts of organizations around the world. It will also include impacts on seemingly unrelated areas including real estate, society, the environment, and global infrastructures.

Study Questions

For any organization utilizing technology to manage their information systems, security of digital information is a major concern. NIST defines a *Data Breach* (Cybersecurity Glossary, n.d.) as “The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.” A data breach data loss, and breaches of data can lead to fines, loss of reputation, and potential criminal charges. To organizations in their entirety, I.T. security is just one of the many concerns that come into play. Questions around employee attrition rates and satisfaction, social and environmental responsibility, and overall profitability are also critical.

This research will attempt to answer the following questions as they relate to working from home and the associated security impacts.

- What are the security risks to an organization when employees work from home versus working in an office?

- What are the impacts of working from home on overall productivity?
- What are the impacts on personnel in relation to morale, work life balance, and mental and physical health?
- What are the impacts on society?
- What are the impacts on the environment?
- What are the impacts to organizational assets?
- What are the impacts to business partners and vendors?

Summary

In chapter I we discussed the following:

- *Introduction*: We identified NIST's CIA Triad as the importance of maintaining data's *Confidentiality*, *Integrity*, and *Availability.*
- *Problem Statement:* We identified how, in the face of COVID-19, many organizations have struggled to maintain the CIA Triad.
- *Nature and Significance:* We discussed how organizations had to shift from around 20% of their workforces working from home to 70%. Also discussed where the short timelines organizations had to facilitate the shift to working from home.
- *Nature and Significance:* Research showed that many organizations saw an average of 25% increases in cyber threats and alerts in 2020.
- *Objective of the Research*: We defined the object of the study as: To explore the challenges, risks, and benefits to organizational I.T. security as the "work from home" models continue to evolve the time of COVID-19 and beyond.
- *Study Questions:* We defined the specific questions the research seeks to answer. These are questions around working from homes impacts to: I.T. *Security, Productivity, Personnel, Society, The Environment, Organizational Assets, Business Partners* and *Vendors.*

Chapter II: Areas of concern related to working from home

Introduction

Prior to the COVID-19 pandemic, only the influenza pandemic of 1919, the attack on Pearl Harbor and subsequent entry into World War II, and the 9/11 terrorist attacks had such an immediate impact to the American way of life. However, none of these included such a large shift in how tens of millions of people go about their workday in and day out. With the pandemic, supply chains stopped, public transportation slowed to a crawl, and our personal vehicles sat idle. Commercial real estate capable of housing millions sat empty. Demand for office equipment, printers, electricity, and internet shifted from commercial locations to residences. With the advent of eCommerce years before, society was used to shopping from home, but working from home and schooling our children from home became a new reality many in society were not prepared for.

This chapter will discuss the specific areas that were impacted by tens of millions of people shifting to a model of working from home. It will also discuss the differences in the areas of working from home before and during COVID-19.

Organizational Impacts

As soon as organizations began shifting to a work from home model some impacts were clear and immediate, while others took time to realize. In the following section we will look at the risks to organizational security, and the impacts working from home has had on the number of cyber attacks organizations have faced. We will also

discuss how working from home has impacted organizational policies and procedures, as well as overall organizational productivity.

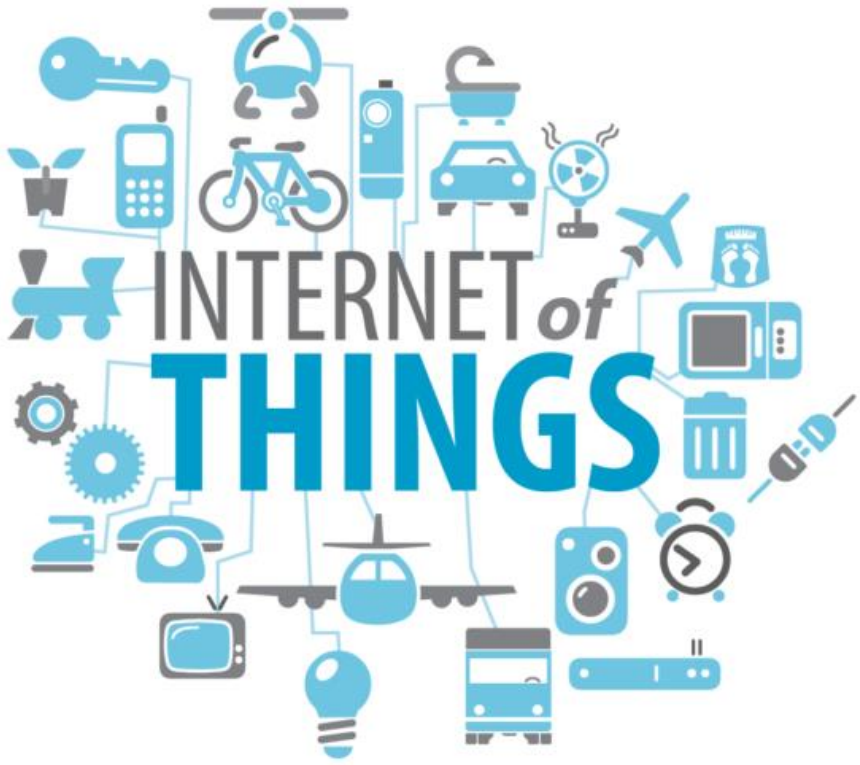
Risks to Organizational Security

In 1998 56-kps modems were becoming the standard (Magid, 1998). This meant that anyone with a telephone line could connect one computer to a remote computer and communicate at 56 kilobits per second. Users were able to connect their home computer to a work network at never-before-seen speeds, all without leaving their homes. Reliable connections with consistent speeds allowed working from home to become a reality. As soon as the first users connected to an organizations network from outside the confines of a controlled office building, new risks were introduced to the security of systems and the data stored on them. In the early days of remote work, there were a minimal number of available connections into corporate networks, and a select number of users with the equipment and knowledge to remotely access those systems. As corporate I.T. Infrastructures began connecting to the internet, anyone with an internet connected device could potentially have access to organizational systems and data. With an estimated 4.66 billion active internet users around the globe (Johnson, 2021), the number of people with potential system access has grown exponentially since 1998. When factoring in that *Internet of Things* (or IoT) devices are estimated to number 35 billion in 2021 (Galov, 2021), the number of connections that can be exploited to illegally access systems is much higher. IoT devices are devices that when connect to the internet can either be controlled or can communicate information over the

internet. Lightbulbs that can be turned on with a cellular phone, sensors that can detect a water leak, and refrigerators that can tell you the weather are all examples of IoT devices. With the average number of IoT devices in U.S. households estimated to be 10 per home in 2020 (Galov, 2021), the number of ways cyber criminals can attempt to connect to user's home network can be substantially higher then when they are working in a controlled office.

Figure 5

IoT Devices



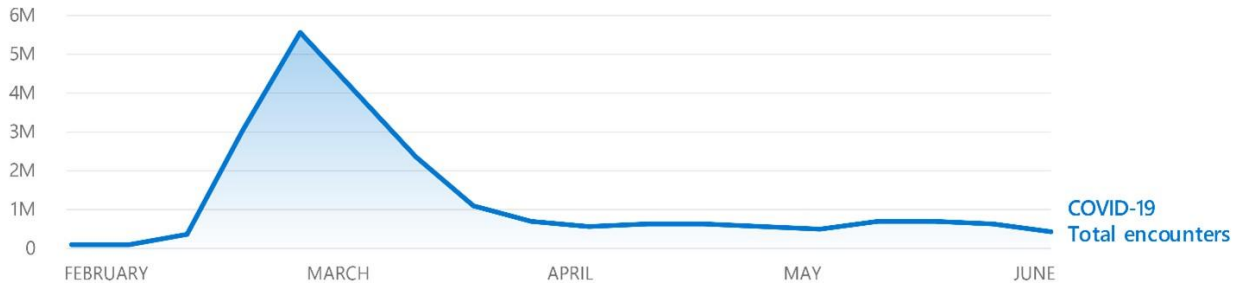
Note. A representation of Internet of Things (IoT) devices (Bly, 2013)

Increased Cyber Attacks within Organizations

In early 2020, as millions of workers shifted to working from home, organizations scrambled to make the changes necessary to allow workers to remotely connect to their office networks. However, as these capabilities expanded, so did the opportunities for unauthorized users to access networks for malicious reasons. In 2020, depending on the attack type, there were double and triple digit increases in cyber attack activity over previous years. A report from Microsoft (Burt, 2020) shows they blocked 13 billion malicious emails out of which 1 billion had web site addresses set up to lure people to bogus COVID-19 websites.

Figure 6

COVID-19 Website encounters



Note. A representation of COVID-19 Website encounters in 2020 (Burt, 2020)

Microsoft also noted a 35% increase in attacks on IOT devices with increases in the complexity of attacks in 2020.

Policy and Process Impacts within Organizations

As millions of users shifted to working from home, the policies, procedures, and equipment needs were overwhelming. I.T. departments scrambled to get people online all while keeping in mind that NIST's security Triad must be maintained. Under normal circumstances, devices would be configured and issued to users, users would receive training around securely connecting to networks, and remote connections would be continually monitored. With little time to prepare, supply chain shortages impacting equipment availability (Dave, 2020), and pressure to resume operations, tens of millions of users were hastily brought online with outdated equipment, little training, and minimal monitoring capabilities. The immediate impacts of bypassing many of the normal processes and procedures appear to have led to an increase in cyber threats and alerts for many organizations.

Impacts on Organizational Productivity

Productivity is of upmost important to any organization. As users shifted to working from home, there were concerns around how productivity would be impacted. A widely cited study conducted by researchers at Stanford University (Bloom et al., 2015) looked at the productivity of call center workers in China from 2010 to 2011. The study's results showed the group of remote workers (working from home) worked 9.2% more minutes per day and took 13% more calls when compared to their counterparts who commuted to the office. Another study from the University of Chicago (Barrero et al., 2021) polled 30,000 U.S. workers inquiring about productivity during COVID-19. The

responses indicated that working from home one day a week boosts productivity an average of 4.8%. However, another study conducted by the World Economic Forum (Fleming, 2021) shows that due to COVID-19 related disruptions during the day, workers have had to work an average of 1 extra hour in each day to maintain previous levels of productivity. Taking COVID-19 out of the equation, studies show that on average workers working from home are more productive than their counterparts working in an office.

Impacts on Corporate Assets and Costs

As workers stopped coming into offices, many of which were in larger urban city centers, the impact to corporate real estate holdings have been dramatic. Per an article from US News (Associated Press, 2021) prior to the pandemic, commercial real estate vacancy rates were between 15% and 16%. Rates have risen to 18.2% and are expected to climb to over 20%. Corporations can, however, also see significant cost savings associated with the maintenance and upkeep of facilities when staff work from home. Several studies, including one from HBF direct, a services consulting company (Companies are Saving Over $1 Billion a Year by Working From Home, 2021), have shown there can be substantial cost savings when not having to maintain office facilities.

As with other impacts, during 2020 many of these impacts have been dramatic, both negative and positive. Only time will tell which changes are permanent as businesses adapt to evolving operational models going forward.

Personnel Impacts

In this section we will discuss how working from home can impact an organizations biggest asset, it's people. In most organizations people program the machines, bring in the customers, and push the buttons that keep organizations moving forward. Without people most organizations would cease to exist.

Impacts on Mental and Physical Health of Personnel

Historically, employees who have chosen to work from home, spend less time commuting, have better work life balance, and show increased rates of morale. As discussed in a Stanford study (Berg, 2019) those working from home have 50% lower attrition rates, take shorter breaks, had fewer sick days, and take fewer days off. There are many studies that show positive impacts of working from home when users have chosen to work remotely. However, what happens when users who do not want to work from home are forced to do so as they were in 2020?

As mentioned earlier, people who like to work from home typically experience better mental and physical health, less stress, and better moral then when they commute to an office. During COVID-19, however, many who were forced home struggled with the idea of being home and not being able to physically interact with coworkers. They found it difficult to separate work and their home life, and many struggled mentally. Under normal, non-COVID-19 circumstances working from home may not be for everyone. With many forced to work from home during COVID-19, mental health issues have become a huge concern over the last 18 months. A journal

article published in the Journal of Occupational and Environmental Medicine (Xiao et al., 2020) found increased instances of decreased overall physical and mental well-being after working from home during the pandemic. The article goes on to discuss stressors such as distractions while working from home, adjusted working hours, as well as issues around where to physically do their work. In short, many have experienced substantial declines in mental and physical health since the start of the COVID-19 pandemic.

Societal Impacts

According to the Census Bureau of the United States (Marshall et al., 2021) levels of education, health, and income can drastically impact who can work from home. As more professional, highly educated people work from home, those in society with lower levels of income and education lack the same opportunity. Some fear that as the gap between the groups grow, more professionals could leave the core cities and migrate to rural areas. This could impact urban schools, crime rates, real estate values and government tax bases. As the tax base of these cities decrease, government agencies could lack the funding necessary to keep their cyber security infrastructure at acceptable levels. This is referred to as the “Cybersecurity Poverty Gap” (Hunt, 2019) and is discussed in an article on Nextgov.com. The article also references a 2018 report from the Office of Management and Budget, and the Department of Homeland Security that found that three out of four federal government agencies had cybersecurity programs either considered at risk, or high risk. With many local and state governments

at even higher risk, widening socio economic gaps could lead to higher crime and increased risks to I.T. security. As most organizations interact with state, local and federal I.T. systems, these increased risks could ultimately impact their security as well.

Impacts on the Environment

The U.S. Department of Transportation showed a total of 213.2 billion vehicle miles traveled on roads and streets in the U.S. in 2020 (May 2020 Traffic Volume Trends, 2020). This represented a decrease of 72.9 billion, or 25.5% from 2019.

Table 2

May 2020 Road and Street Traffic Volume Decreases from 2019

Region	Total Travel	Percentage Change
North-East	26.8	-33.4
South-Atlantic	47.9	-26.1
North-Central	46.2	-26.3
South-Gulf	46.0	-19.8
West	46.3	-24.3

Note. A table representing U.S. traffic volume decreases May – 2019 to 2020

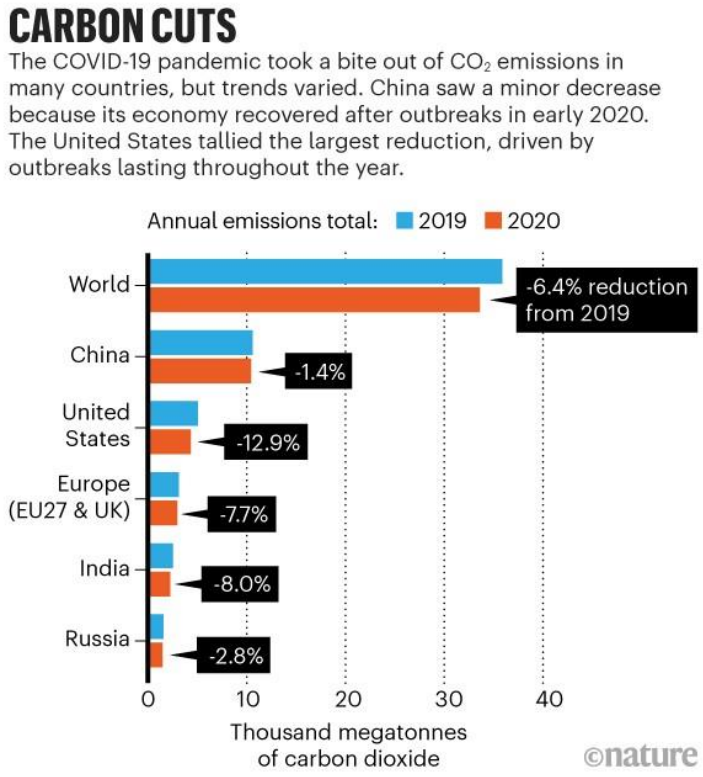
Airline travel was also heavily impacted by the COVID-19 pandemic. According to the U.S. Bureau of Transportation Statistics (2021 Memorial Day weekend middle-distance

travel up from 2019 and 2020, but total trips still down from 2019, 2021) , travel by plane was down substantially during Memorial Day weekend of 2020, the traditional kickoff weekend for summer travel in the U.S. In 2020 travelers took 5.4 billion trips versus 6.9 billion trips in 2019.

2020 reductions in vehicle and airline traffic volume contributed to a 12.9% decrease in carbon emissions in the United States (Tollefson, 2021) in 2020 versus 2019.

Figure 7

Carbon Cuts 2019 to 2020

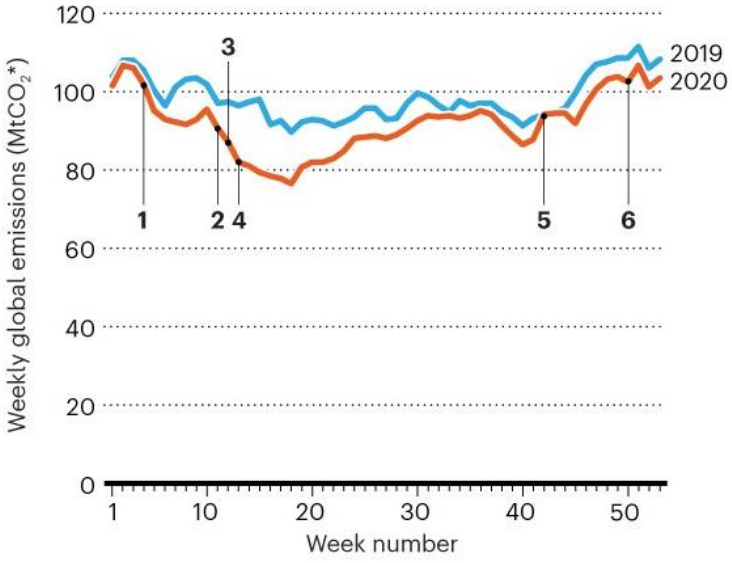


Note. A figure representing global carbon emission reductions from 2019 to 2020

However, air traffic volume increased to 6.1 billion trips for Memorial Day weekend of 2021, an increase of 700 million trips over 2020 (2021 Memorial Day weekend middle-distance travel up from 2019 and 2020, but total trips still down from 2019, 2021). While still below the 6.9 billion trips in 2019, it showed a substantial increase over 2020. Likewise, vehicle travel on roads and streets also increased in 2021. In May of 2021 vehicles traveled 273.9 billion vehicle miles versus 213.2 billion in 2020. While still not at the same levels of 2019 (286.4 billion vehicle miles traveled), 2021 saw substantial increases of road and street vehicle traffic over 2020. With these increases in air and land traffic in the U.S. in 2021, there have also been steep increases in emissions. It is estimated that emissions will rise sharply in 2021 (Tollefson, 2021). With many employers delaying returning to the office until 2022 (Browning et al., 2021), and steep increases in emissions forecasted to close out 2021, the improvements in the environment in 2020 seem to have been short lived.

Figure 8

Emissions 2019 vs 2020



Note. A figure comparing carbon emissions of 2019 and 2020 by week (Tollefson, 2021)

Impacts on Electrical and Internet Utilities

There is little doubt that millions of people no longer commuting to work or sitting in large office buildings would have an impact on utility infrastructure. A report prepared by the International Telecommunications Union from a 2020 roundtable (Economic Impact of COVID-19 on digital infrastructure, 2020) showed that there were dramatic increases in internet usage around the world.

Figure 9

Internet usage increases in 2020

Area	Service provider	Area of usage percent increase	Source
	AT&T (US)	Core network traffic (22%)	AT&T
Telecommunication traffic	British Telecom (UK)	Fixed network traffic (60% on weekdays)	British Telecom
	Telecom Italia (Italy)	Internet traffic (70%)	Telecom Italia
	Vodafone	Mobile data traffic in Italy and Spain (30%)	Vodafone
		Facebook Messenger (50%)	Facebook
Over The Top (OTT)	Facebook	WhatsApp (Overall: 50%; Spain: 76%)	WhatsApp
		Video calling (100%)	Facebook
	Netflix	Subscriber base (9.6% or 16 million)	Netflix
	E-commerce (Mexico)	Number of Users (8%)	Competitive Intelligence
	Zoom	Daily usage (300%)	JP Morgan
Video conferencing	Cisco Webex	Subscribers (33%)	Cisco
	Teams (Italy)	Monthly users (775%)	Microsoft

Note. A representation of increased internet usage during COVID-19

As large commercial buildings the world over closed, energy consumption, however dropped 6% when compared to 2019 (Jiang et al., 2021). This was the largest shock to energy demand in 70 years, and a fall seven times greater than the 2009 financial crisis.

From an organizational I.T. security standpoint, availability of systems to employees is one of the keys areas of the NIST CIA triad discussed earlier. With 66%

increases in internet outages in North America in March of 2020 (Moore, 2020), availability of systems to staff was one of the first obvious negative impacts of working from home.

Summary

In this chapter we discussed the specific impacts that working from home has had on several key areas including:

- *Introduction*: We discussed the scope of the issues to be discussed, historical significance of working from home during COVID-19 and laid out the specific topics we would cover.
- *Risks to Organizational Security:* We discussed the increases in potential risk as the number of ways potential attackers could access organizational systems have increased exponentially as users transition to working from home.
- *Increased Cyber Attacks within Organizations:* We discussed how Microsoft and other organizations have seen increases in attacks, malicious email, and attacks on IoT devices.
- *Policy and Process Impacts within Organizations:* We discussed how changes in policies and processes struggled to keep up with the fast pace of changes during COVID-19.
- *Impacts on Productivity:* We discussed how working from home has had a positive impact on productivity overall. However, many workers have had to work slightly longer hours to offset COVID-19 related distractions.
- *Impacts on Corporate Assets and Costs:* We discussed how working from home has had a positive impact by reducing costs while also having a negative impact

on corporate real estate holdings. Only time will tell which impacts will become permanent.

- *Impacts on Mental and Physical Health of Personnel*: We described how prior to COVID-19, personnel working from home experienced enhanced mental and physical health. However, during COVID-19 many in society have struggled with mental and physical health issues.
- *Societal Impacts*: There are potential negative impacts to some parts of society when working from home. As we discussed, many of the impacts could take several years to assess.
- *Environmental Impacts:* The environment saw large decreases in emissions in the opening months of the COVID-19 pandemic. However, as the pandemic progressed into 2021, many of the decreases have been erased with some forecasts showing higher increases in 2022.
- *Impacts on Electrical and Internet Utilities*: We discussed the impacts on electrical and internet infrastructure. Early in the pandemic outages saw increases impacting the availability of organizational I.T. systems.

Chapter III: Findings

Introduction

This chapter will summarize the overall impacts noted when employees work from home.

Have the risks to I.T. security increased as staff work from home?

There have been double and triple digit increases in global cyber attacks over the past 18 months. However, these do not appear to have led to increases in the number of successful data breaches as breaches in 2020 reached their lowest point since 2016, down 14% from 2019 (2020 Data Breach Report, 2020). The increased attacks appear to be COVID-19 pandemic related and focused on Phishing and Malware. According to Cisco, (What Is a Cyberattack?, 2021) Phishing and Malware were two of the most common types of cyberattacks in 2020. NIST defines *Malware* (Computer Security Resrouce Center - Malware, 2021) as “Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.” NIST defines *Phishing* (Computer Security Resource Center - Phishing, 2021) as “A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.” A journal article (Venkatesha et al., 2021) discuss the prevalence of COVID-19 related malware and phishing attacks during the COVID-19 pandemic. They describe an effective Phishing attack as one that can grab the attention of their victim and get them to respond in one form or another. Prior to the

COVID-19 pandemic, the average internet user had grown accustomed to seeing the typical phishing attacks promising money, or other items. Looking to exploit the fear and anxiety associated with COVID-19, attackers posed as member of the World Health Organization, the U.S. Centers for Disease Control, and others to perpetrate successful attacks. In a multi university research project (Bitaan et al., 2021) there were 2.2 times more victims of phishing attacks in March and April of 2020 than the average month. The report goes on to discuss a massive increase in new, COVID-19 related domain names being created. In early March of 2020, there were 155 Covid related domain names being registered daily. In late March and into April of 2020 , that number increased to 7,453 new domain names being registered per day. As the shift to work from home was made, an unprecedent number of cyber-attacks were hitting the global population and capitalizing on the fear generated by the pandemic.

Impacts on personnel

When considering how working from home impacts I.T. security we must include all the circumstances around our personnel, the single largest risk to our organization's technology infrastructure. The 2015 Stanford study mentioned earlier that looked at working from home in China in 2010 and 2011 (Bloom et al., 2015) will have very different results then a study completed the end of 2020 when the COVID-19 pandemic was at its peak. So too will the study published in April of 2021 (Barrero et al., 2021) showing that the average worker invested 15 hours of time and $561 in home equipment to facilitate working from home. Once employees have invested time and

money into setting up their workspaces and have settled into working from home, many who felt forced to work from home in 2020, will look to have the shift be permanent in 2022.

Research Challenges and Limitations

There were several challenges around finding accurate and consistent information on system breaches and losses of data. Laws such as HIPPA, the Health Insurance Portability and Accountability Act require organizations to disclose breaches of most health data to the United States Department of Health and Human Services. According to the National Conference of State Legislatures, all 50 American states have some form of security breach notification laws (Security Breach Notification Laws, 2021), however, the laws and definitions of what constitutes a breach vary. As do the classifications of breached data, size of companies required to report breaches, etc.

There are two industry respected annual reports on breaches of data in the United States. One of the reports, the *Data Breach Report* generated by the Identity Theft Resource Center is focused on consumer identify theft. The Verizon *Data Breach Investigations Report* is focused on corporate data breaches and security.

- The Identity Theft Resource Center, a nonprofit with many I.T. Security, government, and banking partners generates their annual *Data Breach Report* (2020 Data Breach Report, 2020). They showed 1,108 data breaches in 2020.

- *Data Breach Investigations Report* generated by Verizon (2021 Data Breach Investigations Report, 2021). This report includes full access to dataset's via github.com. Verizon reported 1,037 data breach incidents in small businesses (less than 1,000 employees) and 819 data breach incidents in large business (more than 1,000 employees) in 2020.

Chapter IV: Conclusion

Working from home was forced upon many in society starting in May of 2020. As everyone adapted to the challenges facing the world, the health and safety of the global population became the core priority. Organizations needed to continue operating but keeping everyone alive was the single most important item on the global agenda. As operations transitioned to a work from home model, I.T. security became a secondary priority. With the world's population scared for their lives, once diligent employees clicked links sent by cyber criminals, opened fraudulent text messages to "schedule a vaccination", and navigated to fraudulent websites to find more information about COVID-19. Society was scared, careless and focused on ending the pandemic. Cyber criminals seized onto people's fears and attempted to take advantage of the situation.

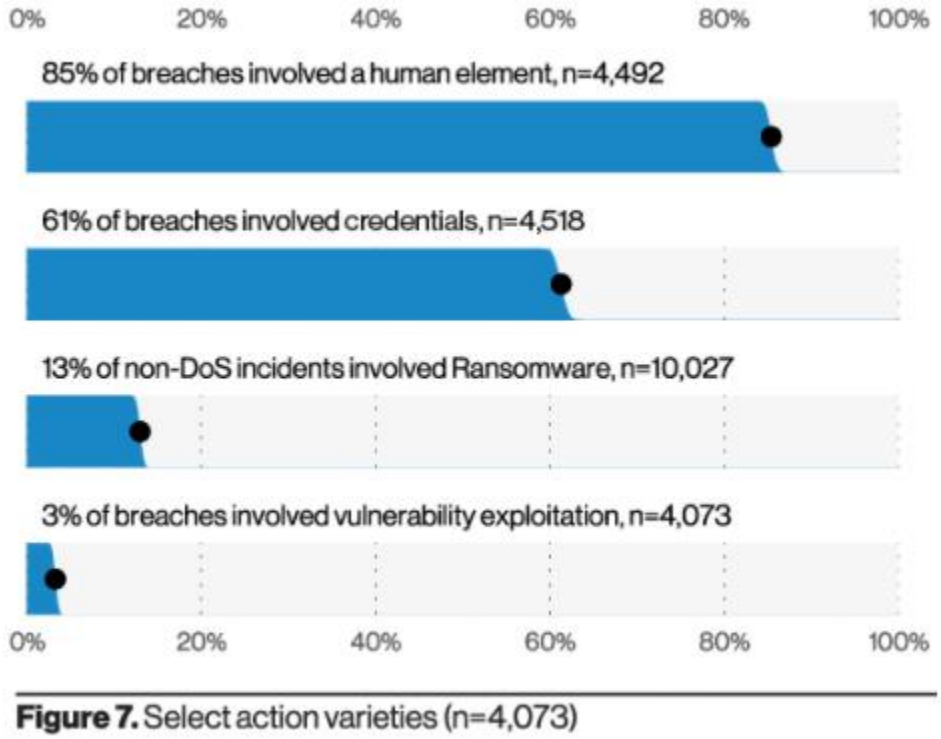
2020 was a wakeup call in many ways. From the fragile nature of global supply chains to the security of our I.T. infrastructure, the rapid shift in the way people live and work had made an impact. Historically many organizations had underfunded their I.T. security efforts. But going forward, this appears to be changing. Gartner, a leading I.T. research firm, estimates spending on worldwide I.T. security and risk management will exceed $150 billion in 2021, a 12.4% increase over 2020 (Moore, 2021).

The question remains, does working from home make organizations I.T. infrastructure less secure? Ultimately the answer involves looking at the single common factor between working in an office and working from home: People. According to data released by the UK's Information Commissioners office (Ingham, 2018), 88% of UK data

breaches were caused by human error. The DBIR report by Verizon (2021 Data Breach Investigations Report, 2021) shows that in the United States, 85% of breaches involved a human element.

Figure 10

Human Factor in UK breaches



Note. A representation of the % of breaches caused by humans in the UK (Ingham, 2018)

Another study conducted by Stanford University Professor Jack Hancock and security firm Tessian (Hancock, 2020) showed that 93% of workers say they were tired and stressed at some point during the week in 2020. When you consider the percentage of human issues around cyber attacks and the physiological impacts of COVID-19 over the last 18 months, the stresses the general populace have been under cannot be overstated.

Closing

Research found little data tying working from home to any documented security breaches. Human mistakes continue to be the biggest threat to global I.T. security. With the potential benefits of working from home to productivity, employee attrition rates, and operational costs exceeding the risk to I.T. security, many may continue to work from home even as the COVID-19 pandemic subsides. However, as more staff work from home, cyber criminals will place more emphasis on attacking home devices, specifically IoT devices and home networking equipment. Continued research around security impacts of home office environments and equipment must continue to grow. Employee education and security policy updates must evolve to keep pace with the working environments, risks, and equipment associated with any organization’s I.T. infrastructure. This must also include employee home office environments.

Definition of Terms

- **COVID-19 Pandemic:** In late 2019 a viral pandemic circled the planet and impacted daily life for the global population.
- **Information Technology**: Called I.T. going forward, is any system used to store, retrieve, or transmit information. This can include computers, cellular phones, networks and more.
- **NIST:** The National Institute of Standards and Technology is the organization that sets technology standards for the United States Government. Many organizations follow NIST Information Technology standards as best practices.
- **CIA Triad:** The CIA Triad is a NIST standard. It stands for Confidentiality, Integrity, and availability. The goal of any
- **Cyber threats and alerts:** Any threat to I.T. and an accompanying notification (alert) in systems designed to identify incoming cyber threats.
- **Work from home:** Working from home is when organizational staff work out of their home as opposed to working in an organizational office.
- **Remote workers:** Any worker who is working from somewhere other than a traditional, access controlled on premise corporate or organizational office space.
- **kilobits per second:** A measure of the speed of transferring data. In 1998 56 kbps was considered high speed. Home internet speeds in 2021 exceed 100

megabits per second. There are 1000 kilobits in 1 megabit, so todays speeds are significantly higher.

- **Internet of Things devices:** Called IoT - are devices that when connect to the internet can either be controlled or can communicate information over the internet. “Smart” devices (TV’s, thermostats, and lights) are examples.
- **Breach:** The unauthorized transfer of information from an information system.

References

2020 Data Breach Report. (2020). ID Theft Center. Retrieved October 1, 2021, from https://notified.idtheftcenter.org/s/2020-data-breach-report

2021 Data Breach Investigations Report (2021). Verizon. Retrieved October 10, 2021, https://www.verizon.com/business/resources/reports/dbir/

2021 Memorial Day weekend middle-distance travel up from 2019 and 2020, but total trips still down from 2019. (2021, June 17). Bureau of Transortation Statistics. Retrieved from https://www.bts.gov/data-spotlight/2021-memorial-day-weekend-middle-distance-travel-2019-and-2020-total-trips-still

America Counts Staff. (2021, August 25). *Minnesota's Population at 5,706,494 in 2020, Up 7.6% Since 2010.* Census.gov. Retrieved September 19, 2021, from https://www.census.gov/library/stories/state-by-state/minnesota-population-change-between-census-decade.html

Associated Press. (2021, April 8). *Pandemic Impact May Weigh on Commercial Real Estate Recovery.* USNews. Retrieved October 17, 2021, from https://www.usnews.com/news/business/articles/2021-04-08/pandemic-impact-may-weigh-on-commercial-real-estate-recovery

Barrero, J. M., Bloom, N., & Davis, S. J. (2021, April). *Why Working From Home Will Stick* (Working Paper No. 2020-174). Retrieved from the University of Chicago, Becker Freidman Institute: https://bfi.uchicago.edu/wp-content/uploads/2020/12/BFI_WP_2020174.pdf

Berg, A. (2019, January 18). *A Stanford University study debunks misconceptions about working remotely*. Solidariteit. Retrieved October 10, 2021, from https://jouwerk.solidariteit.co.za/en/a-stanford-university-study-debunks-misconceptions-about-working-remotely/

Bitaan, M., Cho, H., Oest, A., Zhang, P., Sun, Z., Pourmohamad, R., . . . Ahn, G.-J. (n.d.). *Scam Pandemic: How Attackers Exploit Public Fear through Phishing.* Retrieved October 19, 2021, from ftc.gov: https://www.ftc.gov/system/files/documents/public_events/1582978/scam_pandemic_how_attackers_exploit_public_fear_through_phishing.pdf

Bloom, N., Liang, J., Roberts, J., & Ying, Z. (2015). The Quarterly Journal of Economics: Volume 130, issue 1. *Does Working from Home Work? Evidence from a Chinese Experiment*, 165–218. https://doi.org/https://doi.org/10.1093/qje/qju032

Bly, J. (2013, December 27). *Connected Devices Accelrate the Needfor IPv6 in the Internet of Things.* Arin.net. Retrieved October 21, 2021, from https://www.arin.net/blog/2013/12/27/connected-devices-accelerate-the-need-for-ipv6-in-the-internet-of-things/

Browning, K., Hirsch, L., & Murphy Marcos, C. (2021, September 6). *Why You Might Not Be Returning to the Office Until Next Year.* New York Times Retrieved October 21, 2021 from https://www.nytimes.com/2021/09/06/business/rto-return-to-office.html

Burt, T . (2020, September 29). *Microsoft report shows increasing sophistication of cyber threats*. Microsoft. Retrieved October 17, 2021, from https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J., Sweetnam, J., & Townsend, A. (2020, December). *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events.* nncoe.nist.gov. Retrieved November 11, 2021, from https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect.

Companies are Saving Over $1 Billion a Year by Working From Home. (2021, April 30). HBDirect. Retrieved October 10, 2021, from https://www.hbfdirect.com/companies-are-saving-over-1-billion-a-year-by-working-from-home/

Computer Security Resource Center - Phishing. (2021, October). Cstc.Nist. Retrieved October 10, 2021, from https://csrc.nist.gov/glossary/term/phishing

Computer Security Resrouce Center - Malware. (2021, October). Cstc.Nist. Retrieved October 10, 2021, from https://csrc.nist.gov/glossary/term/malware

Cybersecurity Glossary. (n.d.) Niccs.cica.gov. Retrieved November 1, 2021, from https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#:~:text=Definition%3A%20The%20unauthorized%20transfer%20of,in%20violation%20of%20security%20policy.

Dave, P. (2020, December 4). *Laptops, desktop sales see 'renaissance;' shortages won't ease until 2022.* Reuters. Retrieved October 1, 2021, from https://www.reuters.com/article/us-tech-hardware-yearend/laptops-desktop-sales-see-renaissance-shortages-wont-ease-until-2022-idUSKBN28Y12M

Economic Impact of COVID-19 on digital infrastructure. (2020). International Telecommunucation Union. Retrieved November 10, 2021, from https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.COV_ECO_IMPACT-2020-PDF-E.pdf

Fleming, S. (2021, September 6). *Remote working - does it make us more or less productive?* Weforum. Retrieved October 10, 2021, from https://www.weforum.org/agenda/2021/09/remote-working-hybrid-productivity/

Future of Secure Remote Work Report. (2021, April 22). Cisco. Retrieved November 3, 2021, from https://www.cisco.com/c/en/us/products/security/future-secure-remote-work-report.html

Galov, N. (2021, October 2). *How Many IoT Devices Are There in 2021? [All You Need To Know]*. Techjury. Retrieved October 17, 2021, from https://techjury.net/blog/how-many-iot-devices-are-there/#gref

Hancock, J. (2020). *Physcology of Human Error. Understand the mistakes that compromise your companies security.* Tessian. Retrieved October 17, 2021, from https://f.hubspotusercontent20.net/hubfs/1670277/%5BTessian%20Research%5D%20The%20Psychology%20of%20Human%20Error.pdf

Hunt, G. (2019, July 18). *Closing the Cybersecurity Poverty Gap.* Nextgov. Retrieved September 1, 2021, from https://www.nextgov.com/ideas/2019/07/closing-cybersecurity-poverty-gap/158414/

Ingham, L. (2018, September 3). *88% of UK data breaches caused by human error, not cyberattacks*. Verdit.co.uk. Retrieved October 10, 2021, from https://www.verdict.co.uk/uk-data-breaches-human-error/

Jiang, P., Fan, Y. V., & Klemeš, J. J. (2021). Applied Energy: Volume 285, Issue 1. *Impacts of COVID-19 on energy demand and consumption: Challenges, lessons and emerging opportunities.* https://doi.org/10.1016/j.apenergy.2021.116441

Johnson, J. (2021, September 10). *Global digital population as of January 2021*. Statista. Retrieved October 1, 2021, from https://www.statista.com/statistics/617136/digital-population-worldwide/

Magid, L. (1998, September 28). *The new V.90 standard makes modem life easier*. Los Angeles Times. Retrieved December 6, 2021, from https://www.latimes.com/archives/la-xpm-1998-sep-28-fi-27214-story.html.

Marshall, J., Burd, C., & Burrows, M. (2021, March 31). *Those Who Switched to Telework Have Higher Income, Education and Better Health.* U.S. Census.

Retrieved October 2, 2021, from https://www.census.gov/library/stories/2021/03/working-from-home-during-the-pandemic.html

May 2020 Traffic Volume Trends. (2020). U.S. Department of Transportation. Retrieved November 1, 2021, from https://www.fhwa.dot.gov/policyinformation/travel_monitoring/20maytvt/

Moore, M. (2020, August 5th). *Internet outages have seen major increase during pandemic.* IT Portal. Retrieved October 10, 2021, from https://www.itproportal.com/news/internet-outages-have-seen-major-increase-during-pandemic/

Moore, S. (2021, May 17). *Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021.*Gartner. Retrieved October 17, 2021, from https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem

MPR News Staff. (2021, November 3). Timeline: Covid-19 in Minnesota. MPR News. Retrieved November 17, 2021, from https://www.mprnews.org/story/2021/03/06/timeline-covid-19-minnesota

Niepow, D. (2021, June 03). *Two More Minnesota Companies Added to Fortune 500 List.* Retrieved September 10, 2021, from tcbmag.com: https://tcbmag.com/two-more-minnesota-companies-added-to-fortune-500-list/

Parker, K., Menasce Horowitz, J., Minkin, R. (2020, December 9). *How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work.* Retrieved September 10, 2021, from https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/

Security Breach Notification Laws. (2021, April 15). NCSL. Retrieved October 10, 2021, from https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Tollefson, J. (2021, January 15). *COVID curbed carbon emissions in 2020 — but not by much.* Nature. Retrieved October 19,2021, from https://www.nature.com/articles/d41586-021-00090-3

Venkatesha, S., Reddy, K.R. & Chandavarkar, B.R. (2021, March 11) SN Computer Science. *Social Engineering Attacks During the COVID-19 Pandemic*. Article 78. Retrieved on October 21, 2020, from https://doi.org/10.1007/s42979-020-00443-1

What Is a Cyberattack? (2021, October). Cisco. Retrieved October 10, 2021, from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Xiao, Y., Becerik-Gerber, B., Lucas, G., & Roll, S. C. (2021). Journal of Occupational and Environmental Medicine: Volume 63, Issue 1. *Impacts of working from home during COVID-19 pandemic on physical and mental well-being of office*

workstation users. , Volume 63 issue 3, 181-190.

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7934324/