Modifying Knowledge Risk Strategy Using Threat Lessons Learned from COVID-19 in 2020-21 in the United States

Murray E Jennex[1], Alexandra Durcikova[2] and Ilona Ilvonen[3]
[1]Paul and Virginia Engler College of Business, West Texas A&M University
[2]Price College of Business, University of Oklahoma
[3]Unit of Information and Knowledge Management, Faculty of Management and Business, Tampere University
[1]ORCID 0000-0003-4332-1886
[2]ORCID 0000-0002-6705-202X
[3]ORCID 0000-0002-2418-9077
mjennex@wtamu.edu
alex@ou.edu
Ilona.ilvonen@tuni.fi

Abstract: 2020 and 2021 have shown us that the likelihood of extreme events is more significant than we would have expected. Due to extreme circumstances, organizational resources are stretched to their limits, making organizations more vulnerable to attacks affecting their knowledge systems and knowledge assets. This paper conducts an intelligence-based threat assessment by analyzing published reports on events during the 2020-21 period against a set of five knowledge risks to identify threats and determine if they increase the likelihood of these risks occurring. We identify six possible changes in knowledge risk strategy to mitigate these threats: proper knowledge identification, guidelines for employee online behavior, identification and evaluation of online communication channels, re-evaluation of how work is to be performed, creation of knowledge capture processes for departing personnel, and performing a knowledge risk re-assessment. Additionally, we conclude that organizations need expertise in identifying and countering misinformation and disinformation to defend themselves from these new cyber threats.

Keywords: Knowledge Risk, Risk Assessment, Knowledge, Threats, COVID-19, Knowledge Systems, Knowledge Transfer

1. Introduction

2020 was a year of upheaval and unrest (Gat Labs, 2020) that has continued to impact us through 2021 and into 2022. COVID-19 swept the world and shut down many countries, and once it seemed that COVID-19 was receding, we were hit by the Delta and Omicron variants of the virus. In addition to COVID-19, the United States has experienced various difficulties. These include:

- Widespread civil strife with rioting in many cities beginning in the spring of 2020.
- Multiple natural disasters such as several large wildfires in California, a severe hurricane season that affected the southeast United States, and a record polar freeze that knocked out the Texas power grid during record freezing temperatures in the winter of 2021.
- A controversial presidential election.
- Multiple cyber-attacks that affected hospitals, financial systems, and production systems in food process and gas pipeline transport.
- Widespread misinformation/disinformation campaigns about the election and the COVID-19 vaccine (Parakilas, 2020).
- The great resignation during the second half of 2021(Luze, 2021).

These events challenged our understanding of knowledge risks and threats, and our strategies and approaches for managing them. Therefore, we need to summarize what was learned about knowledge threats from 2020 through 2021 and suggest how knowledge risk strategies should be modified. Thus, our research question is: "How should knowledge risk strategies be modified based on the new knowledge threats from 2020-21?"

While businesses and organizations faced many traditional security issues during the lockdowns and other crises of 2020 and 2021 (such as logj4 and SolarWinds), this paper is not about those issues. Our analysis focuses on threats we had not considered when the pandemic started. We identify these threats as:

- Increased frequency of misinformation

Reference this paper: Jennex, M. E., Durcikova, A., and Ilvonen, I., 2022. Modifying Knowledge Risk Strategy Using Threat Lessons Learned from COVID-19 in 2020-21 in the United States. *The Electronic Journal of Knowledge Management,* 20(3), pp. 138-151, available online at www.ejkm.com

- Increased frequency of disinformation
- Increased reliance and use of social media
- Increased social isolation of remote working employees
- Increased social justice movement
- Increased transience of knowledge workers due to the great resignation
- Increased frequency of large-scale natural disaster events

Our previous research discussed a generic set of knowledge risks and threats (Jennex and Durcikova, 2020); however, we did not anticipate how COVID-19 and the events of 2020-21 effected the above threats and ultimately knowledge risk. This paper discusses primarily the changes in frequency of these threats based on published surveys and reports focusing on the issues observed during the COVID-19 pandemic and other natural disasters in 2020 and 2021.

The rest of this paper is organized as follows: a background section that discusses terms use, COVID-19, other crises during 2020-21, and knowledge risk assessment; a section discussing the specific threat lessons learned from 2020-21; a section discussing how knowledge risk strategies need to be changed; and conclusions.

2. Background

In this section, to establish a common ground, we start with the definitions of terms used in the article. Then, we will explain the COVID-19 context that enabled new knowledge threats. To fully describe the context of our investigation, we also represent other crises during 2020 and 2021. Finally, we review the current literature on knowledge system risk assessment.

2.1 Definitions of terms used in the paper

Misinformation - is false, inaccurate, or misleading information communicated regardless of an intention to deceive. (Wikipedia, 2021a). Managing the spread of misinformation has become a contentious issue due to who decides what misinformation is, what is an opinion, and what is truth.

Disinformation - is false information intended to mislead, especially propaganda issued by an organization to a rival power or the media (Wikipedia, 2021b). Disinformation is a subset of misinformation, with the key difference being the intent to deceive.
Knowledge – is an evolving mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences into corporate decision-making (Davenport and Prusak, 1998). Knowledge is used to support decision-makers.

Knowledge Transfer - refers to the sharing or disseminating of knowledge by a knowledge creator (Alavi and Leidner, 2001). Knowledge transfer is vital in knowledge systems and relies on trusted creators of knowledge moving that knowledge to repositories where knowledge users can retrieve and use it.

Knowledge System/Knowledge-Based System – is a system that captures and uses knowledge from various sources to assist users with solving problems. These systems are primarily used to support human decision-making, learning, and other activities (Nissen, 2002).

Risk – is the net negative impact of the exercise of a vulnerability considering both the probability and the impact of occurrence (National Institute of Standards and Technology, NIST SP800-37, 2018). The negative impact of occurrence is defined in terms of the impact on the confidentiality-integrity-availability triangle. Usually, it looks at a loss or degradation of any combination of these impacts (Samonas and Coss, 2014). The impact of occurrence considers the likelihood of the risk can be broadly viewed as the likelihood of a hazard, an uncertainty, or an opportunity (Billington, 1997). Viewing risk as something more than a hazard is highly applicable to knowledge systems (Jennex and Durcikova, 2014). Additional discussions on knowledge risks come from Durst and Zieba (2019), who list 26 risks that affect knowledge and the five risks listed by Jennex and Durcikova (2020). Durst and Zieba's (2019) 26 risks are a mix of cybersecurity risks and knowledge risks, while the five knowledge risks of Jennex and Durcikova (2020) are focused solely on the misuse of knowledge as discussed by Walsh and Ungson (1991). Ultimately, the knowledge risks of Durst and Zieba (2019) and Jennex and Durcikova (2020) overlap. Further on risk, as KM relies on technologies for most KM processes, it is challenging to separate cybersecurity risks from knowledge risks (Durst and Zieba, 2019. Jennex and Durcikova,

2020). This paper discusses cybersecurity risks as aspects of knowledge risks, with the focus of the paper being on the threats that impact knowledge use. NOTE: we use National Institute of Standards and Technology, NIST, standards to define terms for three reasons: NIST standards are a partnership between academics, practitioners, and Government; the standard development process is a KM process using an expert panel to generate the standard that is then put out to the public comment before publication; and, NIST standards are available for free.

Threat – is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, misinformation/disinformation, and/or denial of service (NIST, 2012).

Threat assessment - is the process of identifying threats that could cause risks to occur. Threat assessment uses as one of its tools in the process of threat hunting.

Threat hunting - is gathering and analyzing events' data, hypothesizing how the events could lead to increased risk, and testing the hypotheses (Bhardwaj and Goundar, 2019). This paper investigates data identified from the events of 2020-21 and hypothesizes how these events could increase the probability of the stated threats.

2.2 COVID-19

2020 was challenging for every country because of the global pandemic caused by COVID-19. As of August 3, 2022, the Covid-19 Healthdata reports that the United States has had 91.6 million cases of COVID-19, with 1.03 million reported deaths (IHME, 2022). Worldwide, Wikipedia (based on Johns Hopkins data) says there have been 579 million cases of COVID-19 with 6.41 million deaths (Our World in Data, 2022). To combat COVID-19, the United States and much of Europe, Asia, and Australia went through a series of shutdowns of most business and social operations. A rapid transition to online media and communication eased the problems these shutdowns created. Social media (Facebook, Instagram, TikTok, Twitter, etc.) and collaboration systems (Zoom, Teams) enabled communications between large numbers of people but with little content moderation. This leads to concerns about the spread of misinformation/disinformation and increased cyber-attacks via phishing and social engineering through social media and traditional email and text communications.

The following are some of the observed outcomes of moving business and life online:

- Workers and students spent extended time working remotely, using their private Internet connections rather than those provided by their organization or school (Kelly, 2021).
- Businesses, organizations, and schools moved business processes online.
- Payment systems went touchless/contactless.
- Tools such as Zoom and Teams were quickly adapted and used (Kelly, 2021).
- Travel and supply chains were disrupted.
- Social media such as Facebook, YouTube, Instagram, Twitter, and Tik Tok became the primary means of social interaction and sources of information.
- Most face-to-face communication outside of immediate family units ceased.

Shutdowns also led to the loss and transience of employees. Many businesses had to lay off employees when they could not continue operations. In addition, many employees left on their own during the great resignation due to burnout. This resulted in a loss of knowledge flow from departed employees and knowledge sharing among remaining employees (both face-to-face and remote). As operations are resuming, businesses are suffering from not enticing former employees to return or hire new, experienced employees, resulting in many organizations losing critical organizational knowledge. To counter the loss of organizational knowledge and knowledge sharing, organizations and businesses used knowledge systems to manage the storage, retrieval, and application of business and organizational knowledge. These knowledge systems had to be remotely accessed by employees during shutdowns. Security issues during the early part of the pandemic forced firms and organizations to defend their knowledge systems (to some degree) from cyber threats using best practices and risk assessments such as:

- Protect their boundaries, repositories, and equipment.
- Monitor for and respond to attacks and intrusions.
- Monitor and guard against phishing and other social engineering attacks.

- Be prepared for disaster response/business continuity.

Organizations and businesses also reduced risk to their knowledge systems by monitoring and guiding remote users on how to connect, what information systems to use, online behavior rules, and configuring the employees' home computers. However, businesses were unprepared for the large-scale remote access and remote system use experienced last year.

Remote work caused employees to communicate with others they did not know in a virtual environment. Virtual environments significantly reduced body language feedback and influence by organizational/corporate behavior rules with the following outcomes:

- COVID-19, social, and election misinformation and disinformation were rampant.
- Social justice, social change and upheaval have caused great uneasiness in organizations causing employees to be afraid to express thoughts or opinions for fear of being "canceled."
- Social engineering and phishing attempts have become the prevalent cyber-attack vector (Columbus, 2021).

However, 2020 and 2021 also presented organizations and companies with remote work issues and increased cybersecurity attacks and threats. These are discussed next.

2.3 Other Crises From 2020-21

COVID-19 was not the only event in 2020-21 that increased knowledge threats. The leading causes of increased knowledge threats were (1) natural disasters such as hurricanes, wildfires, and arctic cold; (2) cyber-attacks through ransomware and hastily implemented technology to support remote workers; (3) social upheaval from elections and riots; (4) misinformation/disinformation campaigns; the great resignation. These events generated more uncertainty and stress overall in organizations and individuals than had been previously experienced since perhaps the great depression. The uncertainty associated with knowledge use is one of the biggest challenges a knowledge system manager faces. This uncertainty can stem from rapidly changing technology and storage media, misuse of new and unexpected uses of knowledge, the basic understanding of the captured knowledge, or the loss of knowledge. Below are some threat issues that arose from these other issues in 2020-21.

- Misinformation/disinformation impacts procedural decision-making on hiring, purchasing, and customer service. This can lead to security issues such as internal threats, transferring funds to the wrong bank, or offending customers (Nabe, 2021).
- Misinformation/ disinformation leads to bad individual decision-making regarding which links to click on or which email to open. Misinformation/disinformation leads to many data breaches caused by human error due to phishing and other errors. The largest Twitter and Facebook hack in 2020 was caused by Twitter and Facebook employees falling for a phishing attack (Gat Labs, 2020; Newman, 2021; Osborne, 2021; Vijayan, 2020). The same is true for the increased ransomware attacks (Ponemon, 2021).
- Hundred-year storms (Texas recently, southeast over the late summer, California wildfires) challenge disaster recovery plans and potentially loss of knowledge; they influence the availability of systems (Alonso and Sanchez, 2020; Gramling, 2020; Timmer, 2021).
- The great resignation in the summer and fall of 2021 resulted in over 19 million people in the United States quitting their jobs (Luze, 2021) and causing larger than expected personnel turnover and knowledge loss, degrading organizational performance
- Organizational culture changes lower trust among workers resulting in less knowledge sharing and, most importantly, less sharing of knowledge critical to decision-making affecting security (bad sites, hacking attempts, social engineering, etc.)
- Organizational members upset at culture changes deliberately do not share knowledge or share disinformation leading to bad decision making
- Social isolation slows the sharing, capturing, and reusing knowledge needed for security decisions.
- Social isolation increases the use of social media leading to more potential disclosures, more opportunities for downloading malware onto worker computers used for home and work, and lower filters for determining misinformation/ disinformation (Vijayan, 2020).
- Generation Z felt the impact of the above issues more than any other group (Sherr, 2021).

The following section analyzes these observations using the threat vectors mentioned earlier.

2.4 Knowledge system risk

Assessing cybersecurity in the organization starts with threat assessment (NIST, 2012). Jennex and Durcikova (2020) discuss risk and threat assessment specific to knowledge systems and build the theoretical foundation for knowledge system threat assessment. In this paper, we apply this foundation in analyzing the events of the recent year 2020-21.

The knowledge system risks are assessed using the Knowledge Security Risk Management approach of Ilvonen, Jussila, and Kärkkäinen (2015) for knowledge security risk management. Ilvonen, Jussila, and Kärkkäinen (2015, p.13) define knowledge security "as the managerial process of organizations to identify threats toward important knowledge and secure the knowledge against those threats."

The point of interest in this definition is essential knowledge: the knowledge that is important to the organization needs to be identified in all the forms and locations that it resides in for the organization to be able to do any risk management measures with it. The knowledge risk assessment process thus begins with identifying knowledge assets by recognizing not only the documented knowledge within different systems of the organization but also the ways of knowledge sharing and transfer and the role of people and tacit knowledge within the knowledge system.

Jennex and Durcikova (2020) present a set of knowledge system-specific risks that need to be threat assessed by each organization. The six risks are:

- Failure to identify and capture critical knowledge in the knowledge creation process.
- Not having knowledge creation, capture, and use aligned with organizational strategy.
- Disclosing critical knowledge to unauthorized recipients in the knowledge sharing processes.
- Losing critical knowledge by not capturing it from critical human sources.
- Losing critical knowledge by not storing it on nonvolatile media, not migrating knowledge with changing storage standards, or not meeting legal standards for storing essential knowledge.
- Giving bad advice by not using appropriate knowledge or by using inappropriate knowledge.

Jennex and Durcikova (2020) provided an in-depth discussion and many examples of how the above risks have threats that impact knowledge systems. However, in 2020-21, because of COVID-19, natural disasters, social upheaval, misinformation, etc., generated more uncertainty and stress that resulted in increased threats in organizations and individuals than had previously experienced since perhaps the great depression.

The uncertainty associated with knowledge use, be it due to rapidly changing technology and storage media, misuse or new and unexpected uses of knowledge, or the basic understanding of the captured knowledge, is one of the biggest challenges a knowledge system manager faces. The following section will analyze the impact of this uncertainty and stress, events, and outcomes from 2020 and 2021 using the above knowledge system threats and the previously discussed process.

In addition to identifying the vital knowledge of an organization, risk assessment requires understanding where the threats can enter the organization and target the knowledge system. This paper uses three threat vectors: technical, behavioral, and legal (Jennex and Durcikova, 2020).

3. Methodology

Jennex and Durcikova (2020) created a generic set of risks for knowledge systems using basic knowledge system processes of knowledge (creation, sharing, and management). We then added misuse risks from Walsh and Ungson (1991):

- Automatic retrieval of knowledge may lead to a routine decision response when a non-routine decision response is warranted.
- The controlled retrieval of knowledge may lead to a non-routine decision response when a routine decision response was appropriate.
- A controlled retrieval of knowledge may be appropriately activated to elicit a non-routine decision response, but it may be implemented poorly.

Misuse of knowledge occurs when organizational members self-serving select knowledge to support positions that serve their political needs rather than the organization's (Walsh and Ungson, 1991).

Using Spears' (2012) misuse cases, we analyzed the above misuses to generate the following six knowledge systems-specific risks:

- Failure to identify and capture critical knowledge in the knowledge creation process.
- Not having knowledge creation, capture, and use aligned with organizational strategy.
- Disclosing critical knowledge to unauthorized recipients in the knowledge sharing processes.
- Losing critical knowledge by not capturing it from critical human sources.
- Losing critical knowledge by not storing it on nonvolatile media, not migrating knowledge with changing storage standards, or not meeting legal standards for storing essential knowledge.
- Giving bad advice by not using appropriate knowledge or by using inappropriate knowledge.

Misuse cases were used as they are an accepted technique for modeling how either outside users or actual users can abuse information systems/knowledge systems. Each of the knowledge systems' specific risks was then analyzed using intelligence threat hunting with three possible threat vectors (i.e., sources of attacks): technology, behavioral, and regulatory-based attacks applied to knowledge system processes (creation, storing, sharing, and management) to generate a set of knowledge system-specific generic threats. The six knowledge specific risks are listed in section 2.4 above

Hazel (2021) defines threat hunting as a purposeful and structured search for evidence of malicious activities that have not yet generated security alerts. This study uses published reports on COVID-19 issues identified through a Google search (using terms such as COVID-19 lessons from 2020, COVID-19 lessons from 2021, cybersecurity lessons from 2020, and cybersecurity lessons from 2021). We used these popular sources rather than those published in scientific journals to identify events/activities that have not yet been linked to knowledge risks. We decided to take this path because of the nascent state of research in the area of knowledge risks and because we wanted to implement the most recent events that have not been analyzed in scientific journals yet. Keeping in mind that not all popular sources are of equal quality and reliability, we focused on mainline American news outlets (e.g., sources such as Associated Press, Forbes, Wired, etc.).

4. Analysis of events and observations of 2020-21

Obasiolu (2020) found the biggest cybersecurity lesson from 2020-21 is that security starts within an organization. Specifically, security starts with top management creating a security culture and expectations of secure behavior. While we agree with this observation, we provide additional and more concrete observations below and specify how they create technical, behavioral, and legal threats to an organization. This section analyzes threats from 2020-21 with respect to the knowledge system/knowledge risks listed in 2.4 above with the exception of not having knowledge creation, capture, and use aligned with organizational strategy as it is determined that this risk is not impacted by events in 2020-21.

4.1 Failure to identify/capture critical knowledge in the knowledge creation process in 2020-21

With most workers working remotely, these workers were delegated to do all the decision-making. Being remote made it difficult for workers to stay current in the knowledge needed to support decision-making. In addition, remote work creates isolation from work networks, which slows the spread of knowledge and enables the spread of misinformation and disinformation. Remote work makes workers more susceptible to not identifying misinformation and disinformation and making wrong decisions as to what is critical knowledge. A focus on COVID-19 may lead organizations and workers to not keep automated tools up to date and collect essential knowledge. Finally, the rapid spread and use of new collaboration tools such as Zoom and Teams (Kelly, 2021) could have led organizations not to integrate these new tools into automated knowledge capture tools. Therefore, new knowledge generated and spread using these new collaboration tools may not have been captured.

Technical threats stem from the quick adoption of new collaboration technologies such as Zoom and Teams (Kelly, 2021). Threats include slow integration into organizational systems and the potential for automated tools not working with the new technology, and all made worse by technical staff working remotely and unable to access the physical systems.

Behavioral threats stem from widespread remote work and worker isolation, resulting in a flood of misinformation/disinformation pushed to socially isolated workers (Nabe, 2021). This increases the likelihood of missing critical knowledge and identifying misinformation and disinformation as critical knowledge.

Legal threats stem from new privacy laws (e.g., California) and a myriad of new social justice, health, and diversity/inclusion mandates, significantly increasing the risk of missing a legal requirement for capturing critical knowledge, not protecting essential knowledge, or identifying incorrect essential knowledge.

4.2 Disclosing critical knowledge to unauthorized recipients in the knowledge sharing processes in 2020-21

Employees replaced in-person socialization with online socialization with widespread remote work, social isolation, and significantly reduced supervision (Galanti et al., 2021). With reduced supervision, malicious employees were more likely to commit fraud (Nabe, 2021), considerably increasing the likelihood of disclosing critical knowledge. Social isolation makes humans more vulnerable to social engineering. New group/collaboration software increases the reach of hackers, including nation-state social engineers. Many instances of over-disclosure were revealed this last year in Zoom and Twitter attacks.

Technical threats stem from exploiting communication vulnerabilities common to all communication systems and focus on communication processes specific to knowledge systems. Additional threats are from storage media that does not correctly secure cloud and server storage access. 2020 increased these threat likelihoods because organizations quickly adopted collaboration software while not having the onsite staff to supervise and monitor installations and updates. These threats include Zoombombing (Downs, 2021) and large-scale hacks on Twitter (Waldman, 2021).

Behavioral threats come from several sources, such as: intentionally or accidentally failing to maintain access control lists for authorizing approved personnel to access knowledge, posting knowledge to inappropriate forums, not following disclosure processes, not encrypting knowledge in motion, falling victim to social engineering attacks, and either disclosing knowledge to unauthorized individuals or allowing malware onto their systems that are collecting and transmitting knowledge to unauthorized individuals (Columbus, 2021). 2020 saw this threat likelihood considerably rise by increasing the attack surface through social isolation and widespread remote workers (Nabe, 2021; Vijayan, 2020; Vodopyan, 2021). Additionally, workers could not create quality relationships with new organizational members as they could only meet remotely (Nabe, 2021). Examples of behavioral threats include social engineering attacks on Twitter (Downs, 2021; Vijayan, 2020) that had workers responding to disinformation.

Legal threats come from intentionally or accidentally not complying with disclosure laws, such as dealing with personally identifiable information or patient health knowledge. 2020 saw new privacy laws in California and myriad new social justice, health, and diversity/inclusion mandates, greatly increasing the risk of missing a legal requirement.

4.3 Losing critical knowledge by not capturing it from critical human sources in 2020-21

The pandemic has forced societies to shut down and many organizations have severely reduced or ceased operations, or moved to purely online environments. As organizations strive for survival, they have been forced to lay off many employees rapidly, discard a lot of old technology, and adopt new technological tools. In addition to layoffs, there have been extended absences due to employees' long-term illnesses and unexpected deaths. Finally, the great resignation, starting mid-2021, resulted in over 19 million workers suddenly leaving their jobs (Singh, 2022). All of these have resulted in losing critical knowledge.

Technical threats are linked to not utilizing established tools and processes for capturing knowledge from departing personnel. 2020-21 saw rapid shutdowns and employee loss that precluded organizations and companies from using their knowledge capture tools and strategies to capture knowledge from laid-off employees. Additionally, COVID-19 caused large numbers of deaths where most of these occurred in isolated wards, which precluded any possibility of capturing knowledge before the employee's death. Another threat stems from ransomware encrypting critical knowledge repositories and the organization or company unable to recover them through backups or by paying the ransom. Notable examples of companies paying ransomware to hackers include JB Swift, $11 million (Associated Press, 2021), the Colonial Pipeline, $5 million (Shear, Perlroth, and Krauss, 2021); and the University of California, San Diego, $1 million to ensure their COVID-19 research data was not destroyed (Winder, 2020). 2020-21 increased the likelihood of the above threats mainly due to the quick adoption of new technologies and procedures while eliminating older ones. A final technical threat comes from

natural disasters (e.g., wildfires, polar blasts, hurricanes, and flooding). Natural disasters challenged disaster recovery and business continuity plans as remote workers could not access backup and recovery systems to support implementing the recovery and thus returning captured critical knowledge to use.

Behavioral threats come from intentionally or accidentally not identifying critical human knowledge repositories and taking actions to capture and store the critical knowledge, such as not capturing knowledge from those who are retiring or other reasons for departing the organization. 2020 saw increased employee stress as organizations changed how they were operating. As new systems and processes were implemented, the likelihood of knowledge loss increased. Knowledge was lost as employees were suddenly let go, got sick, or even died. Social isolation and loss of trust in the organization have reduced knowledge sharing and capture. The great resignation in 2021 saw millions quit their jobs rather than return to the office, with most of their knowledge being lost to the organization (Luze, 2021). Misinformation and disinformation created confusion as to what knowledge needed to be captured, resulting in some critical knowledge not being captured.

Legal threats originated from intentionally or accidentally not complying with required knowledge capture (an example of this was Nuclear Regulatory Commission requirements on nuclear stations to capture critical knowledge from employees before large-scale workforce layoffs). 2020 has lowered the focus on capturing knowledge from departing employees as organizations struggle just to survive. This is likely to become an issue in the long term, even if it has not been an issue in the short term.

4.4 Losing critical knowledge by not storing it on nonvolatile media/not migrating knowledge with changing storage standards/not meeting legal standards for storing critical knowledge in 2020-21

While COVID-19 did not directly impact this outcome, not having personnel in the office meant data migration to newer technologies was slow or non-existent. Natural disasters like California and Australian wildfires, Texas polar blast, hurricanes, and flooding in the southeast United States have affected power and communication grids, affecting secure storage facilities (Gramling, 2020; Weatherford, 2021).

Technical threats are rooted in storage media, hardware, and software failure. Additional threats are from technological obsolescence leading to the loss of knowledge as the organization migrates to newer technologies or the failure of obsolete devices. Other threats come from losing repository devices and not having an appropriate backup process in place or an installed tracking system. A final threat is from ransomware encrypting critical knowledge repositories and not being able to recover them through backups or by not paying the ransom. 2020-21 saw many successful ransomware attacks that resulted in large payouts (see section 4.3 for examples). Additionally, events that cause widespread damage or extended loss of power can cause storage devices to fail or be destroyed. 2020-21 saw a 100 + year winter storm that caused the grid to fail in the state of Texas (Timmer, 2021), wildfires in California (Alonzo and Sanchez, 2020) and Australia (Gramling, 2020) that destroyed miles of transmission lines and equipment, and record hurricanes and storms in the southeast United States (Gramling, 2020) that also destroyed miles of transmission lines and equipment. The technical threats come from failed equipment and backups. Security teams must review their disaster recovery/business continuity plans to ensure that the secure storage being counted on is safe from a power and communication point. Note that Y2K had many of the same issues, and it was important that the work to overcome Y2K technical problems was done swiftly as it was much worse than the public knew.

Behavioral threats stem from intentionally or accidentally not following technology procurement processes, selecting providers without checking their technology, not planning for obsolescence, not testing technologies before applying them or while using them, and artificially obsoleting technologies. 2020-21 saw significant disruptions in supply chains and purchasing decisions, significantly increasing this threat likelihood. Additionally, remote workers were more likely to not follow backup processes due to lack of system access or inability to follow new procedures.

Legal threats are liability issues associated with not following sanctioned or committed storage standards (such as those from NIST, Control Objectives for Information and Related Technology (COBIT), and the International Standards Organization (ISO). 2020-21 saw remote work with many office locations not staffed. This increases the likelihood of legal threats occurring as IT staff could not migrate to new storage standards or make changes to existing ones.

4.5 Giving bad advice by not using appropriate knowledge or by using inappropriate knowledge in 2020-21

This risk is perhaps the most likely, given the proliferation of misinformation and disinformation threats. The response to COVID-19 is replete with this happening. Perhaps the most egregious example of bad advice being that of deciding to send COVID-19 patients to nursing homes so that they could get better care but, in the process, infecting the most vulnerable. The most recent example is those deciding not to get the vaccine. There is misinformation and disinformation in COVID-19, the 2020 elections, the social justice movement, and virtually every other issue. New processes for identifying and censoring misinformation and disinformation significantly contributed to giving bad advice. Finally, remote workers have access to all this misinformation and disinformation but do not have support in determining what is true or false. The media in the United States has become politicized and partisan, and social media firms were trying to censor misinformation and disinformation, significantly impacting an employee's ability to judge information.

Technical threats come from search tools not finding relevant knowledge, improperly prioritizing some knowledge, not using integration tools that would allow knowledge pertinent to be incorporated into search results, or using visualization technologies that influence decision-makers to the wrong option. 2020-21 saw the rise of the use of AI tools to filter out misinformation and disinformation. However, the problem with AI tools is that they reflect the bias of their builders. Additional threats come from the classification of knowledge in knowledge systems. This effort is reduced by workers working remotely and not having access to all the knowledge gathered or the time to solicit and classify knowledge from other remote workers. A final threat comes from knowledge systems not having adequate processes for validating the accuracy of knowledge in the system.

Behavioral threats are from decision-makers using incomplete knowledge and inappropriately applying knowledge to unsuitable decision contexts. 2020-21 saw this likelihood increase as social isolation, social media use, and lack of interactions with organizational experts increased while reliance on media fact-checkers increased the likelihood of using weak knowledge for making decisions.

Legal threats are from decision-makers not utilizing due care or due diligence in assessing knowledge and focusing on politically correct or desired advice. Another threat is not giving advice based on limiting liability rather than stating the direction suggested by the knowledge system. 2020-21 saw a tremendous increase in social unrest, leading to new standards and laws on social justice and revised history, greatly increasing the likelihood of this threat. While not quite a legal issue (it is vigilante justice), society has taken to "canceling" individuals and organizations that don't support new norms. Knowledge systems risk not changing content fast enough to avoid not meeting new norms, which has resulted in canceling organizations and companies.

5. Discussion

The purpose of this paper was to analyze and identify threats that impact risks to knowledge in the light of the recent COVID-19 pandemic and then make recommendations for modifying knowledge risk strategy. Obasiolu (2020) reports that companies did not know themselves well enough to implement a resilient security program to handle the many severe challenges faced in 2020-21. An organization cannot properly secure its knowledge assets if it does not understand its main business processes and validate these processes that create knowledge. The Organization for Economic Cooperation and Development (OECD) reports that cybersecurity risks significantly increase in crises because stressed organizations are more vulnerable to attacks (OECD, 2020). The Risk Management Framework in NIST SP800-37r2 (NIST, 2018) uses the above risk management process to guide organizations in creating a risk management strategy. NIST 800-37r2 guides organizations create a risk strategy by identifying the importance of the system or asset (i.e., knowledge assets) and specifying the organization's risk tolerance for these systems/assets. The organization then selects an array of controls for managing and mitigating the risk within the organization's risk tolerance (NIST, 2018). Knowledge assets tend to be critical assets. The purpose of the risk management strategy for these assets would be to mitigate/minimize the risk to the organization's risk tolerance. This paper has identified threats that can increase the likelihood or severity of the five knowledge risks, including knowledge systems under extreme circumstances, such as those created by COVID-19 and other natural disasters in 2020 and 2021. We identified five specific cases of knowledge risk and described threats enhancing the risk in terms of technical, behavioral, and legal threats. The following recommendations influence the actions/controls an organization should select to mitigate the threats.

The first recommendation is for controls for identifying misinformation and disinformation. Organizations can address this threat through a control focused on training employees to identify misinformation/disinformation (Wetherford, 2021) and control by creating a position responsible for monitoring and identifying misinformation/ disinformation (Levick, 2021). Additionally, technical controls using AI tools are needed to filter news, emails, and identify deep fakes, frauds, misinformation, and disinformation. This long-term solution will be critical for an organization to make sound business decisions using validated knowledge sources. Finally, an organizational communication control for informing their employees about misinformation and disinformation, frauds, and deep fakes, while not overburdening them with additional information is needed.

The second control is forming or rewriting guidelines and instructions for employee online behavior. Organizations need to focus on the social media usage of their employees for both knowledge sharing and knowledge reuse. Organizations' dilemma is creating rules that create acceptable social media usage without denying freedom of speech. Future research should evaluate the limit of what is acceptable and unacceptable to talk about on social media regarding organizations and their lives. There is a need to define the protocols of responding to questions in social media; for example, when an employee responds, should his view be treated as the organization or personal views? Guidelines about social media engagement during and after work hours are needed specifically for the remote workforce because of the blurry line between work and private life. The guidelines for social media engagement should also include a section on how to spot and evaluate potential misinformation and disinformation and the threat of downloading malware. A final aspect of the control is to review and update employee training of social media use and social engineering protection.

The third control is the identification and evaluation of communication channels. The social isolation of employees creates a unique problem. We have learned that employees miss socializing with their coworkers and that virtual social hours do not replace physical socializing. Especially Generation Z is very sensitive to social isolation, and organizations need to create special networking programs for these employees. Promoting socializing channels that help people get together and know each other helps the organization reduce the risk of employees falling prey to social engineering attacks. Proper channels for work-related socializing also reduce the risk of knowledge spillovers and helps promote job satisfaction among the employees, thus reducing unwanted employee turnover.

The fourth control involves re-evaluating the work itself. The resignation of approximately 19 million workers should be a wake-up call to organizations that work-life issues need to be addressed (Luze, 2021). Jennex (2014) proposed a risk assessment framework for determining the risk of losing knowledge from departing employees based on work-life factors. Workers in 2020-21 found out that they could be as productive with more control over their lives working remotely and are not eager to return to their old office. Controls need to be developed for the new work models designed to make the organization more resilient. Additionally, the Jennex (2014) framework did not consider remote work. A future work recommendation is that the Jennex (2014) framework should be adjusted using a required number of days in the office as a new metric and modifying its probability matrix (suggest including 1) required day in the office with the level 6 probability, 2) required days with the level 7, etc.). We urge organizations to develop a knowledge risk management strategy utilizing the Jennex (2014) framework and assessing other work-life balance of their employees to create a strategy that includes more remote work as a strategy for retaining employee knowledge.

The fifth action/control needed is for the organization to implement a knowledge capture process for departing personnel. Jennex (2014) outlines how this process could work with the key parts of this process being the organization knowing what is critical knowledge, where it is stored, and having capture processes and technologies in place that can be used even if the departing personnel cannot or will not participate in the knowledge capture process.

The sixth action/control is a major risk re-assessment is needed in most organizations. Jennex and Durcikova (2020) proposed a comprehensive knowledge risk assessment framework based on the Ilvonen, Jussila, and Kärkkäinen, (2015) knowledge risk framework. The probabilities of many events are higher than expected during 2020-21. Extreme disasters (wildfires, riots, floods, hurricanes, polar blasts, etc.) cause major disruption in the operations of a business. Organizations should use the Jennex-Durcikova (2020) framework to develop disaster recovery/business continuity strategies to secure knowledge when a natural disaster hits and when it may destroy knowledge sources or access to these knowledge sources might not be available. Re-evaluation of existing disaster response/business continuity and backup plans is needed, given that the likelihood of extreme

events is much higher than most organizations anticipated even a year ago. Knowledge systems that allow employees to share and retrieve knowledge must be not only defended against natural threats but also be easily accessible while working remotely. Additionally, the re-assessment needs to ensure that critical knowledge, knowledge holders, and knowledge repositories are identified and included in the security plan. Further, new systems added during COVID-19 are incorporated into the organizational security plan including the asset inventory, that system specific policies are created to guide the configuration of new systems, and that appropriate incident response and contingency plans are created/updated. Finally, the re-assessment needs to include a legal review of new privacy laws and other mandates issued during 2020-21.

6. Conclusions

2020-21 may be outlier years, but they have shown us that the likelihood of extreme events is greater than we like to admit. We conclude that organizations are more vulnerable to attacks on their knowledge systems and knowledge assets when under stress (OECD, 2020), additionally, knowledge systems and knowledge assets are at risk when the organization's environment is in turmoil.

This paper extends the threats to knowledge system/knowledge asset risk based on events in 2020-21 and conclude that knowledge risks are more likely to occur than previously thought. The knowledge system/knowledge risks being investigated come from Jennex and Durcikova (2020) and are:

- Failure to identify and capture critical knowledge in the knowledge creation process.
- Disclosing critical knowledge to unauthorized recipients in the knowledge sharing processes.
- Losing critical knowledge by not capturing it from critical human sources.
- Losing critical knowledge by not storing it on nonvolatile media, not migrating knowledge with changing storage standards, or not meeting legal standards for storing essential knowledge.
- Giving bad advice by not using appropriate knowledge or by using inappropriate knowledge.

However, mitigating many of these threats is outside the technical expertise of the traditional cybersecurity department. This paper proposes six actions/controls that should be taken by organizations to mitigate the likelihood of the threats identified in this paper so that knowledge risks can be managed to acceptable levels. These actions/controls are:

- Add controls to assist in identifying and blocking misinformation/disinformation
- Create/revise guideline controls for employee behavior in online social media forums
- Review organizational communication channels to ensure that employees working remotely are not socially isolated and remain in contact with other employees
- Re-evaluate the way work is performed, where, when, how long, and adjust the work processes to fit worker needs and to improve work/life balance
- Create a knowledge capture process for departing personnel
- Review the risk assessment that has been done to include higher likelihood of extreme events and adjust backups and infrastructure as needed. Additionally this review should include ensuring systems, data, and/or equipment added during COVID-19 are included in the risk assessment, that critical knowledge, knowledge holders, and repositories are also in the risk assessment, and that reviews are conducted to ensure new legal requirements and standards are reviewed and incorporated as appropriate..

To create the control for identifying and blocking misinformation/disinformation additional expertise in identifying and countering misinformation and disinformation may be needed (Weatherford, 2021). Identifying essential knowledge in the organization is not easy, which requires understanding employees' knowledge transfer and retrieval processes, and their practices of evaluating the knowledge they have access to. Thus, it is not enough for the organization that the cybersecurity experts can identify misinformation/disinformation on sight. They need to know how misinformation/disinformation reach the employees and help them spot them. This cannot be only the task of security professionals; the whole organization's involvement is needed and in organizations where misinformation/disinformation is severe they should add a position such as a chief misinformation officer. This position would be responsible for ensuring the organization can identify and block misinformation/disinformation as well as for training employees in how to handle misinformation/disinformation.

Finally, organizations and companies need expertise in organizational psychology to assist the organization in preparing employees to understand, identify, deflect, and reject misinformation, disinformation, and phishing

(Vodopyan, 2021) to aid in identifying the insider threat. Another value of having organizational psychology expertise is assisting employees in dealing with anxiety related to remote work and social justice issues. The bottom line is that the management must first address the human element of knowledge and cybersecurity if cybersecurity efforts are to be successfully implemented in any organization (Vijayan, 2020).

There are limitations to this research. The first and most important limitation is that the research and data used in this paper is United States specific. This makes generalizing the results to the rest of the world difficult. However, it is the conclusion of this paper that most if not all the recommendations and threat findings are applicable to any organization wherever it is located. The second limitation is that the data used for the analysis comes from media and practitioner sources making its reliability a little suspect. This limitation is considered acceptable as the paper is doing an intelligence-based threat assessment and is not quantifying the impact on increased frequency of the threat, just that the threat exists. The third limitation is that the paper does not quantify the impact of the threats on knowledge risks. This is also considered acceptable as the focus of the threat assessment is to identify risks, not quantifying the threats. Also, to quantify the impact of the threats the unit of analysis would have to be on a specific organization as threat quantification is unique for each organization.

Acknowledgement

A previous conference version of this paper was included in the proceedings of HICSS55, the 55th Hawaii International Conference on System Sciences.

References

Alavi, M. and Leidner, D.E., 2001 Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues, *MIS Quarterly*, 25(1), 107-136.

Alonso, M. and Sanchez, R., 2020. California's record-breaking wildfires consume nearly 1 million acres in a month. *CNN*, October 17, 2020. Available at cnn.com, https://www.cnn.com/2020/10/17/us/california-wildfires-saturday/index.html. Accessed on August 7, 2022.

Associated Press, 2021. Meat company JBS confirms it paid $11M ransom in cyberattack. *Associated Press*, June 10, 2021. Available at usatoday.com, at https://www.usatoday.com/story/tech/2021/06/10/jbs-confirms-paid-11-million-ransom-cyberattack/7633299002/. Accessed on August 8, 2022.

Bhardwaj, A., and Goundar, S. (2019). A framework for effective threat hunting. Network Security, 2019(6), 15-19.

Billington, J., 1997. A Few Things Every Manager Ought to Know About Risk. *Harvard Management Update*, 2(3), March, pp. 1-12.

Columbus, L., 2021. Top 10 cybersecurity lessons learned one year into the pandemic. *VentureBeat* March 11, 2021. Available at venturebeat.com, https://venturebeat.com/2021/03/11/top-10-cybersecurity-lessons-learned-one-year-into-the-pandemic/. Accessed on August 10, 2022.

Davenport, T. H., and Prusak, L., 1998. *Working knowledge: How organizations manage what they know*. Harvard Business Press, Boston, MA, USA.

Downs, F., 2021. Major Lessons to be Learned from 2020 Security Mishaps. *InfoSecurity Magazine*. Available at inforsecurity-magazine.com,https://www.infosecurity-magazine.com/blogs/major-lessons-learned-2020-mishaps/. Accessed on August 10, 2022.

Durst, S. and Zieba, M., 2019. Mapping knowledge risks: towards a better understanding of knowledge management. *Knowledge Management Research and Practice*, 17(1), 1-13, DOI: 10.1080/14778238.2018.1538603.

Galanti T, Guidetti G, Mazzei E, Zappalà S, and Toscano F., 2021. Work from home during the COVID-19 outbreak: the impact on employees' remote work productivity, engagement, and stress. *Journal of Occupational and Environmental Medicine*. 63(7):e426-e432. doi: 10.1097/JOM.0000000000002236. Available at the National Library of Medicine, National Center for Biotechnology Information, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8247534/. Accessd on August 6, 2022.

Gat Labs, 2020. The Biggest Cloud Security Lessons Learned in 2020 (A Year in Review). *Gat Labs Blog*. Available at gatlabs.com, https://gatlabs.com/blogpost/cloud-security-lessons-learned-in-2020/. Accessed on August 10, 2022.

Gramling, C., 2020. Wildfires, heat waves and hurricanes broke all kinds of records in 2020. *Science News*, December 21, 2020. Available at sciencenews.org, https://www.sciencenews.org/article/climate-change-wildfires-heat-waves-hurricanes-records-2020. Accessed on August 11, 2022.

Hazel, T., 2021. Threat hunting frameworks and methodologies: an introductory guide. ChaosSeach Blog, April 29, 2021. Available at chaossearch, https://www.chaossearch.io/blog/threat-hunting-methods-and-frameworks. Accessed on August 10, 2022.

Ilvonen, I., Jussila, J. J., and Kärkkäinen, H., 2015. Towards a business-driven process model for knowledge security risk management: Making sense of knowledge risks. *International Journal of Knowledge Management*, 11(4), pp. 1-18.

Institute of Health Metrics and Evaluation (IHME), 2022. COVID-19 projections: United States of America. Available at covid19.healthdata.org, https://covid19.healthdata.org/united-states-of-america?view=cumulative-deaths&tab=trend. Accessed on February 13, 2022.

Jennex, M.E., 2014. A proposed method for assessing knowledge loss risk with Departing Personnel. *VINE: The Journal of Information and Knowledge Management Systems*, 44(2), pp. 185-209.

Jennex, M.E. and Durcikova, A., 2014. Integrating KM and security: are we doing nnough? *International Journal of Knowledge Management*, 10(2), pp. 1-12.

Jennex, M. E., and Durcikova, A., 2020. Creating sustainable knowledge systems: towards a risk and threat assessment framework. *Journal of Strategic Innovation and Sustainability*, 15(4). https://doi.org/10.33423/jsis.v15i4.2965.

Kelly, R., 2021. How the pandemic boosted ed tech adoption. *Campus Technology*, June 8, 2021. Available at https://campustechnology.com/articles/2021/06/08/how-the-pandemic-boosted-ed-tech-adoption.aspx?s=ct_nu_150621&oly_enc_id=6899H3366067E5A. Accessed on August 6, 2022.

Levick, R., 2021. Should companies consider appointing chief paranoia officers to combat disinformation? *Brink*, February 21, 2021. Available at brinknews.com, https://www.brinknews.com/should-companies-consider-appointing-chief-paranoia-officers-to-combat-disinformation/. Accessed on August 6, 2022.

Luze, S., 2021. What employers can learn from 'the great resignation.' *Forbes*, October 22, 2021. Available at forbes.com, https://www.forbes.com/sites/ellevate/2021/10/22/what-employers-can-learn-from-the-great-resignation/?sh=6484fcb87826. Accssed on August 6, 2022.

Nabe, C., 2021. Impact of COVID-19 on cybersecurity. *Deloitte*. Available at deloitte.com, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html#. Accessed on June 11, 2021.

Newman, L.H., 2021. Worst Hacks of 2021. *Wired*, December 24, 2021. Available at wired.com, https://www.wired.com/story/worst-hacks-2021/. Accessed on February 7, 2022.

Nissen, M., 2002. An extended model of knowledge-flow dynamics. *Communications of the Association for Information Systems,* 8(1), article 18.

National Institute of Standards and Technology, NIST SP 800-37 rev 2, 2018. Risk management framework for information systems and organizations: a system life cycle approach for security and privacy, *National Institute of Standards and Technology.* Available at the NIST Cybersecurity Resource Center, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf. Accessed on August 8, 2022.

National Institute of Standards and Technology, NIST SP 800-30 rev 1, 2012. Guide for conducting risk assessments. *National Institute of Standards and Technology.,* Available at the NIST Cybersecurity Resource Center, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. Accessed on August 8, 2022.

Obasiolu, D., 2020. Important Cybersecurity Lessons Learned During the Pandemic. *Forbes*, November 2, 2020. Available at Forbes.com, https://www.forbes.com/sites/theyec/2020/11/02/important-cybersecurity-lessons-learned-during-the-pandemic/?sh=4941e9117aa9. Accessed on August 10, 2022.

Organization for Economic Cooperation and Development, OECD, 2020. Seven lessons learned about digital security during the COVID-19 crisis. *Organization for Economic Cooperation and Development*, November 4, 2020. Available at OECD Coronavirus, https://www.oecd.org/coronavirus/policy-responses/seven-lessons-learned-about-digital-security-during-the-covid-19-crisis-e55a6b9a/. Accessed on August 10, 2022.

Osborne, C., 2021. The biggest data breaches, hacks of 2021. *Zero Day*, December 31, 2021. Available at ZDnet.com, https://www.zdnet.com/article/the-biggest-data-breaches-of-2021/. Accessed on August 7, 2022.

Our World in Data, 2022. Cummulative confirmed COVID-19 cases by world Rregion. *Our World in Data*. Available at https://ourworldindata.org/grapher/cumulative-covid-cases-region. Accessd on August 10, 2022.

Parakilas, J., 2020. The lesson of 2020? security doesn't mean what you think it does. *The Diplomat*, December 23, 2020. Available at Diplomat.com, https://thediplomat.com/2020/12/the-lesson-of-2020-security-doesnt-mean-what-you-think-it-does/. Accessed August 10, 2022.

Poonemon Institute, 2021. The Impact of ransomware on healthcare during COVID-19 and beyond. Ponemon Institute, LLC, September, 2021. Available from censinet.com: https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf. Accessed August 21, 2022.

Samonas, S. and Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. Journal of Information System Security, 10(3).

Shear, M.D., Perlroth, N., and Krauss, C., 2021. Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers. *New York Times*, June 7, 2021. Available at New York Times, https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html. Accessed on Auguast 7, 2022.

Sherr, I., 2021. Gen Z is getting screwed by remote work, Microsoft survey finds. *CNET* March 22, 2021. Available at CNET.com, https://www.cnet.com/news/gen-z-is-getting-screwed-by-remote-work-new-microsoft-survey-says/. Accessed on August 10, 2022.

Singh, V., 2022. Lessons We Have Learned from the Great Resignation. *GettingPeopleRight.com*, January 14, 2022. Available at Professional Leadership Institute.com, https://gettingpeopleright.com/career/lessons-we-have-learned-from-the-great-resignation/. Accessed on August 4, 2022.

Spears, J., 2012. Conceptualizing Data Security Threats and Countermeasures in the E-Discovery Process with Misuse Cases. *AMCIS 2012 Proceedings*. Paper 17. Available at http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/17. Accessed on February 9, 2022.

Timmer, J., 2021. Texas' power grid crumples under the cold. *ARS Technica*, February 15, 2021. Available at ARS Technica.com, https://arstechnica.com/science/2021/02/texas-power-grid-crumples-under-the-cold/. Accessed on August 11, 2022.

Vijayan, J., 2020. 6 Cybersecurity Lessons From 2020. *Dark Reading*, November 3, 2020. Available at https://www.darkreading.com/attacks-breaches/6-cybersecurity-lessons-from-2020/d/d-id/1339333?image_number=1. Accessed on June 10, 2021.

Vodopyan, E., 2021. 2020: IT Security Lessons to Learn. *Netwirx Blog*, June 4, 2021. Available at darkreading.com, https://blog.netwrix.com/2020/12/30/2020-it-security-lessons-to-learn/. Accessed on August 10, 2022.

Waldman, A., 2021. 10 of the biggest cyber attacks of 2020. *Tech Target*, January 5, 2021. Available at techtarget.com, https://www.techtarget.com/searchsecurity/news/252494362/10-of-the-biggest-cyber-attacks. Accessed on August 7, 2022.

Walsh, J. P., and Ungson, G. R., 1991. Organizational Memory. *Academy of Management Review*, 16(1), pp. 57-91.

Weatherford, M., 2021. Misinformation, Disinformation, and what Government can do about them. *Governing*, March 3, 2021. Available at governing.com, https://www.governing.com/security/misinformation-disinformation-and-what-government-can-do-about-them.html. Accessed on August 10, 2022.

Wikipedia, 2021a. Misinformation. *Wikipedia the Free Encyclopedia.* Available at Wikipedia.org, https://en.wikipedia.org/wiki/Misinformation. Accessed on August 6, 2022.

Wikipedia, 2021b. Disinformation. *Wikipedia the Free Encyclopedia.* Available at Wikipedia.org, https://en.wikipedia.org/wiki/Disinformation. Accessed on August 6, 2022.

Winder, D., 2020. The University of California Pays $1 Million Ransom Following Cyber Attack. *Forbes*, June 29, 2020. Available at Forbes.com, https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/?sh=48c1c9c818a8. Accessed on August 7, 2022.