2018

The Effects of Computer Crimes on the Management of Disaster Recovery

Tim Gene Proffitt
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Timothy Gene Proffitt

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. David Gould, Committee Chairperson, Management Faculty
Dr. Howard Schechter, Committee Member, Management Faculty
Dr. Richard Schuttler, University Reviewer, Management Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

The Effects of Computer Crimes on the Management of Disaster Recovery

by

Timothy Gene Proffitt

MS, SANS Technology Institute, 2010

BS, Sam Houston State University, 1998

Dissertation in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

May 2018

Abstract

The effects of a technology disaster on an organization can include a prolonged disruption, loss of reputation, monetary damages, and the inability to remain in business. Although much is known about disaster recovery and business continuance, not much research has been produced on how businesses can leverage other technology frameworks to assist information technology disaster recovery. The problem was the lack of organizational knowledge to recover from computer crime interruptions given the maturity level of existing disaster recovery programs. The purpose of this Delphi study was to understand how disaster recovery controls and processes can be modified to improve response to a computer crime caused business interruption. The overarching research question in this study was to understand what factors emerge relative to the ability of disaster recovery programs to respond to disasters caused by computer crimes. The conceptual framework included a maturity model to look at how programs might be improved to respond to the computer crimes threat. Research data were collected from a 3 round Delphi study of 22 disaster recovery experts in the fields of disaster recovery and information security. Results from the Delphi encompass a consensus by the panel. Key findings included the need for planning for cyber security, aligning disaster recovery with cyber security, providing cyber security training for managers and staff, and applying lessons learned from experience. Implications for positive social change include the ability for organizations to return to an acceptable level of operation and continue their service benefiting employees, customers, and other stakeholders.

The Effects of Computer Crimes on the Management of Disaster Recovery

by

Timothy Gene Proffitt

MS, SANS Technology Institute, 2010

BS, Sam Houston State University, 1998

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

May 2018

Dedication

First and foremost, I would like to give thanks to my wife Crystal and two children, Charley and Samuel, who have given me strength and their precious time to get me through this challenge. I would also like to acknowledge my father and mother who believed in me even when I doubted myself. They encouraged me to stay in college which ultimately led me to the completion of this doctoral journey.

Acknowledgments

I would like to acknowledge and thank the Walden University faculty who took the time to provide valuable feedback and encouragement. Each class was a step in the direction of completing this dissertation, and the faculty made the program enjoyable. I want to give special thanks to my committee of Dr. David Gould and Dr. Howard Schechter who took my project and guided my writing into the dissertation it is today. I want to thank my URR. Dr. Richard Schuttler for his invaluable contributions. I would also like to thank Robert Armstrong and the management team of my company for allowing me to take the time away from work when I needed to stay on track with this program.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Businesses must be able to recover from an unexpected interruption if they are to continue to service their customers and maintain an advantage over their competition. The management of disaster recovery activities is a critical role in restoring the business after it has experienced an interruption. An interruption can include anything from natural disasters to terrorism (Guidry, Vaughn, Anderson, & Flores, 2015). The goal of information technology disaster recovery, a subset of the larger known emergency management theory, includes planning and the resumption of applications, data, hardware, digital communications, and other technology infrastructure. Technology-caused disasters require a response by technology resources to triage and resume the business's technology infrastructure. Information technology disaster recovery is primarily concerned with the minimizing of the interruption of operations, ensuring security, and producing a reliable data. Technology disasters can manifest from hard drive failures, erroneous backup, or loss of a network segment, but computer crimes are an emerging threat that organizations need to consider as an equal threat as a traditional disaster.

In this chapter, I provide information about the importance of understanding the impact of computer crimes on information technology disaster recovery. The disaster recovery problem, purpose of the study, and theoretical framework are discussed. The chapter concludes with the description of the research method, assumptions of the study, delimitations, and significance of the study.

Background of the Study

Interruptions resulting from computer crimes create damages to businesses in the form of financial loss, reputation, data destruction, and privacy issues (Marinescu, 2015; Mossburg, 2015; Mulla & Ademi, 2015; Tran, Campos-Nanez, Fomin, & Wasek, 2016). Computer crimes are often executed against technology infrastructures through the acts of hacking, denial of service, malware, ransomware, or phishing. The 2014 hacking of Sony Pictures Entertainment caused the company to operate for several days without computing resources while the technology infrastructure was being resumed from the attack (Bidgoli, 2016; Solberg Søilen, 2016). In January of 2016, a milestone was reached when a hacking group was successful in attacking regional power authorities in Ukraine that led to the loss of power to over 225,000 customers (Lee, Assante, & Conway, 2016). In February 2016, the Hollywood Presbyterian Medical Center emergency room was disrupted by computer crimes that resulted in the transfer of patients to alternate hospitals (Kandel & Kovacik, 2016; Sittig & Singh, 2016). On June 27, 2017, the Heritage Valley Health System, based in Beaver, Pennsylvania, was forced to suspend operations from a targeted cryptolocker attack that disabled computer systems in two hospitals (Schwartz, 2017a). Computer crimes should be considered as significant risks to an organization's standard operating procedures. Business is being affected by computer crimes that are causing significant interruptions. Computer crime interruptions are becoming a bigger issue, as a business must position itself against a growing range of risks (Allianz, 2015; Jang-Jaccard & Nepal, 2014). Morgan (2016) claimed the damages from computer crimes and their interruptions are expected to reach 6 trillion dollars by

2021. Businesses that are reliant on technology are experiencing significant interruptions due to computer crimes, which lead to monetary losses, customer turnover, reputational losses, and diminished goodwill (Brown, 2016; Ferdinand, 2015). Computer crimes can initiate from multiple vectors and may leverage a risk that was not previously identified by cybersecurity team or emergency planners. Computer crimes will continue to increase as the number of technology devices is being leveraged in businesses.

Problem Statement

Although much is known about disaster recovery and business continuance, not much research has been produced on how businesses can leverage other technology frameworks to assist information technology disaster recovery (Bird, 2015; Brown, 2016; Dines, 2012; Ignatius, 2015; Marinescu, 2015). The general problem, as Ferdinand (2015) noted, was that the ability to resume a business has now become not just a management goal, but a goal for critical technology infrastructures. The specific problem was the lack of organizational knowledge to recover from computer crimes interruptions given the maturity level of existing disaster recovery programs. Guidry et al. (2015) and Ferdinand discussed the lack of a set of control procedures to allow understanding of how business's management can bolster disaster recovery programs to account for this type of interruption.

Traditional information technology disaster recovery focuses on fire, flood, loss of power, and technology hardware failures, but research conducted in the 2016 Cyber Security Intelligence Index by IBM noted 60% of small to medium size businesses fail following a cyber-attack (IBM, 2016). McCreight and Leece (2016) wrote that disaster

planners might not respond to security events where they have no knowledge. Increasing the understanding of the disaster planners, responders, and management teams improves the ability to execute the recovery plan. This research may help close the gap by increasing the understanding of how business may leverage cybersecurity frameworks to modify information technology disaster recovery programs. The information from this study might produce a framework for businesses to find additional capabilities in responding to a computer crimes interruption.

Businesses that are unable to serve their customers do not tend to remain in business for long. The ability to recover from an unexpected interruption is vital if the business is to continue to service their customers and maintain an advantage over the competition. Information technology disaster recovery (ITDR) emerged from the field of emergency management and sought to resume the organization from a technology outage quickly. Traditionally, businesses have needed to prepare for outages from fire, flood, loss of power, and terrorism. With the increase in reliance on technology infrastructures, businesses also need to prepare for computer crimes such as hacking, denial of service, and malicious insiders in interrupting the business by causing a technology interruption.

Purpose of the Study

The purpose of this qualitative Delphi study was to understand how information technology disaster recovery controls and processes can be modified to improve response to a computer crime caused business interruption. This qualitative approach included a focus on information technology disaster recovery participants to develop a new framework of response. Twenty-two participants with at least 5 years' experience in

disaster recovery were interviewed until patterns or themes were detected. The inquiry included a focus on the existing information technology disaster recovery frameworks as they are executed by organizations in resuming the business into a state where normal operations can be conducted. The new model was developed as an understanding of how the information technology disaster recovery processes might be influenced by other frameworks tailored to cybersecurity or computer incident response. A Delphi approach was chosen over other qualitative research approaches, such as a case study, because I aimed to learn what factors affect certain responses and how to improve the disaster response process.

Research Questions

The research may help to build knowledge on several qualitative questions about the current state of information technology disaster recovery and where integration of cybersecurity methodologies would be advantageous. A qualitative inquiry was chosen to allow for rich data analysis from a specific, expert population of participants and theory generation to improve disaster response. The overarching research question in this study is: What factors emerge relative to the ability of disaster recovery programs to respond to disasters caused by computer crimes? Subsequent questions asked in the Delphi rounds sought to understand how successful are disaster responders when following approved information technology disaster recovery plans to recover from computer crimes caused business interruption. What steps do the experts believe can be an improvement for resumption from this type of threat? What interruptions caused by computer crimes cause the response team to recover differently than a traditionally planned? What differences

can be found from a business that prepared for interruptions caused computer crimes as compared to those that do not? What common themes exist where the cause of the technology interruption might have been significantly reduced by modification of the information technology disaster recovery framework to align with a cybersecurity framework?

Conceptual Framework

This study used a disaster recovery maturity model as the conceptual framework. A disaster recovery maturity model depicts multiple levels representing an organization's ability to resume the business within the desired recovery time objective (Randeree, Mahal, & Narwani, 2012; Stewart, Allen, Dorofee, Valdez, & Young, 2015). Based on a capability maturity model, the maturity level speaks to the state of readiness to recover from a business interruption. An organization at the lowest level of *ad hoc* has minimal planning and will scramble to recover the organization. The highest level of *resilience* will exist where the organization has a detailed recovery plan, administrative oversight, and established preventive measure. Assessing the organization's disaster recovery program against key factors such as documentation, recovery time objectives, architecture, and scope provides an understanding of a state of readiness and what processes need to be re-engineered for improvement. The disaster recovery maturity model provided the ability to assign recommendations to improve maturity in action-oriented goals.

Nature of the Study

A qualitative researcher aims to gather an in-depth understanding of a phenomenon and the data surrounding that phenomenon. Woods, Macklin, and Lewis (2016) described qualitative research as the combining of knowledge, experience, and understanding to allow the researcher to make judgments about a phenomenon or circumstance. A qualitative inquiry was chosen because it is the most appropriate design for gaining an understanding of the problem computer crimes interruptions causes to disaster recovery programs. A qualitative inquiry was selected over a quantitative study because of the little knowledge on the subject of computer crimes affecting information technology disaster recovery processes, and the difficulty of soliciting participants willing to discuss their organization's failure. Although empirical survey data might be collected on experienced disasters and a hypothesis designed about what impacts would exist, the nature of a qualitative study allows for a rich data collection on the phenomenon.

A Delphi design was selected over other qualitative approaches, such as case study or phenomenology, because of the goal of the study was for prediction and theory building. In a qualitative case study of an organization's disaster response, the data collected from the small number of organizations may not fully develop a theory of how other organization may leverage a different set of controls for resuming the business. The Delphi design allows for the identification of controls or alternative frameworks that may be used to improve the process by analyzing feedback from experts in the field of disaster recovery. The findings from the data collection activity are triangulated from the

responses of the participants and research during the literature review. The study was exploratory because of the small number of studies on the topic of computer crimes as they affect information technology disaster recovery.

While Delphi is a flexible approach for data collection and consensus generation, the researcher must consider different designs to implement the method correctly. Skulmoski, Hartman, and Krahn (2007) wrote that the initial Delphi questions are typically broad, open-ended questions. Extra care must be made by the researcher to ensure the initial set of qualitative questions set the proper path for the research. The researcher may see limitations in the research by not executing Delphi with a proper set of initial questions, not populating the panel with the correct expertise, and not correctly communicate the requirements of the participants. To address these limitations, I worked with the committee to refine the initial round of questions, conducted a pilot round to solidify the questions and instructions, diligently sought the proper panel members, and carefully crafted communications to each participant. The number of participants chosen was a number large enough to allow for the loss of multiple panelists as well as to obtain data saturation.

The topic of information technology disaster recovery activity resulting from computer crimes does not raise an ethical concern. Delphi is used in an anonymous fashion that allows for participants to provide their expertise on how the traditional disaster recovery methods can be positively altered. The panelists are not affiliated with a business so that there can be no negative perceptions of an entity or employer. Disaster

responders and technology management are not considered a traditional protected class in scientific research.

Definitions

Business continuity planning: Business continuity planning is the methodology that ensures certain critical business functions will continue to operate regardless of the disasters that may be encountered by the organization. Business continuance is mainly business facing and will focus on planning (Thejendra, 2008).

Computer crimes: An act performed by a person, sometimes referred to as a hacker that illegally uses, steals or destroys information. This individual or group of individuals may destroy or corrupt the computer data (Schultz & Shumway, 2001).

Computer exploits: A technology exploit is a mechanism for executing an unintended, potentially damaging process afforded by a technology vulnerability that offers an advantage to an attacker (Sen & Heim, 2016).

Contingency: A contingency is something that has occurred out of the ordinary. A contingency could range from a fire to a malicious insider deleting data (Togio, 1989).

Crisis management: Crisis management is defined as the process by which a group of senior management will control conversing with the media, dialog with the customers, and act as a panic prevention team (Tucker, 2014).

Cybersecurity incident responders: An incident responder specifically trained and charged with resuming the organization in the event of an information security incident (Schultz & Shumway, 2001).

Disaster recovery: Disaster recovery is the planning and execution needed to quickly recover from a disaster that is usually caused by technology (Tucker, 2014).

Disaster recovery site: A disaster recovery site is usually an alternative computing site that can be used to run the technology the business needs if the primary site fails or becomes unstable (Togio, 1989).

Emergency management: The managerial function of creating the framework by which communities reduce vulnerabilities to disasters and how to cope with the disaster when encountered (Hiatt, 2000).

Failover: Failover is the mechanism used to migrate the production system to a redundant server upon the previous active backup (Grigonis, 2002).

First responders: Someone designated or trained to be the first to respond to an emergency (Bishoff et al., 2015).

Recovery time objectives: The designated duration of time and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences to the organization (Thejendra, 2008).

Resumption: The act of returning an organization into the state it was in before a disaster or interruption (Thejendra, 2008).

Security: Security is defined as that state where an organization is free of unacceptable risk (Mihut, 2014).

Assumptions

Several assumptions are considered in this research. First, there is an assumption that the Delphi participants are experts in their fields of disaster recovery or cybersecurity

and have sufficient knowledge about disaster response to propose solutions for the problem. Each participant was selected based on interviews, recommendations, or their visibility as a researcher in this subject matter. There is an assumption that the participants would answer the questions from the Delphi design truthfully and provide clear communication on answers that were deemed outliers from the Delphi round. I assumed that participants who stayed for all three rounds of the study and, when asked to provide additional data about an outlier, I gave the participant the proper amount of time to give an answer. This study was a qualitative study to obtain rich, descriptive data. Participants were guided through each round of the Delphi design and allowed a window of time to provide their responses to keep the rounds allocated to a reasonable timeframe to complete the study.

Scope and Delimitations

The participants of this study were selected from disaster recovery programs for businesses that are large enough to plan regularly, conduct testing and have experienced an interruption from computer crimes. Organizations including Information Systems Audit and Control Association (ISACA), Information Security Certification (ISC2), Information Systems Security Association (ISSA), Cloud Security Alliance (CSA), and the InfraGard were contacted for applicable participants in the United States. Experts from the disciplines of emergency management, information technology disaster recovery, and cyber resiliency were asked to rate qualitative indicators using the Delphi design. I targeted experts from medium to large business in the United States. To reach a quality panel of experts across the United States, I collected data via electronic mail. The

ability to leverage the Internet allowed for the panel to have flexibility when they provided data and the ability to reflect on their answers. When interviews were identified as necessary, Internet-based video or a conference call was used.

The role of the researcher in the data collection process is to facilitate the multiple rounds of the Delphi design and conduct interviews for outlier concepts after the Delphi rounds are complete. Researchers have the unique ability to increase an understanding of how participants experience the phenomenon being studied, which provides valuable data for the research. I narrowed and filtered data as it was collected, without altering the data, to be analyzed into patterns or themes theories, as recommended by Maxwell (2013). To reduce the threat of bias in this research I performed triangulation with data collected from participants and data found in the literature. Special attention was paid to collect participant data in each round of the Delphi and conducted interviews.

For each round of the Delphi, the consensus was sought, and answers to the questions were provided to the panelists for review and adjustment when requested. As the data collection process from the Delphi study is electronic, presentation, importing, and archiving were simplified. Okoli and Pawlowski (2004) highlighted a significant value of the Delphi design is in the ability to produce theoretical research. Zahidy, Azizan, and Sorooshian (2016) wrote about the Delphi design being suited for a study where there is incomplete knowledge about a problem where there are no correct answers or incomplete knowledge.

I chose the Delphi design to provide for greater access to disaster responders across multiple businesses and service offerings, anonymous responses, and the ability to

produce theoretical data for an improved information technology disaster recovery response. Interviews were conducted with certain participants for interesting disparities to understand the deviation from consensus. Like disaster recovery planning, a Delphi study by Pieko (2005) was successfully used to improve the quality of information technology security audits. The panel of experts was asked to rate indicators on a Likert scale from 1 to 6 which were divided up into several categories such as data destruction, resiliency, and disaster planning issues.

Limitations

The research was limited to the disaster recovery and cybersecurity participants' understanding of information technology disaster recovery and cybersecurity incident response. The research included how disaster recovery teams and cybersecurity teams could better plan for and resume the organization from a computer crimes interruption. My focus for the research study did not include the motive behind the cyber attackers, describe the type of individuals or groups that comprise cyber hackers, or developed a method for preventing the attacks. The findings from this research may not apply to all organizations. I assumed that applicable organizations would have information technology disaster recovery programs in place and the findings may not apply to very small enterprises without dedicated incident responders or cybersecurity staff.

Significance of the Study

The research presented by the study is unique in that it is focusing on an under-researched area of information technology disaster recovery. The existing literature on disaster recovery has yet to collaborate cybersecurity response to the traditional

emergency response. The ability to recover quickly from a technology interruption is crucial, and the need to prepare for computer crimes may not be as adequately addressed as possible. The results of the study may provide insights into what areas of information technology disaster recovery are weak as it pertains to computer crimes and what areas can be supplemented. The findings may have a significant influence on how disaster planning is conducted for organizations that have a strong reliance on technology infrastructure. The study could have a significant influence on a business that experiences significant computer crimes related interruption and could recover in a manner as to limit the impact of the business offering and minimizing financial loss.

Building a new understanding of an information technology disaster recovery framework that focuses on traditional business interruptions and security responses that assist in resuming computer crimes would be beneficial to disaster recovery planners, disaster recovery responders, and business owners. Organizations that rely on a significant foundation of technology infrastructure may be able to apply or assess the gap between their existing traditional disaster recovery methods and the new knowledge being created in this study. The research presented in this study should be read by disaster recovery managers, technology first responders, and business continuance planners for the knowledge being created to improve the response to an emerging threat.

Significance to Practice

The ability to recover an organization's data processing is directly related to the prosperity of the organization (Marinescu, 2015; Mossburg, 2015). The improvement of disaster recovery practices to respond to computer crimes offers an advantage to disaster

recovery programs. Providing better planning and procedures to incident responders should allow for reduced resumption times.

Significance to Theory

Information technology disaster recovery has been historically based on methods borrowed from medical first response and military emergency management from the battlefield. Guidry et al. (2015) and Ferdinand (2015) discussed the lack of organizational understanding of how a disaster management program could modify measures to account for computer crimes interruptions. Using the Randeree et al. (2012) and Stewart et al. (2015) disaster recovery maturity model conceptual framework can allow for the measurement of the effects of this study to improve organizational response to a technology disaster. Supplementing the existing disaster recovery frameworks with new controls to mitigate emerging technology risks provides an opportunity to modernize the practice of information technology disaster recovery.

Significance to Social Change

The experience of information technology disaster recovery experts and cybersecurity experts represents a section of information, which could facilitate a change in the response and recovery from technology disasters. Technology disasters are a risk that is increasingly affecting organizational survivability. Keeping a viable business following a technology interruption, assists in the profitability of the organization and the employees remain on the payroll. By improving the disaster recovery response to an event, a community that is relying on vital services from the affected entity will experience a reduced interruption as opposed to a prolonged disturbance. Hospitals,

emergency response, local law enforcement, and transportation are examples of vital services that can leverage an improved information technology disaster recovery response to service the local community. Responses to disasters such as an earthquake can reveal parallels for organizations recovering from technology disruptions. This study of computer crimes as it pertains to disaster recovery is a relatively new topic and this research places organization in a better position to respond to an emerging threat.

Summary and Transition

The purpose of this qualitative study was to understand how information technology disaster recovery controls and processes can be modified to improve response to a computer crime caused business interruption. The risks to organizations continue to rise as new technology threats emerge and more business processes rely on data processing. Information technology disaster recovery must improve and cybersecurity incident response may provide new methods that can be collaborated to reach a more mature disaster recovery program. A better understanding of cybersecurity in the context of disaster recovery may allow disaster recovery planners to improve their organizational resumption processes. In the next chapter, I present a literature review I conducted on the theories and practices for disaster recovery practitioners, review of the applicable law and regulations for disaster recovery, information security frameworks, and the common threats to organizations. The literature review describes where the information technology disaster recovery concept has evolved and where the current research is being conducted in response to computer crimes. Chapter 3 includes the research methodology and the use of the Delphi design.

Chapter 2: Literature Review

Businesses unable to quickly recover from a technology-caused interruption will find significant barriers to servicing their customers and maintaining an advantage over their competition. Critical technology infrastructure must be resumed to an acceptable operating state that allows the service to the client. As technology becomes more embedded in the core of business processes, the vulnerability to organizational interruptions as technology fails to operate as expected becomes greater. Traditional disaster recovery placed a high priority in recovering from the loss of power, fire, and flooding. As the expertise of the underground criminal increases, the ability to cause a technology interruption upon a business becomes a greater risk. Information technology disaster recovery is primarily concerned with the minimizing of the interruption of business operations, the risk of delays, ensuring security, producing a reliable data backup, and restoration promptly. The management of the recovery activities plays an important role in restoring the business after it has experienced an interruption. Chapter 2 includes a literature review of emergency management, information technology disaster recovery, business continuance planning, cyber-attack interruptions, information security practices, technology frameworks, and laws about disaster recovery. The literature examined in this chapter was collected from disaster management books, online repositories, disaster recovery journals, research studies, and disaster conferences. The purpose of this literature review was to gain insight into the process, people, and threat vectors that are considered when building and maintain an information technology disaster recovery program.

Literature Search Strategy

The search strategy for this review collected the primary sources from seminal books, peer-reviewed journals, standards body websites, and federal government websites. The *Journal of Information Systems & Operations Management*, *Journal of Business Continuity & Emergency Planning*, Centre for Disaster Management and Hazards Research, *Disaster Recovery Journal, Disaster Prevention and Management*, and *Computers & Security Journals* are focused on for the relevant research in the last several years. Additional journals were obtained from ProQuest, Business Source Complete, InfoSCI, and ABI/Inform Global. The keywords used in the search were *business continuity planning, crisis management, cyber resilience, cyber terrorism, data breach, disaster preparedness plans, disaster resilience, emergency response management*, and *enterprise risk management.* The range used in the search was limited to 5 years and less from the anticipated time of this dissertation completion. I used this strategy to identify the risk of cyber-attacks on organizations ability to recover systems and the need to incorporate information security practices into the management disaster recovery programs. The relevant articles were reviewed for application to the topic, credibility, dependability, and transferability. I created Figure 1 to show the order and method of the topics researched.

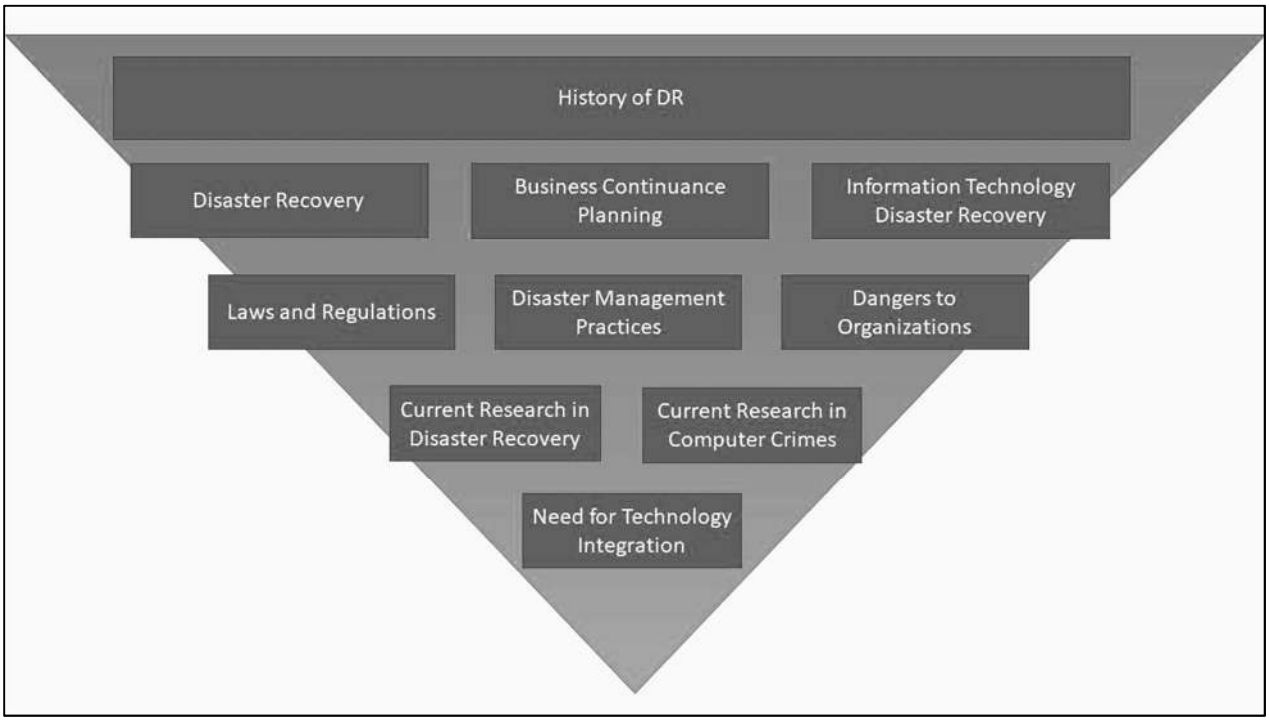

Figure 1. The literature review method to understand the impacts of computer crimes.

Conceptual Framework

Recent headlines describe the increasing damages and disclosures caused by cyber criminals and yet organizations are still lacking the necessary controls and methodology needed to prepare for technology disasters (Rittinghouse & Ransome, 2011). A capability maturity model (CMM) has been a popular tool for the development of an improvement program to transform an organization into a better operational state. The purpose of a maturity model is to provide understanding for improving processes for development and maintenance of products and services. The six common capabilities are incomplete, performed, managed, defined, quantitatively managed, and optimized (Barclay, 2014). Maturity model focus can include technology, a business initiative, or a financial process (Latif, Arshad & Janom, 2016). A process of dependability can be

determined using a maturity model, which assumes the positive movement towards a goal in stages (Dorfman & Thayer, 1997). A popular way to evaluate the levels of a maturity model is a five-point Likert scale as first seen in the Carnegie Mellon Capability Maturity Model Integration (Latif et al., 2016). Leveraging a maturity model may provide a greater understanding for improving processes that respond to computer crimes caused disasters.

One method to improve the standing of an organization's disaster management is the use of a disaster recovery maturity model (DRMM). Allen et al. (2015) encouraged organizations to use defined maturity model, such as the CERT-RRM, to measure progress and to assess their programs. Stewart, Allen, Dorofee, Valdez, and Young (2015) claimed that a disaster recovery program's effectiveness comes from direction and approval from the executive levels of the organization. The DRMM is used as a tool for assessing the capability of the disaster recovery program (Al Hamed & Alenezi, 2016; Lindström, Samuelsson, & Hägerfors, 2010; Randeree et al., 2012; Stewart et al., 2015). The DRMM provides the ability to communicate outcomes with ease based on the data ranking in the model, allows organizations to recognize shortfalls, and the identification of improvements over time. The ability of the DRMM to provide dashboards and metrics that can be reviewed by executives provides a mechanism to justify the DR investment and the organizational readiness for implementing a business continuance program. A DRMM should eliminate subjectivity, reduce disaster planner bias, and provide a clear picture of an organization's stance towards readiness. Lindström et al. (2010) explained the need for a less abstract way for senior management to understand disaster recovery and to use a concept that would be familiar with a common decision-making tool.

Randeree et al. (2012) claimed a maturity model proposes a life cycle that is explicitly defined, managed, and measurable. By using a disaster recovery maturity model, an organization may identify strategic areas where improvement could be made to amend the recovery from computer crimes.

The process of the maturity concept implies growth in the process, capability, and consistency of the program. Al Hamed and Alenezi (2016) proposed a model based on their research that consisted of an evaluation of a process quality dimension versus a scope capability dimension. The vertical axis represented the maturity stages from initiated, planned, implemented, controlled, integrated and optimized. The horizontal axis represented maturity stages where each stage builds on the previous level. The Carnegie Mellon University's Software Engineering Institute developed the CERT Resilience Management Model (CERT-RRM), which focuses on enterprise management of operational resilience (CMMI, 2007; Lindström et al., 2010). The CERT-RMM defined processes for 26 functional areas that are organized into enterprise management, engineering, operations and process management. Stewart et al.'s (2015) research used the CERT Resilience Management Model to define a more granular maturity scale for organizations that need a greater depth of detail than the original CERT-RMM. The Allen (Dorofee et al., 2015) model defined four maturity levels of incomplete, performed, managed, and defined with an additional component of Maturity Indicator Levels (MIL) for describing upward progression. The MIL was described as incomplete, performed, planned, managed, measured, defined, and shared. Lindström et al. (2010) research intended to improve the process of explaining BCM to senior management by increasing

the organizational understanding of the current disaster recovery maturity level it belongs to and what is required to improve the standing of the current level. The staircase methodology presented by Lindstrom was applied at the organizational and department level to highlight risks that are deemed necessary to mitigate known disaster events. Randeree et al. (2012) proposed a disaster recovery maturity model developed using focus groups with 10 United Arab Emirates banks and their BCM experts. Randeree, et al. argued that the BS25999 BCM standard missed necessary components of a framework for organizations to benchmark themselves as a maturity model is necessary for measurement. The U.S. Department of Energy Cybersecurity Capability Maturity Model (C2M2) is a public-private effort established to improve the energy sector's cybersecurity capabilities (Department of Energy, n.d.). The C2M2 is comprised of three cybersecurity capability maturity models. With the capability maturity model being a popular tool for the improvement of a program, organizations should consider the use of a disaster recovery maturity models to improve the disaster response to computer crimes.

The topic of the effects of computer crimes on disaster recovery was examined, through the lens of a DRMM, throughout the literature review. The multiple levels of the DRMM represented the ability to recover the organization, which allowed for the analysis of methods that could improve the disaster response to a technology caused service interruption.

Literature Review

History of Disaster Recovery

Disaster planners, first responders, and organization management teams should understand how information technology disasters came to be an important aspect of organizational risk management and how disasters have affected organizations over time. A disaster can be experienced in many degrees of severity and, according to Lord (1981), should be approached through a lens of contingency planning. An up to date, well-rehearsed disaster recovery plan can be the difference between restoring to a state of normalcy in a matter of hours or restoring the system in months or years (Hiatt, 2000).

Emergency management. Emergency management seeks to control the activities of evacuation, recovery, and relocation of people and resources. Development of an emergency management plan requires a role of a recovery coordinator to designate teams and responsibilities to various recovery tasks. Without an emergency management plan for coordination of activities, inefficiencies will lengthen the time to resume the entity. Emergency management has been identified as an aspect of disaster recovery that is often difficult for disaster responders (Togio, 1989). Existing research on emergency management tries to understand organizational interactions, the analyzation of key indicators, and the critical structures within the event (Kapucu & Hu, 2016).

To assist the public sector in the United States, the Federal Emergency Management Agency (FEMA) was placed into existence by President Carter's 1979 executive order 12127 to provide disaster-related responsibilities into a formal government agency. The creation of FEMA consolidated the Federal Insurance

Administration, National Fire Prevention Administration, National Weather Service Preparedness Program, Federal Disaster Assistance Administration, and components of the Defense Civil Preparedness Agency (Cutter et al., 2016; FEMA, 2017). The FEMA mission statement is to provide the support, tools, and resources to ensure that the agency can build, sustain, and improve the capability to prepare, protect, respond and recover from all hazards. Cutter et al. (2016) explained that FEMA, in the beginning, was focused on attacks from abroad and then evolved to a focus on natural disasters under President Clinton, and back to security and counter-terrorism planning under President Bush. Kapucu and Hu (2016) claimed intergovernmental and cross-sector collaboration had become the norm in emergency response due to the necessity of sharing resources. With the development and maturity of emergency management in the government, efficiencies from a dedicated budget, staff and education should shorten the time to resume the impacted target.

Recent studies (Kapucu & Hu, 2016; Lachlan et al., 2016) have shown greater success in disaster response due to the building of collaborative networks between public, private, and nonprofit entities. Emergency planning teams for private organizations are often grouped into concentrations such as a software applications team, network recovery, communications, administrative support, offsite storage, and security (Togio, 1989). Corporate emergency management would plan the evacuation, recovery, and relocation of employees and readiness of alternative locations for conducting businesses. The use of planned, coordinated emergency management will place an organization in a better position to respond to the disaster.

Crisis communications. Latif et al. (2016) noted it is crucial in disaster management to communicate the right information to the right people in the right place at the right time. Effective communication is the key to successful recovery (Bartock et al., 2016; Bishoff et al., 2015). Houston et al. (2015) wrote that disaster communication is focused on strategies that can protect the organization's image during a crisis. A comprehensive communication plan will describe the phone calling decision tree of contacts, location of the continuance plan, basic communication script, who receives press releases, plan for providing updated information, and inform third parties. Bartock et al. (2016) claimed the most successful recovery teams would develop a clear and concise communications plan. Key stakeholders will need to be provided sufficient data about the disaster to understand responsibilities and decision-making steps. Key stakeholders are often defined as organizational management teams, external partners, technology teams, legal counsel, and customers (Bishoff et al., 2015). Failed communication channels must be considered during planning and document alternative solutions for use (Bishoff et al., 2015; Grigonis, 2002). Cloud communications solutions such as SIP trunking, fax services, text messaging, virtual contact centers, and interactive voice response are optimal alternatives for failed primary, on-premises solutions. Organizations that dedicate resources to identifying effective communication may find the key to successful recovery came from the communications plan.

A review of the crisis communication literature highlighted two common frameworks. The Crisis and Emergency Risk Communication (CERC) model and the Disaster Communications Intervention Framework were designed to protect an entities'

image and to improve an understanding of how leaders should respond to a disaster (Houston et al., 2015; Lachlan, Spence, Lin, Najarian, & Del Greco, 2016). Both models use disaster communications to prevent injury, promote calm, and direct the entities operational response. Research by Lachlan et al. (2016) and Matar, Matar, Balachandran, and Hunaiti (2016) indicated that organizations have new avenues via social media technologies that are likely to be utilized by affected audiences under disaster scenarios.

Technologies such as Facebook, YouTube, Reddit, or Twitter can quickly educate and inform audiences that otherwise could be harder to reach through traditional means of radio or analog phone calls. Research by Takahashi, Tandoc, and Carmichael (2015) found that Twitter is a popular communication tool for the public with the intent of assisting in the response and recovery efforts to the disaster. David, Ong, and Legara (2016) wrote that Twitter has shown to be a valuable channel of information for government and private sectors through the affected users posting updates, text, and photos. David et al. highlighted the emerging advantages of social media for crisis communications due to the features of information transmission, activity reporting, media content sharing, back-channel capability, rapid dissemination, and the sharing of experiences.

Traditional disaster recovery. Disaster recovery is often described as a response to natural disasters such as fire, floods, and earthquakes (Alexander, 2015; Tucker, 2014). Alternate descriptions include responses to human-made disasters such as hazardous spills, terrorism, and technology failures. The disaster recovery literature lists the four phases of disaster recovery as preparedness, mitigation, response, and recovery (Berke,

Kartez, & Wenger, 1993; Elliot, Swartz, & Herbane, 2010; Mojtahedi & Oo, 2017; University of Oregon, 2007). Disaster recovery often includes discussions on historic site preservation, transportation plans, capital improvements, economic stimulus, Red Cross Outreach, Health and Human Services programs, emergency operations, and natural hazard mitigation plans (University of Oregon, 2007). Disasters are more than common emergencies that are exhibited in car crashes or injuries to humans (Phillips, 2015). In a disaster, local resources are reduced, eliminated, or exhausted and will directly affect the community. Disasters can exist at a magnitude where state or federal agencies are needed for assistance. Emergency services, public works, city planners, elected officials, local business leaders, school districts, the local chamber of commerce, and department of transportation are frequently listed as stakeholders (University of Oregon, 2007). A disaster requires complex efforts for communities to recover (Philips, 2015). Commitment to recovery planning is essential if the organization implements a disaster recovery program (Bishoff et al., 2015). Research by the University of Oregon (2007) indicated that for every dollar spent on disaster planning, communities could save four dollars in response and recovery costs. In 1995, global disasters cost the insurance section over $180 billion (Hiatt, 2000) and in 2013, $3.6 billion of damage was attributed to tornadoes (Kantamaneni, Alrashed, & Phillips, 2015). Mojtahedi and Oo (2017) claimed the annual spend on disaster recovery activities has increased to $200 billion since the 1980s.

Mojtahedi and Oo (2017) believed that certain disasters could not be completely averted, even with proper planning and mitigating controls. Disaster insurance has

traditionally been utilized for limiting loss and as a transfer mechanism to allow organizations to be protected in the event of a disaster. Butler (1998); Rittinghouse and Ransome (2011) wrote that disaster insurance has historically focused on buildings and property and not designed to address technology needs. Modern technology risk has created new vulnerabilities and new management objectives requiring an updated insurance strategy from one a decade ago. Modern disaster insurance offers many plans for organizations recovering from a disaster that has affected their technology infrastructure (Siegel, Sagalow, & Serritella, 2002). A technology-focused insurance policy will provide superior loss prevention which dovetails with an enterprise risk assessment program. Determining the potential disaster and business impact allows organizations to choose the right policy for the specific needs of the industry.

Business continuance planning (BCP). In 1969, a small airplane crash created a disaster that crippled the Applied Data Research data center housing an IBM System 360 (David, 1969; Herbane, 2010). The Applied Data disaster is considered the first major incident that caused organizations to consider hardware alternative sites for data processing. Other researchers believed business continuance planning was developed with the changing landscape of technology at the core of business processes in the 1970's (Jedynak, 2013). Rittinghouse and Ransome (2011) believed business continuance planning was not about technology but a new way of managing a business functionality in all circumstances. In the late 1970s, Comdisco and SunGard housed more computing resources than was needed for their data processing needs and the companies decided to

lease out computing resources. Butler (1998) noted the Comdisco and SunGard concept was considered the launch of the modern backup, alternate data center.

Business continuance planning is not a new concept but has gained momentum in the last few decades. The initial interest in business continuance planning appeared in the 1950s and 1960s when organizations began to understand the criticality of certain business data and the risk of availability if a disaster was encountered (Randeree et al., 2012). In 1978 a seminal study at the University of Minnesota examined the maximum amount of downtime that can be tolerated by specific industries before the recovery would be impossible (Aasgaard, Cheung, Hulbert, & Simpson, 1978). The 1978 University of Minnesota study indicated that financial industries have the lowest tolerance for downtime and insurance and manufacturing could tolerate up to five days of interruption. Butler (1998) highlighted that in the 1990s the credit card and financial sectors would lose between $5.6 million to $7 million per hour in downtime. Hiatt (2000) claimed the business continuance planning process has evolved into an extensive set of tasks that is filled with various pitfalls where the best-intentioned, seasoned planners will unintentionally overlook critical processes. Planning is essential for organizations charged with reducing risk to a business interruption. Hiatt (2000) claimed a well-planned and rehearsed disaster recovery plan could mean the difference between an immediate recovery or a set of devastating repercussions that can bankrupt a business.

Alexander (2015), Grigonis (2002), Iqbal, Widyawan, and Mustika (2016), Lam (2002), and Rittinghouse and Ransome (2011) defined the business continuance life cycle as including the phases of enterprise risk analysis, business impact analysis, definition of

requirements for continuance, design of a continuance strategy, implementation of the strategy across the organization, development of plans for technology, people and premises, reoccurring testing activities, and continuous process improvement actions. I created Figure 2 to capture the major components of business continuance planning.

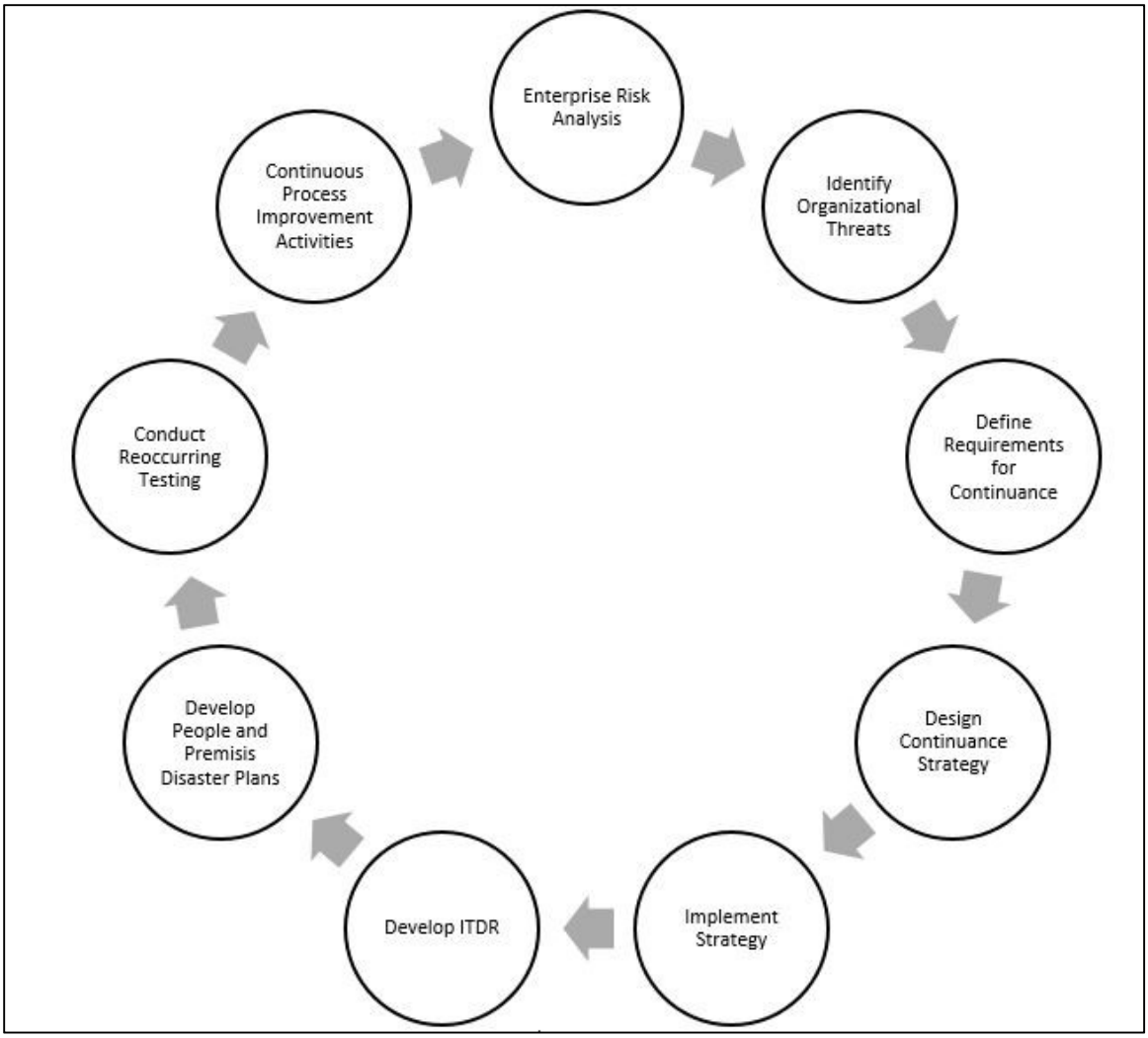

Figure 2. A typical business continuance life cycle.

The risk analysis activity or business impact analysis being conducted for BCP works to ensure that controls and expenditures are deployed in a way that reduces risk to

the organization following a disaster. Bartock et al. (2016) wrote that most activities of the BCP process come from the planning and documentation of the system before any event occurs. Lam (2002) wrote that organizations should consider technology threats, information threats, and people threats. When a risk analysis is conducted the organizations assesses the likelihood and impact of the threat occurrence (Bartock, 2016; Fallara, 2003; Grigonis, 2002; Lam, 2002).

The risk management process categorizes and prioritizes the threats according to risk levels and ascertains levels of risk that are acceptable to the organization. Organizations will need to consider which threats to ignore due to a significantly low likelihood or inconsequential interruption. Yang, Ku, and Liu (2016) claimed most organizations would use software tools to perform risk-based compliance analysis. Organizations have options when dealing with risk. Risk response is a component of the business continuance risk analysis. Organizations have options for a risk response in avoidance, transference, mitigation, and acceptance (Bhoola, Hiremath, & Mallik, 2014). Bhoola et al. claimed the identification of risks alone would not ensure the success of the project, but an implementation of a risk response plan offers greater protection when the risk is needed to be mitigated. Avoidance is often leveraged in a manner that has the project being implemented in a way that the identified risk will not be encountered because of changes to the plan eliminate the probability of the risk (Bhoola et al., 2014; Lam, 2014). Risk transference will place the responsibility of the risk component with a vendor or alternative stakeholder (Lam,2014). Risk mitigation reduces the risk by applying a solution to reduce the vulnerability or threat (Bhoola et al., 2014).

Organizations looking to mitigate the risk of a loss of power incident will deploy uninterrupted power supplies to supplement the loss from the utility provider. Risk acceptance recognizes the risk that remains after controls have been applied. McManus (2003) pointed to the documentation of an evaluated risk as an advantage in the planning process. Organizations that have a good understanding of how different risks will be controlled have an advantage when it comes time to recover from an interruption.

Al Hamed and Alenezi (2016), Butler (1998), Fallara (2003), Grigonis (2002), and Torabi, Soufi, and Sahebjamnia (2014) defined the business impact analysis (BIA) as the activity that identifies critical functions and determines supporting resources for critical business processes. Identification of business threats provides an understanding of how resources can be affected by a disaster and the BIA should be used in decision-making when formulating resumption plans. The BIA is a key part of a business continuity management system (BCMS) because the activity collects key processes and critical functions to calculate the minimum business continuity objective (MBCO) and the maximum tolerable period of disruption (MTPD) according to Al Hamed and Alenezi (2016). Torabi et al. (2014) research revealed that the data gathering and data analysis phases are the two most time-consuming steps of the BIA. The main advantage of the BIA is the early identification the risks and the data provided on requirements for a continuance. Data from the BIA feeds into the subsequent phases of business continuance planning. The risk analysis process is significant because most of the remaining planning components will leverage what was indicated in the risk analysis phase.

Testing is a major consideration in BCP as the activity will directly improve the accuracy of the execution of the plan. Lam (2002) wrote that there are four main reasons to test the business continuance plan, which included the validation of the effectiveness of the stated service levels, identification of any shortcomings, assessment of the service levels being achievable and realistic given the time constraints, and to provide confidence in the plan. BCP testing should address as many applicable, conceivable disasters as possible but still assume that the actual disaster will be a scenario that was not specifically tested. Stanton (2005) argued that having a technology disaster recovery processes is not the equivalent of having a complete business continuance plan in place. Butler (1998) and Hiatt (2000) claimed business continuance testing of a resilience plan would not completely align with what a real disaster will exhibit, and organizations should consider that. Alexander (2015), Bartock et al. (2016), Fallara, (2003), Rittinghouse and Ransome (2011), and Wold (2002) wrote that testing activities should be implemented at a frequency that applies to the organization, has realistic objectives, and assigned responsibilities to test the hypothetical disaster adequately. Organizations that plan and execute on recovery testing will have a more accurate and practiced resumption plan than an organization that does not.

Lessons learned is a major component of BCP. Bartock et al. (2016) and Hiatt (2000) claimed periodic testing and disaster recovery exercises should be continually scheduled to identify improvements from the lessons learned during the testing. The lessons learned activity assists improvement in the recovery process and provided a feedback mechanism for decision-making. The timing of the activity can be a factor in

quality. Bartock et al. (2016) wrote the longer the period between testing and the lessons learned activity, the less likely the lessons learned will be accurate. Togio (1998) presented some guidelines for disaster planners to maximize the effort of training the responders:

- Disaster planners must develop a rapport with team leaders.
- It is important to package the information in short, digestible amounts.
- Target the audience for the proper level of terms and language.
- There should be an attempt to address all questions to the extent possible.
- Give team members copies of the sections that apply to them for their review to return comments or suggestions.

Testing frequently and a timely review of the outcome can improve the disaster recovery program.

Alexander (2015), Bartock et al. (2016), Rittinghouse and Ransome (2011), Thejendra (2014), and Tucker (2014) wrote that a critical component of the recovery comes from having guidance, playbooks, and plans to support the stated organizational recovery objectives. Hiatt (2000) and Rittinghouse and Ransome (2011) listed several common recovery plans that included contingency, business continuance, business recovery, continuity of operations, technology contingency, crisis communications, and incident response. Written guidance and plans are often necessary because of the large number of business processes that need to be recovered, clarity needed on what response teams are assigned what actions, identification of the critical systems that must be addressed according to the business, and the proper order of resumption. Clearly written

playbooks that can be immediately accessed during a disaster offer a large advantage to an organization as opposed to resuming business processes from management's experience managing the procedures.

The use of a continuance strategy improves the chances of proper resumption. The business continuity planning body of knowledge has provided multiple frameworks and strategies described later in this chapter. Bajgoric (2014), Grigonis (2002), and Rittinghouse and Ransome (2011) concluded that a BCM strategy, when organized and managed properly, would improve the performance of the recovery. The ISO17799 is an international standard for business continuance planning and covers ten domains that can be modified to accommodate most any business planning requirements (Aronis & Stratopoulos, 2016; Choudhary, 2016; Junttila, 2014). Organizations looking to improve the response to a disaster should consider the adoption of a BCP framework.

Information technology disaster recovery. Rittinghouse and Ransome (2011) noted that leading up to the middle 1970s, most companies had no form of technology-focused disaster recovery but instead relied upon traditional business insurance to mitigate the losses to property. By the mid-1980s organizations had started planning for alternate datacenters and by the 1990s recovery plans encompassed resilient networks (Butler, 1998). Butler pointed to a new urgency of recovering from a disaster because of the expanding role of technology found in critical business processes. The loss of technology resources, reliability, or integrity of data can interrupt the normal processing of business data. The Business Continuity Institute (2013) Horizon Survey reported in

2013 40% of a sample of 730 international organizations was significantly disrupted by a technology-induced outage.

Bajgoric (2014) argued that disaster recovery is typically part of a larger business continuance program, which includes services outside of the technology department. disaster recovery has become more relevant because of the growing need for computers in business. Alexander (2015) and Neaga, Winters, and Laufman (1997) defined an information technology disaster recovery disaster as an extended service interruption for an organization where data processing could not be conducted and correction not available within an acceptable time frame. Butler (1998), Hiatt (2000), and Togio (1989) defined the technology disaster as an event that interrupts the business because of the loss of critical information needed in data processing. Bishoff et al. (2015) claimed disasters are not limited to physical phenomena but events that inflict the whole business ecosystem. A generalized workflow for information technology disaster recovery is defined in Figure 3. Although disaster recovery can be conducted outside BCP, disaster recovery can leverage requirements gathering, data collection, risk assessment, stakeholders, and planning from a larger business continuance planning program. Figure 3, which I created, describes the components of information technology disaster recovery.

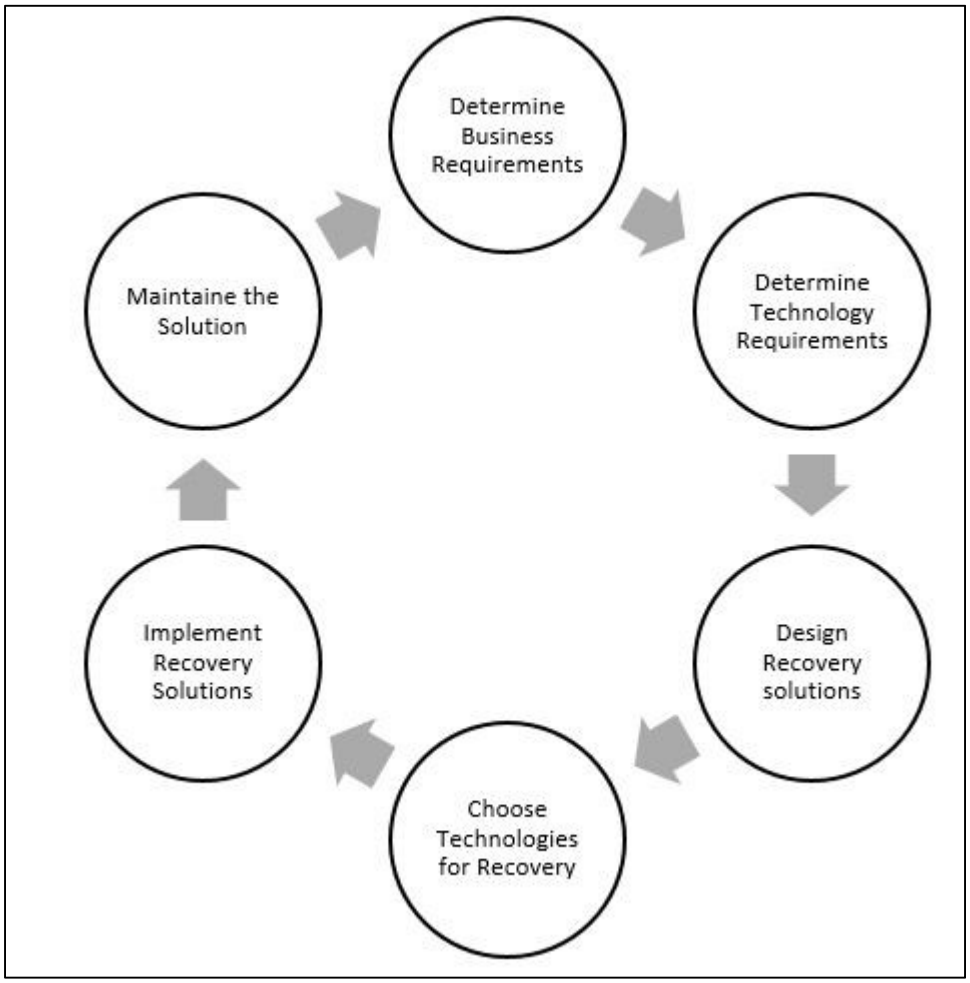

Figure 3. Typical disaster recovery cycle for interruption planning.

Traditional disaster events such as fire, floods, loss of power, earthquakes, and hardware failures can represent a significant risk of an interruption of a business's data processing. Neaga et al. (1997) predicted that as organizations become more dependent on data processing, the availability aspects of technology become increasingly critical. In the mid-1970s, operating a computer mainframe such as the IBM 370 system placed the main computing hardware in a datacenter far away from the end users who were using dumb terminals. With the mainframe system in a single location, securing and preparing

the mainframe for disasters was an easier solution than the inexpensive, distributed computing now available. Information technology disaster recovery for the 1970s-era mainframe had the disaster planners seeking hardened data centers, daily backups, and alternate locations for migrating the mainframe (Grigonis, 2002). The 1980s introduced the workstation and the client-server model of distributed computing. These added complications to the disaster planner because now computing was being conducted at multiple locations and within reach of the user. Disaster planners in the 1980s needed to understand how to best provide recovery for not just the mainframe and data center, but the workstations and the unstructured data that was being created outside the datacenter. Present day disaster recovery planners focusing on information technology disaster recovery may consider many technologies such as resilient networking, data in the cloud, data in a private datacenter, server hardware, storage area networks, electronic data interchange (EDI), personal computers in an office, mass media devices, where critical data may reside, enterprise printing, and information and communications technology (ICT).

The alternate data center can be an important component of an organization's recovery effort. Lord (1981), Neaga et al. (1997), and Rittinghouse and Ransome (2011) noted the decision to operate an alternate data center site was vital for organizations to consider when a fast recovery was required. Several things must be considered when operating an alternate data center. The alternate site is often defined as a cold standby, a warm site with no staff, or a hot site with full-time staff (Fallara, 2003). A cold site can be minimalist building with environmental controls ready to take equipment to a site with

some equipment but ready to be quickly built into a production environment. Thejandra (2014) argued the cold site could be a non-IT facility that can be used for an extended period. A warm site will have the technology equipment, but disaster recovery efforts will need to be completed in major tasks to resume the system. A host site will normally operate in an active-active state where data processing can be computed in the primary data center or the alternate data center with only minor configuration changes (Jones, 2007; Thejandra, 2014). Hot sites will have near real-time backup data from synchronization processes to ensure the data is available if there is a loss of a data center. Distance is often discussed as a factor in determining where the alternate data center can reside. Neaga et al. (1997) claimed you could have alternate sites in the same building with fire being the only major risk. Jones (2007) argued that distance between data centers was critical to avoid disasters from power grid failures, hurricanes, flooding, and supply chain and distribution disruptions. The choice of a recovery site is an important decision-making action. Organizations must choose the applicable strategy that can maximize the use of the monetary investment in the data center. Recovery capacity and availability of resources, during the interruption, must be considered for operating the critical data processing and business processes.

The return on investment (ROI) is often discussed when disaster recovery is being budgeted. Cybulski (2016), Hiatt (2000), Million (1997), Sarmiento, Hoberman, Jerath, and Ferreira Jordao (2016), and Stanton (2005) argued the return on investment for disaster recovery makes good business sense, and when a single event triggered the response activity, the investment has been realized. The initial cost to an organization to

start the planning process is a small investment in employee time to start the planning the risk assessment phases of an disaster recovery framework. Sarmiento et al. (2016) wrote the benefits from the BCM understanding how intangible components of the business impact tangible decision-making can reap relevant ROI results. Stanton (2005) argued that standard ROI calculations may not apply. Similar to the purchasing of insurance, until the organization experiences the need to recover the business the ROI will not be obvious. Once the disaster event is experienced, and the BCP program is leveraged, the investment is justified (Sarmiento et al., 2016). The better argument for ROI may come from the focus being placed on interruption risks to assure customers and partners that the organization has placed priority on reducing risks to an acceptable level.

Traditionally the information technology risk assessment for disaster recovery has been identified as a responsibility of the technical staff because they would have the best understanding of what technologies comprise the infrastructure. Moreover, technology risk assessments have typically been performed within the technology department with little input from other departments. Schmitting and Munns (2010) claimed that a traditional business risk assessment method had reached a limitation as technology systems have become more complex and integrated into all aspects of the business. Hiatt (2000) claimed that a technology risk assessment assists in planning, can improve the business, reduce recovery problems, and produce better-managed disaster recovery controls. The technology risk assessment may differ from traditional risk assessment depending on the business sector. A technology risk assessment includes identifying a large sample of technology threats, which include hacking, malicious administrative

insider, computer fraud, the value of various types of data, and disasters affecting technology infrastructure that would not normally be evaluated under a traditional risk assessment (Schmitting & Munns, 2010). An information technology risk assessment can be aided by recognized guidance from existing works such as the ISACAs IT risk practitioners guide, CERT Guide to Threats, Council on Cybersecurity critical security controls, NIST cybersecurity framework, and the OWASP top ten. The ISACA defined the objective of the technology risk assessment is to understand the security requirements, connected network architectures, information available, physical assets available, the location of data repositories, applications in use, security components, authentication mechanisms, regulation the organization must adhere to, and what documented policies are used. Lanz (2015) argued that information technology risk is like traditional audit risk and managers should consider the combination of detective risk strategies and technology controls to reduce risk to an acceptable level. Lanz recognized that firms might need to bring in a technology resource to address the cyber-risks and complexities that may not be present from traditional audit staff. Each organization will be different. Thus the decision of how to conduct the information technology risk assessment, what to include, and how the risks will be prioritized will be dependent on how that organization has their technology deployed.

The basic information technology disaster recovery planning contains recovery scoping, processes and procedures for specific technologies, business impact assessment actions, rules for invocation, identification of team's responsibilities, backup strategies, restoration procedures, stakeholders, plan maintenance, and required testing (Lam, 2002;

Lord, 1981; Neaga et al., 1997; Rittinghouse & Ransome, 2011; Wold, 2002). Butler (1998) claimed that most companies perform the least amount of disaster recovery planning as possible and ignore the potential for disasters. Instead, many organizations rely on redundant networks and computers to keep the data processing functioning. In designing the plan, organizations will identify critical business services, establish recovery time objectives, affirm key constraints, identification of possible strategies, and the drafting of plans to meet senior management's goals. Disaster plan scoping is an important concept in the planning process.

The purpose of scoping is to gain a clear understanding of what systems the information technology disaster recovery program will recover. Butler (1998) argued that the recovering of computers and data following a disaster was no longer sufficient for modern businesses as disaster recovery plans must now take into consideration all critical business operations that use the same technology. Organizations must have a clear understanding of the scope of the technology being resumed, or there will be a gap in the disaster response.

Whether the disaster is sudden or an emanate event is on the horizon, human judgment is needed to decide when to act on the disaster planning. The purpose of planning for invocation is for the disaster recovery teams to understand when to stand down and when to put the plan into action. A routine problem or maintenance downtime should not be eligible to be a disaster and have the plan invoked. A data center power anomaly may not invoke the plan, but a prolonged power outage that cannot be restored before the uninterrupted power supply (UPS) fails may deem acceptable to invoke the

plan. Hiatt (2000) and Thejendra (2014) wrote the decision of an emergency management team or assigned figurehead, using the best available information, should be the authority to invoke all or part of the plan. Hiatt (2000) and Toigo (1989) listed principles that can be used contribute to the decision-making process to invoke the plan:

- Can the organization maintain routine operations?
- Can the damage be contained without affecting normal operations?
- Are facts about the disaster being taken at face value and without bias?
- Can the organization coordinate activities ahead of time to mitigate the risk?
- Is this solely a technology problem?

Defining the point at which the organization will failover will differ depending on the organization and the disaster. An advantage is leveraged when the organization has a defined set of disaster scenarios metrics where the plan will be invoked when experienced. Many organizations will have comprehensive, traditional disaster recovery program but will be likely to invoke the plan only for very significant outages lasting greater than a day. For those organizations in this state, invoking disaster recovery is seen as a significant task and in dealing with the disaster plan is considered the lesser of two evils.

Testing is a significant component in the quality of the information technology disaster recovery program. Butler (1998) claimed the purpose of conducting disaster recovery testing is to determine if the plan is working as expected by the stakeholders. Lam (2002) highlighted the need for technology testing to rehearse the schedule of events, assess the plan, identify the weaknesses for improvement, and to ensure the

distribution of the plan is at the correct levels. Neaga et al. (1997) pointed to research indicating that during an actual disaster event the plan is rarely executed as planned. The purpose of testing is to provide revisions to the plan that will mirror the changes being conducted in the infrastructure and applications over time. No disaster plan is foolproof, and there are limitations to disaster recovery strategies. Testing should include unannounced drills, conducted during various times, targeted destruction, documentation of test results, and a corrective action plan written (Butler, 1998). Hiatt (2000) wrote that the only way to get reasonable assurance that the plan will produce the expected results is to test the plan. Plans can be tested by conceptual group activities such tabletops or field-based simulations that will walk through the documentation and plans to understand how the response will be conducted on paper. Alternatively, plans can be tested with an activity to failover the organization's primary to the designated alternative business processes and locations for a period (Hiatt, 2000; Togio, 1989). Testing is important because of the living nature of disaster recovery planning. As Togio (1989) pointed out, plans must be maintained and tested to keep up with the ever-expanding technology embedded in business processes.

The development of written disaster recovery policies and procedures should be conducted for managing all major applications, technology infrastructure, data centers and critical processes that rely on technology. Rittinghouse and Ransome (2011) and Wold (2002), wrote the disaster recovery plan should document the before, during and after the activity of the affected system, application or datacenter. Rittinghouse and Ransome commented that the documentation would normally overlap with other

components of the business continuance plan and redundancy should be removed. Butler (1998), Fallara, (2003), and Wold (2002) highlighted the importance of executive management understanding and agreeing to use the written policy. The act of writing the policy solidifies the work that has been conducted in the phases of the disaster recovery lifecycle. Wold (2002) claimed that it is advantageous to an organization to develop pre-formatted policy templates to facilitate the writing process and provides consistency to the teams using the plan. The written disaster recovery plan organizes the detailed procedure, identifies chronological steps, and provides a roadmap for the maintenance or creation of policies. A thoroughly developed information technology disaster recovery plan will consider the team approach and have assignments for functional components of the resumption.

Laws and regulations influencing disaster recovery.

In the U.S., presidents, federal, and state legislators have written several laws, regulations, and executive orders influencing the disaster recovery field over several decades. The regulations span from protecting public confidence to assisting communities to recover from natural disasters. In some cases, the regulation applies to government agencies while another regulation is assigned to the private business. This literature research reviewed several applicable statutes but what is discussed is not intended to be a comprehensive list. Organizations should consider the regulations that may be applicable and if the intent of the regulation is being met by the controls in place.

The Securities Exchange Act of 1934 instituted an internal control mechanism for corporations that placed responsibility on executive management for maintaining

adequate controls over financial procedures and reporting (Law & Robson, 2014; SEC, n.d.). The Exchange of 1934 act was passed to provide the public with confidence in the financial data being presented and overseen by the Securities and Exchange Commission (SEC). Benston (1973) wrote that the financial legislation is believed to have forced organizations to pay closer attention to how financial data is generated, and more importantly retained to mitigate loss from a disaster. The mid-1970s to the 1980s marked the appearance of several regulations that were created which included disaster management concepts for public organizations. These regulations would lead to the business continuance movement known today. Dietel (2015) described the Flood Disaster Act (1973) as the major introduction of disaster recovery plans to organizations that would directly impact the communities where they existed. The Flood Disaster Act allowed the government to offer subsidies to owners that accepted the requirements of the program. The Flood Disaster Act intended to reduce flood damage throughout a community by introducing an insurance mechanism (Dietel, 2015). The United States Foreign Corrupt Practices Act (FCPA) (1977) was a separate implementation of disaster recovery planning for organizations. Elliot, Swartz, and Herbane (2010) claimed the FCPA required public organizations to have internal mitigating controls to safeguard assets from a disaster. Schreider (1996) wrote that the disaster recovery aspects of the FCPA come in the *Standard of Care* wording that evaluated organizations on mismanagement of data. The Office of Comptroller of Currency's Banking Circular BC-177 (1983) regulated financial institutions to implement disaster recovery plans. Hall (1989) and Schreider (1996) described the BC-177 as a control that made banks prove to

an examiner that a disaster recovery program was in place, had been tested, and it was likely to succeed. The BC-177 was important because it made bankers aware of the importance of a disaster recovery program. The United States Expedited Funds Availability Act (1989) added to the need for disaster recovery and business continuity plans in U.S. federal chartered financial institutions (Dahlberg & Guay, 2015). The Federal Reserve (2016) defined the requirements for next-day availability and the need for the institution to make transactions available by the next business day. The Comprehensive Environment Response, Compensation and Liability Act (CERCLA) from 1980 were written to address the cleanup efforts following a human-made or natural disaster (Revesz & Stewart, 2016). Davis, Strell, and Wallace (2005) wrote that CERLA is well suited for responding to natural disasters because it was written to apply to a wide array of substances including water, soil, and air. A critical component of Section 104(a) of the CERLA defined the government authority to act when the substantial danger to the public is determined (Davis, Strell, & Wallace, 2005).

New regulations emerged in the 1990s that forced organizations to build a set of stronger mitigation steps to protect critical assets and customer data. Organizational incident response strategies and resilience planning were targeted by legislators to be mandatorily improved. A significant upgrade of disaster recovery legislation was written, and the International Organization for Standardization (ISO) developed a DR standard (Herbane, 2010). The ISO lead the disaster recovery movement into a more mature state with roadmaps for organizations to gain improvements in their DR programs and provided the ability to certify to the standard. The 1993 Office of Management and

Budget (OMB) Circular A-130 sought to place attention to government records, specifically strategic planning, to ensure record preservation is conducted (OMB, 2000). Bartock, et al. (2016) noted the A-130 circular forced a redesign of organization's DR programs to leverage the use technology systems to preserve records in the event of a disaster. The circular highlighted that information technology is not the sole solution to the problem but one set of resources to meet the objective of recovery of critical records. An important aspect of the A-130 was that the circular specifically called for federal information systems administrators to be trained to manage the technology resumption effectively. Aligning with business continuity planning, the A-130 circular specifically pointed to risk assessment activities to understand the magnitude of the harm that would exist from the loss or modification of federal information. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is widely known as the privacy and technology regulation that applied to the healthcare industry. Cervone and Cervone (2016) claimed HIPAA's primary purpose was not technology security but more importantly designed to improve the resiliency of the data used for patients. The HIPAA Security Rule Standard 164.308(a)(7) Contingency Plan was specifically written for governing the use of the protected health information (PHI) and how the safeguards will keep the data safe by the recovery strategies (Cervone & Cervone, 2016; Rittinghouse & Ransome, 2011). The Gramm-Leach-Bliley Act (GLBA) of 1999 was similar to HIPAA in that the regulation intended to enhance the financial services sector by providing a clear framework for regulation that included disaster recovery components (Rittinghouse & Ransome, 2011). Executive management team members that are proven to have fallen

short of compliance may be subject up to a $250,000 fine and a prison term for each violation (Cervone & Cervone, 2016; Rittinghouse & Ransome, 2011). In 2002, the U.S. Congress set into law the Sarbanes-Oxley Act (SOX) of 2002 in response to a wave of high-profile reporting scandals (Cervone & Cervone, 2016; Elliot et al., 2010; Garner, Hutchison, & Conover, 2016). Although Sarbanes-Oxley does not specifically create controls for BCP or DR, Cervone and Cervone (2016) and Elliot, Swartz, and Herbane (2010) argued the requirements of the act invoke BCM concepts through a risk management requirement that applies to public organizations. Sections 302 and 404 of SOX require publicly traded companies to evaluate the effectiveness of the internal controls protecting financial data. The GLBA and HIPAA regulations are unique in the disaster recovery space due to the penalties that can be levied when an entity is found to be out of compliance. Iguer, Medromi, Sayouti, and Tallal (2016), Samanta and Dugal (2016), and Srinivasan (2016) claimed that providing disaster recovery controls is commonly used as audit control evidence to show compliance by the organization.

The President of the United States has implemented controls over the years through the issuing of presidential directives. In 2003, the Department of Homeland Security published the Presidential Policy Directive 7 (PPD-7) that reinforced the need for a risk assessment of critical infrastructure and key resources to terrorist attacks. The PPD-7 pointed to an important fact that it is not possible to protect all critical infrastructure but focusing on strategic improvements can lessen the impact of attacks that may occur (Department of Homeland Security, 2003). Niglia (2015) wrote that Section 7(d) of the directive is important in that it enhances protections that will assist in

the capability to ensure the orderly functioning of the delivery of private sectors essential services such as the energy sector, transportation sector, and nuclear sector. In 2011, the Department of Homeland Security published the Presidential Policy Directive 8 (PPD-8) that sought to strengthen the resilience of the United States via risk assessments focused on terrorism, cyber-attacks, pandemics, and natural disasters (U.S. Department of Homeland Security, 2011). The goal of the PPD-8 was to account for concrete, measurable, and prioritized objectives that could be used to mitigate risk. PPD-8 assigned responsibility to the assistant to the President for Homeland to periodically review the progress of the government's risk plan and to produce reporting metrics from meetings with federal, community-based, and private organizations. The presidential directives offer an advantage to disaster recovery teams in that the directives offer requirements and raise awareness of the need to focus on disaster recovery practices.

Some disaster recovery guidance has come from national emergency management agencies. Karter (2003) claimed that $12.4 billion in property damage was recorded in 2012 and the National Fire Protection Association (NFPA) develops publishes and disseminates standards to minimize the effects of fire and other risks. The National Fire Protection Association (NFPA) 1600 (2010) recommended improved practices for disaster management involving the fire code, life safety, and vehicle safety. The NFPA 1600 standard defined several elements for disaster recovery and emergency management that included emergency response, responsibilities, actions to take to save lives, and communication channels (Kellman, 2016; McLaughlin, 2005).

Disaster Recovery Standards, Certifications, and Guidelines

One of the major challenges of disaster recovery and the need for management involvement comes from the inability to recover all resources immediately following an interruption. During the interruption, every application must wait in a priority queue to be restored. The priority and procedures for determining how the organization will resume the technology systems are at the core of the DR management practice. The body of knowledge in information technology disaster recovery provided several models by which an organization can choose to build and manage the information technology disaster recovery program. The beginning of business continuance planning was a simple component of technology and financial standards and over time evolved into an important role for organizations to consider (Pasquini & Galie, 2013). Several models, guidance, and frameworks have been presented by researchers and standards bodies such as the International Organization of Standards.

The IT Governance Institute and ISACA collaborated to present the COBIT framework. The COBIT framework's main objective was to link business goals with IT goals. One major advantage of the COBIT in DR came from the guidance of top-level decision making within the organization as it pertained to disaster planning. The DSS04 objective of COBIT detailed the necessity to ensure continued services (Iqbal et al., 2016; Pasquini & Galie, 2013). Butler (1998) described a general, six-step disaster recovery model that has been widely adopted. Butler's plan started with demonstrating the business value of disaster recovery. Butler claimed the model's strength came when Management commitment is obtained, the current configuration is documented, DR

planners compose how the business uses the technology, the disaster recovery budget is funded, and the DR planners develop disaster recovery plans. Bishoff et al. (2015) described a model by Miram Kahn detailing a four-phase disaster response that can apply to any disaster. The Miram Kahn model included notification response, assessment of damages, rescue and recovery, and resumption of services. Gibb and Buchannan (2006) proposed a disaster recovery framework where the recovery process was compared to phases of a project. The Gibb and Buchannan framework provided inputs and outputs for nine project activities necessary to reach the organization's resilience goals. Neaga et al. (1997) presented a model where data categories were used to define the backup and recovery, application, database, infrastructure and system to assist in finding the critical systems needing to be recovered. Kadar (2015) provided a BCM risk index that allowed disaster planners to conduct metrics and status of the BCM program. Kadar's goal was to allow organizations to align the risk index to the culture or the organization. The Sendai Framework for Disaster Risk Reduction (SFDRR) addressed knowledge issues in the organization and highlighted the critical role of knowledge in disaster risk reduction (Weichselgartner & Pigeon, 2015). The SFDRR assisted in understanding disaster risk, strengthening governance to manage risk, investing in risk reduction, and enhancing preparedness for an effective response. The British standard BS25999 was published in 2006 and provided an agnostic approach that organizations could follow for their BCM planning (Herbane, 2010). The ISO 17799 is an international security standard that covers ten different sections. The ISO 17799 sections are defined as business continuity planning, system access control, system development and maintenance, physical and

environmental security, compliance, personnel security, security organization, computer and network management, asset classification and control, and security policy (Grigonis, 2002). The ISO 22301 outlined the requirements to implement a disaster recovery program. Al Hamed and Alenezi (2016) and Bajgoric (2014) noted the ISO 22301 was specifically written to be applicable to all industries and is the most influential standard in the disaster recovery literature. The Department of Homeland Security published the Ready.gov site to provide information to build an information technology disaster recovery plan for businesses to leverage. The National Disaster Recovery Framework (NDRF) provided an evolving framework for disaster planners to address disaster recovery (Chand & Loosemore, 2016; Smith, 2017). NIST Special Publications (SP) 800-34 series defined the contingency planning for information technology systems. Elliot et al. (2010) wrote that the 800-34 publication had a clear focus on technology and the planning methodology offered a similar approach to BCM planning. dPlan, an online disaster planning tool for civic institutions, was released by the National Center for Preservation Technology and Training (NCPTT) to allow for easy creation of a disaster plan (Yeh, McMullen, & Kane, 2010). The dPlan program collects data through a simplified questionnaire process to create a customized plan that can be maintained by an organization. Yeh, McMullen, and Kane (2010) argued that although the dPlan could develop a comprehensive plan, many found the plan lacked vital, necessary sections and was considered time-consuming.

Bartock, Cichonski, Souppaya, Smith, Witte, and Scarfone (2016) wrote that existing federal policies, standards, and guidelines exist for cyber event handling but

none focus on improving cybersecurity recovery capabilities. Bartock et al. (2016) claimed the fundamental information is not found in a single document but spread out in security, contingency, disaster recovery and BCP plans. Although there are many models, frameworks, and guidance, there is a gap when it comes to specifically preparing an disaster recovery program for computer crimes induced interruptions. The generalities of these models can assist an entity in preparing for a general response and recovery, but the models found in the literature do not provide clear guidance on additional steps that would address the emerging risk from computer crimes.

First Responders

A first responder is often associated with the personnel that is first to perform the medical response at the scene of trauma. Bobko and Kamin (2015) defined the first responder as fire, police, medical personnel, and in some cases civilians. Bobko and Kamin claimed that in most of the cases following a disaster the first responder is not a formally trained person. Bystanders are often thrust into situations where they can take actions to stabilize the situation until trained first responders can arrive. Similarly, organizational employees can often be pulled into disaster response without having any formal knowledge of how to successfully recover the business during the interruption. Butler (1998) wrote that once a disaster is experienced, the first responders must know their roles if the organization plans to maximize the success of the recovery. Bishoff (2015) and Lam (2002) claimed the organization should consider who is assigned to the response team as the members of the team should be able to perform when placed under a significant amount pressure from the disaster recovery. Rabjohn (2013) explained that

first responders could experience trauma through the exposure to a human suffering from the effects of the disaster. A law enforcement officer may work a murder one day, a fatal car accident the next day, and witness a human drowning the next. The psychological stress can compound according to Rabjohn (2013) and reduce the capacity of the response. After the incident has been experienced, the first responders initially gather and triage the casualties (Butler, 1998; Kamali, Bish, & Glick, 2017). The triage process will categorize the known casualties based on the severity. Kamali et al. (2017) and Tucker (2014) claimed the purpose of the first responders conducting the triage process is to use the available resources most efficiently.

There are several methods used by first responders when conducting the triage. The Simple Triage and Rapid Treatment Method (SMART), Homebush, Triage Sieve, Sacco Triage Method (STM) and CESIRA are the more popular found in the literature (Jain, Ragazzoni, Stryhn, Stratton, & Della Corte, 2015; Kamali et al., 2017; Lea & Tippett, 2017). The Committee for Tactical Emergency Casualty Care (C-TECC) took experience from military events learned from the battlefield and applied the knowledge to improving the civilian first responder activities. C-TECC is overseen by a broad range of leaders focused on high-threat medicine, fire, rescue, emergency medicine, emergency medical services, police, and the special military operations community. Pennardt et al. (2016) wrote that the TECC had become a professionalized, national, standard core of competencies that created a common language for incident response capabilities regardless of the situation. Pennardt et al. (2016) pointed out that despite major efforts by

government agencies, there are still no nationally agreed-upon standards for first responder certification or training.

Rodriguez (2016) wrote about the differences between an information technology disaster recovery incident responder versus the traditional medical responder. Rodriguez claimed the technology-focused first responders operate with ROI as the primary consideration and would assess and prioritize technology tasks based on the urgency or recovery time objectives. Rodriguez (2016) stated the triage process that is utilized by medical first responders is transferable to technology management. Technology first responders can take concepts from mature incident response models and use them when recovering technology systems. Ning, Wong, and Shi (2015) wrote that the technology incident response at the core is simply an approach for commanding, controlling, and coordinating the recovery team's effort. Rittinghouse and Ransome (2011) claimed the technology first responder must focus on the business effect of the disaster as opposed to a damage assessment.

Entities that do not focus on obtaining the correct talent for the initial response risk the responders failing to execute the plan as expected. Organizations looking to improve the quality of disaster response will place time and effort into choosing and training the people that will make up the first responders. By training responders and running testing scenarios, organizations can keep the knowledge necessary for disaster recovery fresh in the minds of those responsible for the task.

Disaster Planners

Alexander (2015) and Lam (2002) defined disaster planners' activities as a coordinated process of preparing to match urgent needs with available resources. The phases include research, documentation, dissemination, testing the plan, and revising. The disaster plan is a living document that is continually evolving to match the changing business procedures needed in the emergency response. Disaster planning involves a combination of plans and procedures, informed by planners, to be used by the incident responders. Alexander (2015) wrote that disaster planning must be realistic and pragmatic activity but also a collaborative process. There is no use in planning to use resources that would not likely be available during a disaster and planners should highlight where resources may be a problem in the recovery. The role of planners must consider the scarcity of resources during the recovery. To avoid an omission or major flaw in a disaster plan, disaster planners should have experience and training. Alexander (2015) and Smith (2017) wrote that the planning profession had been described as a vehicle to transfer knowledge, expand alternatives, generate social change, inform citizens, foster sustainable improvements, and identify vulnerabilities. Disaster planners are commonly employed by the organization to project manage the activity of disaster recovery. Stakeholders, a component of the planning team, are integral to disaster planning. Mojtahedi and Oo (2017) defined a stakeholder as the entity involved in decision-making and benefits from the resumption of the organization. The main goal of the stakeholder is to improve the performance of the disaster recovery project. Mojtahedi and Oo's (2017) research found where stakeholders exhibited legitimacy and urgency in the planning

process were where a reduced the effect of disasters was experienced. Alexander (2015) and Smith (2017) claimed that disaster planners should not be frightened of a black swan or unanticipated events because the black swan has been replaced by the red herring. Alexander claimed very little in the future that had not occurred in some form from the past. Disaster planners hold a significant role in the success of the resumption of the organization. Planning, testing, pre-coordination with the teams and education are all major components found in the literature. Organizations that can dedicate resources to proper planning improve the ability to resume from a technology disaster quickly.

Risk Assessment

Risk assessment is a large component of disaster recovery programs. Butler (1998) defined risk as the product of impact and probability. Al Hamed and Alenezi (2016) and Grigonis (2002) described a risk management plan as a systematic and analytical tool which establishes the likelihood and a known threat where harm would fall on the organization. To decrease risk to the organization, a disaster recovery management team should plan to minimize the effect of a disaster by understanding the specific exposures to their organization. Al Hamed and Alenezi (2016), Bishoff et al. (2015), and Neaga et al. (1997) pointed to the need to conduct a risk assessment before any disaster recovery solution could be constructed. The purpose of conducting the risk assessment activity was to quantify where potential problems the organization may be exposed. The risk assessment is an avenue for selecting the applicable mitigating controls. Lord (1981), Toigo (1989), and Tucker (2014) claimed risk assessment is a commonly misunderstood aspect of disaster recovery planning and poorly written or missing risk assessments will

lead to failure to recover. Grigonis (2002) described where a simple matrix of events could be used to document how resources can be affected by disaster events. Lord (1981) wrote the tough part of risk assessment is found in accepting that there is an unknown quantity, in the future, where an estimated loss must be made. The ability to recover all technology components of the organization during an interruption is extremely difficult and may be costly depending on the type of disaster. Neaga et al. (1997) wrote the risk assessment activity allows business processes to be evaluated for their negative impact on the organization when they are unavailable. A successful risk assessment should result in the required preventative measures, the type of recovery required, and acceptance of risks not being addressed.

There are multiple risk assessment frameworks leveraged by organizations across the globe. Yang et al. (2016) wrote that the NIST SP 800-30 Risk Management Guide for Information Technology Systems provided a common baseline for all levels of personnel and the 800-30 framework can be used to support the risk management process in disaster recovery. The CCTA Risk Analysis and Management Methodology (CRAMM) was developed by a British government organization to calculate risks from vulnerabilities and assets. Yang, Ku, and Liu (2016) claimed the CRAMM provided organizations with the ability to pick the risk appetite for important versus unimportant assets. The Information Security Risk Assessment Model and the InfoSec Assessment Methodology (IAM) are leveraged by multiple U.S. Federal agencies to assist federal managers to implement an enterprise information security risk assessment process. Clark, Dawkins, and Hale (2005) argued the InfoSec Assessment Methodology provides a means to gain

an understanding of critical systems but does not adequately draw relationships between the assets and the objectives of the assessment such as recovering from a disaster. The Vendor Risk Assessment and Threat Evaluation (V-RATE), Security Attribute Evaluation Method (SEAM), Risk Filtering, Ranking and Management Model (RFRM), Survivable Systems Analysis (SSA), Control Objectives for Information and related Technology (COBIT), and Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE) are all well known risk assessment frameworks that can be used to streamline and optimize the assessment of technology risks for organizations (Allen, & Sledge, 2002; Axelrod, 2016; Haimes, Kaplan, & Lambert, 2002; Snyder, 2014; Yang et al., 2016).

Organizations must understand how critical processes will be impacted by an interruption and which will need to be resumed first. Regardless of the risk model or framework that is used, any form of risk analysis done properly will establish likelihoods and threat to the organization. By building an understanding of the risks that can impact the organization, management teams can spend money and resources to mitigate the threats and document the recovery plans needed to resume the process.

Dangers of Disasters to Organizations

Organizations have multiple threat vectors that can affect standard operating procedures. Some threats have been a risk since the beginning of civilization while other threats have evolved. Lord (1981) recorded that it was estimated in 1985 that there would be $30 billion dollars of loss due to computer fraud. Liao, Balasinorwala, and Rao (2017) claimed that in 2017 the estimation of computer fraud reached $100 billion and is

estimated to be two trillion by the year 2019. To better understand the risks to an organization, planners must look at traditional threats and the emerging cybersecurity threats.

Traditional threats. Natural disasters negatively affect homes, businesses, infrastructure, and communications which ultimately affect people. Not all disasters are equal events, and not all people are affected in the same way. Flooding from thunderstorms, tornadoes, dam breaks, snow melts, or storm surges was the most common type of disaster to affect communities in the United States (Philips, 2015). Flooding brings damage to electronics, furniture, buildings, roads, and in some cases wastewater treatment needed for clean water. In the 1990s, flood damages to people and businesses in the United States neared $50 billion (Koenig, 2016). Storms as a natural hazard can vary in damage and impact. Hurricane Andrew in 1992 claimed 23 lives, cost the state of Florida and Louisiana over $26.5 billion, and displaced entire communities (Logan, Issar, & Xu, 2016; Philips, 2015). Texas, Kanas, and Oklahoma hold a high risk of tornados which can reach wind speeds of 200 miles per hour. Winds at this speed can level entire commercial buildings and residential homes. Research by Kantamaneni et al. (2015) revealed that tornado research in 2013 recorded 54 fatalities with damages of $3.6 billion. Lord (1981) and Wold (2002) alleged the fire had been the highest probability of being the disaster as compared with other general threats such as flooding or ice storms. In some cases, as in a 1997 North Dakota flood, fire is a result of an initial, separate disaster which will do more damage than the initial event (Kweit, & Kweit, 2004). Fallara (2003) noted the threat of fire is the primary reason organizations backup systems

to offsite locations. Earthquakes are determined by magnitude, motion, and duration. Depending on the earthquake and the construction standards of the buildings, considerable damage can be experienced. The Kobe Japan earthquake of 1995 was considered the costliest earthquake to have occurred with losses of a $132 billion. In 2010, a magnitude-seven earthquake was experienced in Haiti, which led to over 32,000 deaths (Miura, Midorikawa, & Matsuoka, 2016; Philips, 2015). The high death toll of the Haiti earthquake was linked to substandard building codes and may serve as a warning to disaster planners choosing data center locations for organizations. Modern technology and communications systems run on stable, waveform electricity. Blackouts, dropouts, brownouts, surges, and phase shifts can damage and create anomalies in technology infrastructure. Electrical anomaly problems and complete outages exist as a threat to organizations in the number of millions of dollars each year and thousands of hours of downtime (Grigonis, 2002). Organizations will deploy uninterrupted power supplies (UPS) and diesel generators to supply clean power to the data center in the event of anomalies or service interruptions and to mitigate the risk of electrical issues. Sizing of the UPS should be considered. Small office home office (SOHO) or mid-sized UPS may not handle the power needs of a larger organization when a complete power failure is experienced. The right choice of a UPS can prevent a disaster (Butler, 1998; Grigonis, 2002).

Hazardous materials are another threat that must be considered. Toxic spills, chemical explosions, train derailment, or debris from severe storms can become expensive problems for affected organizations. Philips (2015) wrote that 4.5 million

facilities in the United States work with some form of hazardous materials and could cause a disruption in a business process of production, use, transportation, or disposal. The United States has installed a *super fund* from the Comprehensive Environment Response, Compensation and Liability Act (CERCLA) from 1980 that was allocated to repair the damages from a hazardous materials disaster (Revesz & Stewart, 2016). Regulations from the state and federal level will need to be considered when dealing with a hazardous materials disaster. Disaster planners should consider what chemicals are in use in the organization and understand how they could create a disaster scenario.

Terrorism can be a difficult hazard due to the nature of the deliberate and unexpected attack on innocent people and organizations (Philips, 2015). Terrorism's goal is to cause physical and psychological harm to people, infrastructure, communities, and nations. Terrorism can be domestic or international and negatively affects governments, organizations, and individuals. Brooks (2011) wrote the terrorist attack on September 2001 that leveled World Trade Center buildings created a disaster that took the lives of many Americans and due to the destruction, ended the ability for some organizations to stay in business. Grigonis (2002) wrote about the actions of a nefarious individual or group could spell disaster for an organization. When an individual has internal access to the technology infrastructure with malicious intent, the organization could be disrupted by undetermined means. Hiatt (2000) and Lord (1981) wrote that people must be considered when listing hazards and studies have shown that the greatest risk involving computer-related disasters come from people. Patterson et al. (2002) claimed human

operators will always make errors, even when they have a clear understanding of what to do.

Natural and human-made disasters are a common and reoccurring threat to organizations. Although the threats are wide-ranging, organizations should be able to identify and craft controls that can mitigate the risks of these disasters. The body of knowledge on natural disasters is large, and the responses that were taken to recover the technology infrastructure is available. Organizational planners should look closely at what natural disasters the organization may be vulnerable to and apply the necessary mitigating controls to the disaster plan.

Current cyber-attack threats. Devastating losses can emerge from an interruption of technology infrastructure. Butler (1998) and Schultz and Shumway (2001) noted when an organization is conducting any aspect of business on the internet, risks are introduced that must be considered. In the 2015 state of cybercrime survey (PWC, 2015), 76% of the respondents claimed they were more concerned about cybercrimes than in previous years. Vaidya (2015) claimed that cyber-attacks not only cause billions of dollars in damage but have lasting psychological effects on the victims. Raiyn (2014) and Schultz and Shumway (2001) listed the common cybersecurity related threats as reconnaissance, access, reputation, harassment, denial of service, eavesdropping, extortion, pornography trafficking, subversion, and hoaxes. Rittinghouse and Ransome (2011) listed categories of internet fraud as financial, gaming, communications, utility, insurance, government, investment, business, and confidence. The 2016 ISACA State of Cybersecurity RSA conference survey revealed the threat from computer crimes, and

other information security breaches continue unchecked, and the financial impact of those losses increases every year (ISACA, 2016). According to the survey, 28% of the ISACA respondents reported a loss of intellectual property to cyber incidents at least quarterly, 25% indicated intentional damage to computer systems at least quarterly, 42% indicated they would be able to detect only simple cybersecurity issues, and 31% recorded cybercriminals had exploited their organization within the last year. While attacks have become more sophisticated and the motivations behind them seem to evolve each year. Barber (2001), Butler (1998), and Gagneja and Gagneja (2015) claimed the primary focus of company breaches led to financial gain, extortion, intellectual property theft, and disruption of service.

The emerging cyber threat continues to flourish because the computer crimes vector is cheaper, more convenient, and less risky than other vectors of attack (Jang-Jaccard, & Nepal, 2014). Stalans and Finn (2016) wrote that the Internet invites deviance and crime by providing a mechanism for alternative justifications and viewpoints into a form of cybercrime. The exponential growth of the business conducted on the internet and by the technology used in core business processes has led to significant growth in cybercrime. As of 2016, 96% of data breaches involved external actors with financial motivation (Verizon, 2017). The literature on cybersecurity attacks contains a significant number of high-profile events that were directed towards critical infrastructure, companies, government agencies and the public. Several of these events were first-time scenarios and pointed to the capability of future attacks. In 1988, Burleson was convicted of a third-degree felony in the United States' first computer virus trial. Burleson planted

malicious routines into data processing software being utilized in a securities and insurance firm (Marion, 1988). The malicious software destroyed data and erased volatile memory thirty days after Burleson was terminated from the organization. Burleson's attack caused an undisclosed amount of damages to his company in recovery and reputation. The 1999 Melissa virus, written by Smith, was designed to replicate exponentially by exploiting Microsoft Word and internal email systems (Ford, 1999; Simons, 1999). Melissa damages were estimated at $1.1 billion, and even though the virus did not have a malicious payload, it did cause a considerable denial of service to corporate email servers across the globe. The Code Red worm of 2001 infected over 350,000 computers in less than half a day by exploiting the Microsoft IIS service and damages to organizations were estimated at $2.6 billion (Vaidya, 2015). The Blaster worm and Slammer worm created havoc on the internet in 2003 causing a denial of service attacks and affecting Microsoft SQL Server (Moore, Paxson, Savage, Shannon, Staniford, & Weaver, 2003). The Stuxnet virus attack of 2010 physically destroyed over one thousand nuclear reactors in Tehran and significantly set back the Iranian atomic program (Singer, 2015; Steiner, 2014). Stuxnet was a multifaceted virus, and the complexity of this type of attack had not been seen before the release. Stuxnet attack had four never-before-seen, targeted, vulnerability exploits and used digital signatures that were stolen from legitimate organizations. Singer (2015) claimed the Stuxnet malware was the first specially designed cyber weapon designed by a government agency to do physical harm. In 2011, over 217,000 Citibank customer records were stolen by external hackers, resulting in a multi-million-dollar loss to the company (Aspan & Soh, 2011;

Vaidya, 2015). The Citibank attack consisted of hackers using keyloggers to gain user access to critical servers to defraud the company (Vaidya, 2015). In 2004, the Sasser computer worm infected global technology systems including Delta airlines which resulted in disabled technology systems for transatlantic flights and several hospitals were unable to operate until the technology could be repaired (Schultz, 2004; Steiner, 2014; Vaidya, 2015). The Estonia attacks of 2007, from a pro-Kremlin terrorist group, used ping floods and botnets to denial of service banks, newspapers, government systems, and communications for several days (Shackelford, 2009; Vaidya, 2015). Estonia was a disastrous attack in that it was the most technology-centric country in Europe where 90% of banking and government interfaces were delivered over the Internet. Shackelford (2009) pointed out that Estonia was built to operate how a future society would, and this is what made the attack more effective and was named the first information warfare event on society. The Sasser worm of 2004 spread using a buffer overflow in the local security authority of Windows 2000 and Windows XP operating systems. The Sasser worm damage attributed to organizational outages was estimated at over 550 million dollars (Schultz, 2004; Vaidya, 2015). Zimmerman and Restrepo (2009) reported the Sasser worm disrupted an oil and gas platform for several days before the systems could be restored and the platform usable. Bidgoli (2016), Solberg Søilen (2016), and Vaidya (2015) commented on the Sony PlayStation network being compromised in 2011 by cyber hackers that caused $2 billion dollars in damages and the data exfiltration of 77 million users credit card numbers. Sony experienced a 24-day outage as the

company incident response team, which did not have a contingency plan, restored systems and mitigated the vulnerabilities that allowed the breach (Solberg Søilen, 2016).

Cybersecurity experts believed that malware is the key weapon of the new cyber-criminal (Jang-Jaccard, & Nepal, 2014). Ransomware, a form of malware that encrypts data until a ransom is paid, is on the rise. A recently significant change to ransomware has seen the attack move away from single targets and targeting vulnerable organizations (Cabaj & Mazurczyk, 2016; Verizon, 2017). The largest ransomware payment to date, 1 million dollars, was recently paid by a web hosting firm after the technology department realized that the backup to the systems needing the restoration was also encrypted (Schwartz, 2017). Kharraz et al. (2015) claimed that cryptolocker ransomware has infected over 250,000 computers and disrupted several critical infrastructures in the last three years. Kharraz suggested that organizations need to invest in mitigating controls to counter the significant, growing risk of this type of attack. Cabaj and Mazurczyk (2016) argued that developers of the ransomware are constantly improving the attack and make any existing countermeasures ineffective. Cabaj and Mazurczyk claimed that organizations that can quickly find and block the communication between the infected machine and the command infrastructure of the attacker could prevent the encryption of the target. Lacking technical visibility poses a significant challenge for incident responders as they lack the tools or required response time to act. Organizations would need to provide monitoring technologies to the incident response team. The sharp rise of this risk has created a response by a few organizations. The nomoreransom.org coalition is comprised of 57 security vendors, law enforcement, and technology organizations to

assist victims in the recovery of the encrypted data without paying the ransom (Allman, 2016; Mansfield-Devine, 2016; Verizon, 2017). Many organizations will need to rely on disaster response and backup administrators to respond to a ransomware attack by restoring infected systems to a known good period before the attack initiated. In the case of the hosting entity, backup media needs to be protected and available to responders.

Phishing, coined on AOL in 1996, is a social engineering technique to acquire information such as credentials or financial information to mascaraed as the user. Alsharnouby, Alaca, and Chiasson (2015) claimed the assumption by the attacker is that they will be able to deceive users into believing the communication is legitimate. The 2017 Verizon breach report recorded over 2400 major incidents due to social engineering techniques with phishing being the entry point 90% of the time. Alsharnouby, Alaca, and Chiasson (2015) and Khonji, Iraqi, and Jones (2013) highlighted the weakness in humans being able to spot the attack allows the exploit to be difficult to mitigate and have led to many organizations being breached. Organizations may find that they have been compromised by external attackers acting as internal administrators via the stolen credentials. In a major attack against the security company RSA, phishing was successful in allowing attackers to compromise the organization and subsequently allowed the attackers to pivot to Lockheed Martin (Khonji, Iraqi, & Jones, 2013). Researchers point to the first line of defense in a phishing campaign is detection by the user (Khonji, Iraqi, & Jones, 2013; Verizon, 2017). There are multiple lines of defense against a phishing campaign that can be deployed (Alsharnouby et al., 2015; Khonji, Iraqi, & Jones, 2013; Verizon, 2017):

- Organizations can work to take down the shared host by the phisher.
- Users can be continually notified of various types of social engineering.
- Organizations can deploy toolbars to rewrite HTTP links eliminating the hidden destination that the user is being sent.
- Blacklists and whitelists are frequently used block communications to the Internet protocol of phishing webservers.
- DNS-based blacklists use the DNS specification to inform on malformed links that may be used by phishers.
- Programmatic toolbar helpers can detect phishing activity through data mining to alert users of the malicious intent of the link.

Education and awareness may not be enough to protect an organization from a phishing attack. Disaster recovery responders should understand if the cause of the service interruption is due to compromised credentials from a phishing campaign. If the attacker's intention is a disruption of the business, disaster responders may see services that have been restored will be taken back offline. Complete eradication of the intruder's stolen credentials will need to be conducted before the organization can be resumed.

Barber (2001) called the Denial of Service (DoS) attack one of the most infamous attacks conducted by hackers to cause harm and had increased in size and complexity over the last ten years. Long and Thomas (2001), Moore, Shannon, Brown, Voelker, and Savage (2006), and Schuba et al. (1997) claimed a DoS attack leverages a weakness in the TCP/IP protocol and cannot be corrected without significant changes to the standards of the protocol. A DoS is initiated by an attacker by sending too many connection

requests to the victim that causes the victim to allocate all available resources and denying legitimate connections (Raiyn, 2014). DoS can be a significant nuisance to an organization that is conducting business over the internet; unable to process legitimate requests the organization will appear offline. Research by PWC (2015) indicated the DoS has become increasingly damaging and is one of the most frequent types of attacks. Schuba et al. (1997) claimed that organizations could defend against the DoS attack by allocating more resources, reducing timeouts, modifying routers to block flooding SYN packets, utilizing the firewall as a relay, and sending reset packets. The drawbacks to the defenses are cost, stability, delays in communication, and continual monitoring by the incident responders (Schuba et al., 1997). In 2015, a DoS attack affected the Microsoft Xbox Live service for a week causing substantial connections problems for their gaming customers. November 2016 a large distributed denial of service impacted half of the internet as attackers targeted the Dyn domain name service company serving many of the world's largest organizations. In September of 2016, Krebs on Security was hit with a DDoS that was 20 times larger than any DoS that had been previously recorded on the internet and is thought to have been in retaliation to an article being published by the researcher (Shuler & Smith, 2017). The Verizon 2017 breach report noted the finance, retail, and technology sectors experienced more than one million DoS during 2016 (Verizon, 2017). Verizon Research has shown that incidents involving a web application are caused by 80% denial of service, 20% malware and the remaining percentages are due to stolen credentials. The Internet of Things (IoT) has become a risk point for denial of service attacks. With more of the consumer electronics being manufactured having the

ability to connect to the internet, the more hackers are finding ways to leverage the devices maliciously. Organizations must understand what their capabilities are to mitigating DoS attacks and how the incident response team will react to mitigate the attack. Making the monitoring of the network data available, response planning to firewall rulesets changes, and contact numbers at the telecom provider can greatly assist the disaster responder in mitigating the attacks.

A web service is commonly described as an application or service that is made available from an organization's exposed internet server. Research on web services attacks indicated hacking against web services are on the rise (Raiyn, 2014; Razzaq et al., 2014; Salini & Shenbagam, 2015). Razzaq et al. (2014) wrote that web services have greatly improved the profitability of organizations and at the same time increased the risk to cyber-attacks. A web application attack is an incident where the internet exposed application was the vector of the attack. The attack includes code-level vulnerabilities, data exfiltration and the circumvention of authentication schemes (Verizon, 2017). Gupta and Gupta's (2017) research revealed 55% of the banking industry's web services are always considered vulnerable and 21% frequently vulnerable to attack. Salini and Shenbagam (2015) claimed web application security is the primary concern for e-business and their research indicated 75% of hacking is being deployed at the application layer. A 2013 survey by WhiteHat Security claimed the Cross-Site Scripting (XSS) vulnerability is the top weakness among web applications, has the capability to DoS, and contributes to a significant data leakage problem. Martin and Lam (2008) described XSS as a JavaScript code injection attack that allows for a malicious script to be run in the

victim's browser to gain access to sensitive resources on the backend server. Wang and Zhang (2016) described the 2013 Yahoo attack where accounts of Yahoo's users were exploited by an XSS vulnerability causing a massive malware and spam campaign. Cao, Yegneswaran, Possas, and Chen (2012) and Gupta and Gupta (2017) described how XSS vulnerabilities produced the Boonana, SpaceFlash, Renren, Samy, and Yamanner worms that created damage to millions of users and workstations. Gupta and Gupta (2017) suggested that organizations should consider XSS attacks to be a serious threat and deploy mitigating controls to safeguard data and systems. A SQL injection attack (SQLIA) is a web service attack technique that can damage and exfiltrate sensitive data from databases. Pearson and Bethel (2016) argued the SQLIA lead the threat to web services instead of XSS. Sharma and Jain (2014) and Pearson and Bethel (2016) described the SQL-structured query language as the means for web applications to interact with a database. When applications are not properly hardened in the coding, the very popular SQL-injection attack can change the intended logic of the application to a malicious logic that returns data that was not authorized to the attacker (Sharma & Jain, 2014). The malicious input from the injection causes the interpreter to execute involuntary commands to the database without proper authorization. Finding the design loophole allows the attacker unlimited access to the database. The literature on SQL injection describes multiple attack types including orderwise injection, blind, double-blind, database fingerprinting, authentication bypass and remote commands against the database. Regardless of the attack leveraged, SQLIA can exfiltrate data, plant malware, and drop database tables resulting in a complete loss of data. Incident response teams

should understand the ramifications of SQLIA on the organization's web services and what would be needed to recover from modified or deleted data from the database.

Cyber-attacks are becoming more destructive and are a threat that can strike any private or public organization (Solberg & Søilen, 2016). Cyber-attacks can be initiated by foreign entities, government intelligence apparatus, universities, organized crime, or competitors. The PWC (2015) study showed that 75% of cyber-attacks would spread from the first victim organization to the second victim organization within one day and 40% of those attacks will hit the next organization in less than an hour. A study by the Ponemon Institute found that 70% of the entities responsible for critical U.S. infrastructure had experienced at least one annual technology interruption from a cyber-attack (Mansfield-Devine, 2014). The Ponemon study also documented only one in six respondents claiming their technology security program as mature and capable of responding to a cyber-attack. Malicious hacking is a risk to any organization with systems connected to the internet. Stalans and Finn (2016) claimed the accessibility and availability of the Internet in supporting societal institutions cultivates cybercrime as there is no centralized government body to establish rules or enforce criminal laws in specific countries. Solberg Søilen (2016) compared the cyber army of the twenty-first century as what the military air force was a few decades ago. Militaries all over the globe are fortifying cyber-attack personnel and cyber-warfare toolset after witnessing the US Stuxnet attack on Iran’s nuclear program. Iran responded by cyber-attacking Aramco that resulted in eight days of service interruption on critical systems (Bronk & Tikk-Ringas, 2013; Lewis, 2013; Solberg Søilen 2016). Raiyn (2014) claimed traditional cyber-attack

detection has limitations in that it can only detect known attacks. Forums and chat rooms on the Internet allow for trustworthy underground markets for the sale of drugs, prostitution, sensitive data, and terrorism (Stalans & Finn, 2016). One common mitigating control to hacking comes from an internal white hat hacker. The white hat hacker is slang for an ethical computer hacker who specializes in testing and methodologies to protect an organization from external hackers. The white hat tests the technology infrastructure with the same techniques as a malicious hacker and may offer organizations a better understanding of how they may be vulnerable to attack. The increase in cyber-attacks should cause executive management to seek to understand how the organization can protect itself from this type of specific risk. A strong security program will reduce risk but cannot eliminate it. A mature organization should prepare disaster recovery plans for resuming from a cyber-attack risk that applies to their Internet offering.

Common Information Security Frameworks

There are many information security frameworks available in the information security literature for an organization to align, and no single framework would be applicable for all organizations. Implementing a security program by leveraging a framework means the entity will have defined principles, policies, means, and methods. Yang et al. (2016) claimed the security requirements of an organization's framework could serve useful for building a program and as simple as a checklist activity for compliance. The common components of the security frameworks found in the literature consist of planning, implementation, and verification (Mihut, 2014). Planning

components included management processes, risk management, and security design. Implementation components included implementing security metrics, security toolsets, defensive technology, monitoring, and training. Verification components included monitoring, audits, testing, and evaluations.

Yang et al. (2016) claimed the use of ISO 27001/27002 is considered the most prevalent practice in the domain of information security management. Cefaratti, Hui, and Wallace (2011) described the ISO 27000 as a framework designed to address the essential controls needed to safeguard an entities technology asset. Gillies (2011) claimed previous studies indicated the ISO 27000 framework had seen a slower adoption than previous ISO frameworks such as the 9001 series. An ISO 27002 based survey by Cefaratti et al. sought to measure the effectiveness of IT-related investments in best practices and found that the respondents considered the effectiveness of the controls and the investments by the organizations to be linked to positive results found by external auditors. Research by Gillies (2011) revealed that 50% of the organizations holding an ISO 27000 certification were from 50 or less employee, SME types of organization. Gillies highlighted that 80% of the respondents indicated the 27000 certifications were obtained for a competitive advantage in marketing the organization and not for improving the security program. Gillies argued the adoption problem of the ISO 27000 framework come from complexity and the $22,000 certification price for smaller organizations without a large technology audit budget.

The NIST SP 800-184 Cybersecurity Event Recovery Framework (CSF) provides a high-level framework for organizations to improve their posture by following a five-

phase approach. Souppaya, Feldman, and Witte (2017) described the 800-14 as a framework that is suited for improving policies and plans for recovering from evolved threats. Shackelford, Proia, Martell, and Craig (2015) claimed the NIST framework had the potential to improve international corporations that favor a voluntary approach to cybersecurity. Souppaya et al. (2017) claimed the planning components of the 800-184 enables the organization to improve the risk scenarios activities by reviewing recent cyber events to assist in the development or recovery playbooks. The 800-14 could identify gaps to be addressed before the disaster is experienced. NIST released the SP 800-184 as a guide for cybersecurity event recovery and defines five functions of identification, protection, detection, response, and recovery (Lindström et al., 2010; Souppaya et al., 2017). Metrics generation is encouraged in this framework, and the metrics are used to improve the quality of the response actions.

NIST SP 800-53 was defined as the framework for the Security and Privacy Controls for Federal Information Systems and Organizations (Montesino & Fenz, 2011). Cardenas et al. (2009) noted the 800-53 framework consists of over 180 controls that are not enforceable on federal systems but were designed to provide guidance. Ericsson (2007) claimed the 800-53 was designed to influence a wider audience than just federal systems and the largest challenge for organizations is to select the appropriate security controls from a framework. Montesino and Fenz's (2011) research found an advantage in leveraging the 800-53 framework for other organizations in that 30% of the controls could be automated by software solutions. The 800-53 framework provided a set of

baselines that would allow an organization to find a section of countermeasures needed for that vertical.

Yang et al. (2016) claimed the NIST 800-26 Security Self-Assessment Guide for Information Technology Systems, established the foundation for standardization on several levels of security status. Organizations choosing to align with the 800-26 can leverage the framework to determine whether a described five levels are adequately implemented by the security program. Johansson and Johnson (2005) asserted the 800-26 framework provided an extensive questionnaire that should be used to test security controls against a classified or unclassified system.

CIS 20 Critical Controls, sometimes referred to as the Consensus Audit Guidelines (CAG), is a framework of 20 prioritized actions to defend an organization from known cyber-attacks (CIS, 2017; Montesino & Fenz, 2011). Lewis (2013) claimed the NSA originally defined the initial list of controls from the active compromises they were involved in remediating. Lewis pointed that the NIST frameworks are several thousand pages which can create implementation barriers, but the CAG correlated the most commonly used attacks along with defensive measures.

The Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE) is a methodology developed by the Carnegie Mellon University to streamline the process of assessing information security risks and the development of a security strategy. Yang et l. (2016) claimed the OCTAVE offered an alternative approach specifically designed to assess technology assets and the resiliency of the applied controls. Johansson and Johnson (2005) described the advantages of the OCTAVE come from the business unit

and technology staff working together to address the security needs of the organization. The team drew on the collected knowledge to define the current state, major risks, and a clear security strategy.

Iqbal et al. (2016), Lainhart (2000), and Yang et al. (2016) wrote that the Control Objectives for Information and Related Technologies (COBIT) could be deployed as a supporting toolset to bridge the gap between information technology and top-level decision making about business continuance planning. Von Solms (2005) evaluated the COBIT framework against the ISO 17799 for security governance. Von Solms summarized the COBIT was lacking in the detailed installation of controls and was designed to guide a framework to be integrated into a wider IT governance program. Lainhart (2000) claimed the main objective of COBIT was the creation of superior policies and technical controls that would eventually lead to endorsement by auditors. Ridley, Young, and Carroll (2004) wrote the highest concentration of COBIT adoptions are found in the United States. The adoption base is understandable as the COBIT framework was developed in the U.S. and aligned easily with IT governance drivers found in industries such as the financial sector.

Information Security Forum (ISF) includes a standard of practices in five sections. The ISF is broken out into 30 areas and 135 sections and offers advantages when measuring the information security program in an organization (Da Veiga & Eloff, 2010); Kruger & Kearney, 2006). Da Veiga and Eloff (2010) claimed the ISF should guide improve the security culture that provides an improved security behavior from employees.

Information Technology Infrastructure Library (ITIL) is a framework designed to address IT service management and provide management guidelines for incident response, capacity management, problem management, and others. Kanapathy and Khan (2012) described the ITIL framework as a set of best practices that can increase IT service management and enable IT departments to demonstrate strong systematic execution of processes. Sharifi, Ayat, Rahman, and Sahibudin (2008) claimed the ITIL is the most widely used, general IT framework in the world. Sharifi et al. (2008) claimed organizations that have failed at implementing the ITIL framework were lacking in management commitment, creating complicated processes, missing process owners, and having a project team that was too ambitious. Kanapathy and Khan (2012) argued the ITIL framework does not recommend a standard for the implementation of the controls and their research found larger IT teams with established programs were more likely to be familiar with ITIL.

The National Security Administration's InfoSec Assessment Methodology (IAM) (Cross, 2003; Yang et al., 2016) proposed by the National Security Agency provides an analytical framework for information security. The InfoSec Assessment addresses three tiers of quality and 18 distinct areas by which the program would be managed. NSA (2002) noted the framework sought to improve vulnerability assessments and provide quality guidelines to security programs. Cross (2000) claimed the strengths of the IAM comes from the documentation, focus on awareness training, and standard operating procedures found in the framework.

The Survivable Systems Analysis (SSA) method was developed by the SEI CERT® Coordination Center. Yang et al. (2016) wrote the SSA is a process that provides an advantage in the assessment of the survivability properties of a technology system. The analysis is carried out at a high level and proceeds through a set of joint working sessions to compile findings and recommendations for upper management decision-making.

The frameworks summarized in this section, along with the many supplemental frameworks that can be found in the information security body of knowledge provided many options for organizations to create a security program, measure the program for maturity, achieve governance, provide awareness, and reduce risk to the organization from technology risks. An organization should carefully choose which framework will best fit the professional vertical and current state of the information security program. Failure to properly align the framework with the organization may result in significant vulnerabilities, a false sense of security, or a program operating in a lesser state than optimal. Organizations with less than optimal security posture and exposing vulnerabilities in the technology infrastructure increases the risk of a computer crimes service interruption.

Current Research in Information Technology Disaster Recovery

Innovative technologies have been studied to improve preparedness for disaster recovery planners, incident responders, and executive management. In the past, information technology disaster recovery planners needed only to focus on keeping the mainframe operating during a natural disaster, and ensure there was a good working set

of backups. Alexander (2015) wrote that disaster planning must now evolve to face the challenges of the technology age and understand the immediacy means of communications available. Alexander stated another challenge is to ensure that the increasing dependency on technology for the recovery of the organization does not create a vulnerability in its right. Ee (2014) wrote that new technology threats are making organizations more aware of the need for continuance planning but many organizations do not reach a state of business resilience. To approach business continuity management traditionally may not be enough to reduce modern risk scenarios such as computer crimes. Bajgoric (2014) claimed the traditional approach focuses the organization to think in limited aspects and leaving out different threat dimensions. Organizations failing to reach a mature BCP will focus on past incidents, incomplete knowledge, perform weak business impact analysis, and follow only portions of a framework. Ee (2014) wrote that inadequacies in BCP could be solved through a standard approach and a commitment to a BCM discipline by upper management. Al Hamed and Alenezi (2016) wrote about the importance of a strong connection between information security and disaster recovery. Al Hamed and Alenezi claimed not all information security controls are part of disaster recovery and not all DR measures are found in information security frameworks. Where information security is primarily a preventative measure, disaster recovery is more aligned to be preventative, repressive and corrective.

New cloud alternatives. Cloud computing has recently transformed the thinking of backing up data in disaster recovery (Bisshoff et al., 2015). Alhazmi and Malaiya (2013) claimed cloud technologies had provided an affordable alternative to disaster

recovery plans for small and medium-sized organizations with no significant addition to office or facilities cost. Razvi Doomun (2008) believed that cloud providers that offered strong disaster recovery and security options could gain an organization a competitive advantage. The advantages of cloud solutions come from the removal of many local infrastructure dependencies. When the technology infrastructure is delivered from a cloud computing provider, many traditional tasks such as backup and maintenance are transferred to the solutions provider. Chang (2015) highlighted the need for contingency planning in the cloud because of the need for a clear understanding of data management. Outsourcing to a public or private cloud can move data off the local premises for cost savings, but the risk of data loss has just shifted to the service provider. Chang argues the risk of data loss applies regardless of whether the data is stored in the cloud or on premises. Alhazmi and Malaiya (2013) pointed to a limitation of cloud disaster recovery comes from the cloud provider serving as the DR component for many organizations and the provider may become overwhelmed if it experiences a high demand from several customers at once. Cloud-based disaster recovery may provide some advantages in cost, but the redundancy of the data must be considered. Alhazmi and Malaiya wrote that cloud services have a limited history to review and it is not clear how cloud providers will respond to a serious disaster or a cybersecurity attack.

Disaster recovery communications. Improvements in ICT have allowed organizations to improve the facilitation of the recovery during crisis response. Matar et al. (2016) claimed the progress and fast rise of social media platforms for communication had found application in disaster recovery incident management. Bortree and Seltzer

(2009) research indicated that social media provided a positive means for two-way communication between its users and entities to deliver vital information. Social media features, in the disaster recovery context, provides the users, responders, and disaster team management the ability to leverage native, mobile applications for a communication channel. Matar et al. pointed to the success of communication via social media during Virginia Tech shooting in 2007 in providing vital details to first responders and other students. Research by Quang Tran, Kien, Borcea, and Yamada (2014) found an advantage in connecting disaster responder mobile devices to surviving wireless access points for a multi-hop wireless access network that effectively mitigated losses by allowing connectivity to communications systems. Providing Internet connectivity to the large disaster area can improve the emergency response by allowing video conferencing, instant messaging, access to disaster plans in a cloud provider, and electronic mail with disaster recovery coordination teams. Research by Suaybaguio (2016) found that Short Message Service (SMS) was perceived as an optimal communication channel during a disaster for the timely dissemination of information from disaster managers. SMS messages do not require the mobile device to be activated for the user, and the messages are transmitted with the same cell tower technology as voice calling. SMA can also be sent from a computer to an ordinary mobile device using software automation and scripting.

The ability to have users continue to operate during the loss of a facility or campus can be advantageous for most entities. The September 11, 2001, terrorist attacks forced organizations to rethink how employees could operate remotely during a disaster

(Grigonis, 2002). Gartner used the phrase *workforce resilience* to describe the need for employees to have remote access to commodity Internet using the power of mobile devices and virtual private networking. Organizations that are location-specific have a greater risk of being disabled. Grigonis (2002) claimed enterprises that have engineered the ability for employees to work remotely are positioned to respond quickly in the event of a disaster. Mobile work schemes offer the organization to put employees back to work quickly. Lam (2002) wrote that traditional organizations would temporarily shore up people resources with contract staff, call-out arrangements, rental offices, manual procedures, and service forwarding agreements. Virtual Private Networking (VPN) technologies can place employees anywhere and still protect the confidentiality, availability, and integrity of the network transmission (Grigonis, 2002). One minimizing the impact of a disaster is distributed computing, including end-user computing. Greene (2006); Sprague (2015) wrote that although VPN technologies are not the only mechanism for flexibility, VPN technology allows for organizations to accommodate many displaced employees with minimal effort. Heng, Hooi, Liang, Othma, and San's (2012) research found a strong agreement in the VPN technology as a solution for reacting to unseen events and still providing an adequate platform for normal business operations. Organizations that use a VPN solution that can place the user base anywhere that has Internet capability has an advantage when a disaster affects a location.

Need for technology integration. The review of the cybersecurity frameworks and the disaster recovery frameworks highlighted commonalities but also revealed gaps in the disaster recovery incident response to computer crimes. Johansson and Johnson (2005),

Lindström et al. (2010), and Souppaya et al. (2017) wrote that although multiple frameworks had components for disaster recovery, there was a gap in focusing on recovery for cybersecurity. Figure 4 was created to describe a potential improvement to the disaster recovery response process.

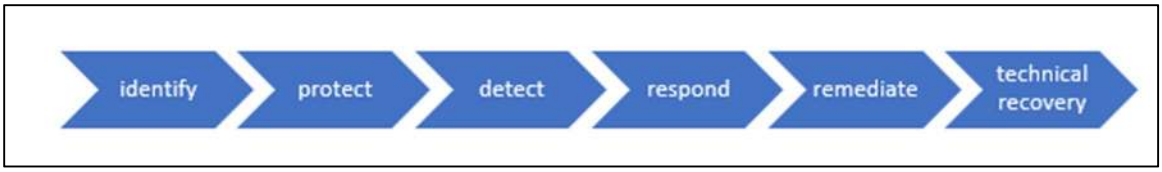

Figure 4. The improved disaster recovery response workflow.

Johansson and Johnson (2005) research compared multiple security frameworks and found that while certain frameworks were strong in planning, others were strong in controlling, and others were strong in governance. Johansson and Johnson claimed that that depending on the framework chosen, organizations will receive different levels of information security controls and recovery. Bartock et al. (2016) wrote it is important to understand that a cybersecurity incident response plan should be developed as part of a larger contingency plan. Gupta, Chaturvedi, and Mehta's (2011) research found that organizations should be better prepared to handle cyber-attacks if the security program is part of an overall, mature information technology program. A strategic focus on risk management strategies should help the organization to reduce the effect of materialized risk. Lindström et al. (2010) claimed one of the more important issues in disaster recovery comes from IT and cybersecurity planning. Top managers may not have the proper understanding of information security which can lead to decisions that do not improve the organization responds to a computers crimes type of interruption. The BCP

should include other procedures for reducing a service interruption risk to business functions. Iqbal et al. (2016) wrote there is a benefit to organizations that can manage and monitor its information technology program by better benchmarking to improve the service availability. Cardenas et al. (2009) argued that the current tools of information security not provide a sufficient defense in depth system to protect specific organizations such as those with control systems (SCADA). Lindström et al. (2010) wrote that information security management standards focus on mature processes and not the content of what they are securing. The ISO, GASPP, and SSE-CMM are popular in use and practitioners face a limitation in focus on ensuring processes exist while being less focused on how the processes accomplish improving the security stance of the organization. Barber (2001) noted the ISO 17799-1 is being explored by companies to provide a framework to manage cyber risk and judge the security controls in place. Integrating information security responders with disaster recovery first responders should have advantages. Loui and Finn (2016) claimed cross-training system administrators and first responders is essential to be sure the correct coverage will be available when disaster strikes. Organizations that can find opportunities to integrate the cybersecurity incident responders, Security Operation Center (SOC) monitoring, disaster recovery planners, and disaster recovery first responders should experience improved recovery over organizations that do not integrate.

Summary and Conclusions

The literature review included the concepts of emergency management, crisis communications, types of disaster recovery, laws affecting disaster recovery, disaster

risks to organizations, disaster recovery frameworks, and information security frameworks. Disaster recovery efforts have evolved from simple people management and planning for the effects of natural disasters to adhering to federal regulations and managing the risks of technology interruptions such as computer crimes. A common theme found in the disaster recovery body of knowledge was that there are risk factors that planners and first responders must prepare for to expect an optimal recovery. Those risk areas were natural, human-made accidents, terrorism, and technology. The more detailed information technology disaster recovery literature detailed the influence of computer crimes and the need to account for the risks. Although there were many strategies discussed for managing disaster recovery efforts, there were only a few sources that presented strategies to combat computer crimes interruptions. Bird (2015), Brown, (2016), Dines, (2012), Ferdinand (2015), Ignatius (2015), Marinescu (2015), and McCreight and Leece (2016) provided studies that assisted in the analyzing the gap. This research reinforced the necessity to understand the emerging threats that computer crimes have on organizations and the need for disaster recovery programs. Chapter 3 includes the research methodology to investigate how information technology disaster recovery can be modified to better respond to emerging threats.

Chapter 3: Research Method

The purpose of this qualitative study was to understand how information technology disaster recovery controls and processes can be modified to improve response to a computer crime caused business interruption. The problem statement highlighted in Chapter 1 was the lack of knowledge organizations have to recover from some computer crimes interruptions given the maturity level of existing disaster recovery programs. Guidry et al. (2015) and Ferdinand (2015) discussed the lack of a set of control procedures to allow understanding of how business management can bolster disaster recovery programs to account for this type of interruption. The literature reflected the importance of planning for disasters and incident responders understanding the significant disaster risks to the organization. I did not find where there was a comprehensive framework developed to collaborate information technology disaster recovery and cyber security controls to combat this disaster risk. In this study, I focused on how organizations can better plan and build procedures to improve the recovery of an organization from a computer crimes disaster. This chapter includes a review of the research design, the role of the researcher, selection of the participants, use of the instrument, explanation of data collection, analysis of the data, challenges of the method, and any threats to the validity of the findings.

Research Design and Rationale

I sought to understand what factors significantly affected the ability of technology responders in responding to computer crimes caused disasters. Cybersecurity experts, disaster recovery researchers, and incident responders represent a participant pool that

holds an understanding of the current events affecting disaster recovery. An expert participant pool may create new knowledge to improve the process of responding to computer security interruptions. A qualitative research inquiry has exploratory and theory building attributes. Many of the qualitative paradigms could be used to generate a better understanding of how disaster recovery responders and planners should respond to a computer crime interruption. The rationale for this study is provided based on a review of the qualitative research methods that may apply to answer the stated research question.

Choosing a phenomenological research study could provide generalizations about how disaster planners, disaster responders, and cybersecurity experts view the specific interruption caused by cyber attackers. The generalizations would provide the viewpoints and the shared experience of the targeted groups (Babbie, 2007) but the generalizations would not develop the cause and effect relation, nor the theory building needed to improve the process. A case study method would include how and why the service interruption happened, in a small sample size of one to three organizations, which had experienced a computer crime caused disaster (Yin, 2011). A disaster case study would involve extensive interviewing and observation of a disaster recovery team that had recovered from a computer crimes disaster. Organizations may be reluctant to approve to conduct a study when the team had failed to recover from the incident properly. The case study would allow for real-life situations to provide in-depth data collection. A researcher would be limited in that the qualitative data gathering would focus on the specific cases selected (Yin, 2011) and any conclusions may not apply to all disaster recovery programs. A narrative research inquiry would seek to understand the motivation and

experiences of disaster recovery planners and incident responders as they are recovering the organization from a technology-caused disaster. The narrative design would provide an understanding of factors that allow for successful incidence response, but narrative methods are usually limited to a few individuals and would not suffice for broad theory generation (Maxwell, 2005). Ethnographic research would focus on cultural groups (Babbie, 2007), which would limit the type of disaster responders and planners used in this study. The technology field of disaster recovery consists of multicultural workers (Niederman, 2004) and would severely limit the understanding that could be gained by narrowing to a single cultural group. The desire to have multiple perspectives, expert experience, and ability to conduct theory building aligns with the use of the Delphi design.

A Delphi design was selected over other qualitative approaches because of the accuracy of forecasting (Linstone & Turoff, 1975) and goal of the study was prediction and theory building. Skulmoski et al. (2007) argued that the design can be used when there is an incomplete understanding of a problem and should be used to explore what does not exist. The Delphi design allows for the identification of controls or alternative frameworks (Okoli & Pawlowski, 2004) that may be used to improve the process by analyzing feedback from experts in the field of disaster recovery. The Delphi design is based on a formal process for collecting and disseminating expert knowledge through a series of qualitative questions with controlled moderation (Linstone & Turoff, 1975). The Delphi design is a useful form of communications and anonymous consensus building to facilitate group judgment. The findings from the Delphi data collection activity were

triangulated from the responses of the participants and research conducted during the literature review (Linstone & Turoff, 1975; Okoli & Pawlowski, 2004; Skulmoski et al., 2007*)*. The study was exploratory because of the small number of studies on the topic of computer crimes as they affect information technology disaster recovery. The use of the Delphi design in this study was to create new strategies for responding to computer crimes caused service interruptions. The Delphi technique provides quantitative data to quantify the participant's responses and potential for consensus (Linstone & Turoff, 1975; Okoli & Pawlowski, 2004).

Role of the Researcher

As the researcher, I held multiple roles during this study. I assembled the panel of experts with the experience in disaster recovery, incident response, and cybersecurity. I designed the questionnaire with questions relevant to the study of disaster recovery and grounded in the literature review from Chapter 2. The questions were designed to be qualitative, and I administered each of the three rounds of surveys and analyzed the responses. Based on the responses, the next survey allowed for the participants to revise their original responses and answer other questions based on the previous group feedback (Okoli & Pawlowski, 2004). I reiterated this process until the participants reached a consensus in providing themes or disparities. When disparities were recorded from the collected judgments, interviews were conducted with the participant to gain an understanding of the deviation from consensus. In the case of nonresponses during any the three rounds of the Delphi, I communicated to the panelist to obtain assurances of

participation and move the process along. When participants dropped out, I filtered the data from the collected responses.

To mitigate any research bias, I can disclose that I am neither affiliated with nor employed by any of the participants. The panel was recruited by a snowball sampling of suggestions from experts I consulted with about this research. While I may be known to some of the experts, there was no employment relationship with any of the participants.

Methodology

The Delphi design was developed by the Rand Corporation in the 1950s and was intended to be a technique for the collation of judgments on a specific subject (Skulmoski et al., 2007). Linstone and Turoff (1975) and Skulmoski et al. (2007) claimed the Delphi design is typically executed through a set of designed, sequential surveys mixed with the summarized feedback of earlier responses. Donohoe and Needham (2009) wrote the Delphi design is best used when complexity and uncertainty are present, and there is imperfect knowledge. The Delphi design is primarily used in cases where judgmental information is valuable, and the procedure uses a series of questionnaires interspersed with controlled opinion feedback (Okoli & Pawlowski, 2004). Okoli and Pawlowski (2004) claimed researchers could apply the Delphi design to situations as a tool for expert problem solving and long-range forecasting. The design does not require the expert panelists to be in any single location making it a viable option to be conducted by electronic means such as the Internet. Internet communications is an advantage in that participants can be from geographically disperse areas and still collaborate simultaneously (Skulmoski et al., 2007). Linstone and Turoff claimed three rounds are

sufficient to attain consensus in the expert responses. Skulmoski et al. and Okoli and Pawlowski wrote that additional rounds beyond three offer only small changes to the analysis and becomes repetitious to the panelists. Fowles (1978), Linstone and Turoff (1975), and Skulmoski et al. described the following steps for the Delphi design:

- The researcher will design a team to undertake and monitor a Delphi on a given research subject.
- The researcher selects panelists to participate in the exercise. Panelists are chosen by the expertise in the area to be researched.
- The researcher develops the first round of questions to begin the study.
- The questionnaire is tested for ambiguities, vagueness, and appropriateness.
- The researcher submits the first questionnaire to the panelists, over a predefined communications method, to collect the qualitative data.
- The researcher collects the data from all panelists and analyzes the first-round of responses.
- Preparation is made for the second-round questionnaires based on the answers from the previous round. Feedback is provided in the previous rounds to allow the experts to provide clarity if they deemed necessary.
- The researcher submits the next round of questionnaires to the panelists for data collection.
- Analysis of the responses and developed questions based on the data is reiterated as long as it is necessary to achieve consensus in the results. During each round,

the experts are provided feedback on their responses to ensure the researcher has fully understood the answers that were submitted. This includes arguments.

- A report by the researcher or team is generated to present the conclusions of the exercise.

Linstone and Turoff (1975) claimed an important issue in the Delphi process is the understanding of the aim of the exercise by all expert panelists. When the panelists understand the goal, they become less frustrated and less likely to lose interest. Linstone and Turoff argued that technical experts must be convinced that their judgments may need to be made before all aspects of the problem are available which may be different from their standard decision-making process. The experts should be persuaded that the judgments are still a valuable piece of data.

Anonymity for participants is an important factor in the Delphi process. Okoli and Pawlowski (2004) wrote that the participants are always anonymous to each other but not the researcher. Habibi, Sarafrazi, and Izadyar (2014) wrote that in groupthink exercises some members could dominate weaker members and pressure the weaker members to confirm that results in ineffective problem-solving. The anonymity principle of the Delphi design solves this problem (Habibi et al., 2014; Linstone & Turoff, 1975).

The initial set of questions were carefully crafted. Linstone and Turoff (1975) and Skulmoski et al. (2007) pointed to the need for the researcher to decide at the beginning of the design if the initial set of questions will be focused or broad and open-ended. When the questions are focused, the participants are guided to a certain goal. When broad questions are designed, I could collect more data and from a wider range of responses.

For this study, I asked a broad set of open-ended questions to allow for a range of qualitative responses. Each subsequent round narrowed the results. The filtered results may lead to an improvement in controls and processes necessary for response to a computer crime caused business interruption.

Participant Selection Logic

The Delphi design does not require a statistical sample that attempts to be representative of a population but instead is intended as a groupthink mechanism that uses qualified experts who hold specific knowledge of the subject being studied (Okoli & Pawlowski, 2004). Skulmoski et al. (2007) cautioned that as the panel size increases with experts, the more cumbersome the analysis of the data becomes. The Delphi technique allows a panel of about 15-18 experts to collaborate to generate themes, disparities, or reach consensus (Linstone & Turoff, 1975; Okoli & Pawlowski, 2004). A requirement for the Delphi to be valuable comes from the selection of the qualified experts. Approximately 70 experts were invited to participate in this study. The final panel size of 22 was large enough to determine patterns in the responses without the data becoming overwhelming. This sample size was large enough to see patterns in responses but not large enough to overwhelm the data analysis process of all responses. Five experts were selected to represent disaster recovery first responders, five experts were selected from disaster recovery researchers, and five experts were selected from a cybersecurity background. The disaster recovery responders in the panel were selected from disaster recovery programs of businesses that are large enough to fund a full-time disaster recovery program, properly plan, conduct testing, and have experienced an interruption

from computer crimes. The disaster recovery researchers must have multiple published, peer-reviewed papers on disaster recovery. The DR researchers that authored publications need their research to study current trends in disaster recovery. Each participant was selected based on interviews, recommendations, or their visibility as a researcher in this subject matter. The diversity of knowledge was considered an important selection factor along with the field of expertise when the participants were asked to join the research. This panel included an adequate number of experts who are interested in identifying a successful strategy for disaster recovery. Organizations including Information Systems Audit and Control Association (ISACA), Information Security Certification (ISC2), Information Systems Security Association (ISSA), Cloud Security Alliance (CSA), and the InfraGard were contacted for applicable participants in the United States. Experts from the disciplines of emergency management, information technology disaster recovery, and cyber resiliency were asked to rate qualitative indicators using the Delphi design.

Potential expert participants received an email invitation to participate (see Appendix A). The research topic and description of the study was explained. The email described the protection of the expert's identity. Each expert panelist was asked to agree to a consent form (see Appendix A). The anonymity of the panel experts is protected because the only expert opinion will be collected. Participant identity was not be revealed in the study. The consent form includes an explanation of the study in clear language as outlined by the Walden's Institutional Review Board (12-11-17-0500644). The consent form included a description of the importance of the study, the research process, and the

Delphi expectations. The form also includes a note that participation in the study is voluntary and that the expert participant can leave the study at any time.

Instrumentation

When sufficient information about the topic is available, it is appropriate for the researcher to create the first round of questions and streamline the process for the panelists (Hsu & Sanford, 2007). Delphi is used to develop a consensus from independent judgments on the research topic or identify discourse for follow-up interviews. The following questions were used for the study regarding best practices and understanding from the disaster recovery literacy:

1. What factors significantly affect the ability of disaster recovery programs in responding to computer crimes caused disasters?
2. How successful can disaster responders be when following traditional technology disaster recovery plans to recover from computer crimes caused business interruption?
3. What steps could be an improvement for resumption from a computer crimes disaster?
4. What interruptions caused by computer crimes cause the response team to recover differently than a traditionally planned recovery?
5. What differences can be found from a business that prepared for interruptions caused computer crimes as compared to those that do not?

6. What common themes exist where the cause of the technology interruption could have been significantly reduced by modification of the information technology disaster recovery framework to align with a cybersecurity framework?

The design includes a note for the disaster recovery and cybersecurity experts with questions for the first round of the Delphi study. The participants were provided their understanding of forecasting trends and analysis of possible controls that can improve the disaster response. A final list was created by a pilot study.

Pilot Study

Linstone and Turoff (1975) suggested the researcher pilot the study on any willing expert participants, including the sponsor, before finalizing each round. Okoli and Pawlowski (2004) wrote that pretesting appeared to be an important reliability attribute for the Delphi design but argued that the test-retest reliability is not relevant since it is expected that participants will revise their answers to the surveys based on feedback from the other participants. Skulmoski et al. (2007) claimed the pilot is important for inexperienced researchers who may underestimate the survey and participant response.

This pilot intended to determine if the instructions are understandable, if the questions are clear and concise, can the pilot participants provide suggestions for the improvement of the materials provided, and if the data that was collected aligned with the intent of the study. The pilot can improve the process by working out any procedural of comprehensive problems. The pilot study was conducted with an open-ended list of initial questions described in the instrumentation section above. The final revision of the

questions for the first round was created during the pretest by the experts in the pilot study.

Procedures for Recruitment, Participation, and Data Collection

The purpose of this qualitative Delphi study was to understand how information technology disaster recovery controls and processes can be modified to improve response to a computer crime caused business interruption. The outcome should provide new mitigating controls that can improve the response when a technology disaster is experienced. The Delphi design and participant recruitment for this study were conducted using electronic mail. An advantage of a Delphi design is the ability to conduct the study entirely over the Internet (Skulmoski et al., 2007). As the researcher, I received the emailed responses during each round and crafted the feedback that was sent back to the panel. The Delphi was scheduled to be conducted over three rounds with an expert panel of between 15 and 20. For each round, the panelists will be asked to respond within one week. After a week of no responses, I contacted the nonparticipants to encourage their responses or confirm their exit from that round. As described in the participant selection logic, the number of experts asked to participate in the Delphi was designed to allow for participants to drop out of the study and still allow the study to provide valuable knowledge and consensus. As the Delphi was conducted via email, the data remained in the panelist's original responses in the existing digital format. Feedback, individual responses, and further clarifying questions were communicated over email and retained as data to be analyzed. Participants were notified that the study had ended after the third round of the Delphi has completed and all feedback had been accepted.

Data Analysis Plan

Quantitative Delphi responses are tabulated by the mean or median score from each round of questions. The median is considered the most valuable when tabulating quantitative scores (Dalkey, 1967). Skulmoski, Hartman, and Krahn (2007) wrote qualitative Delphi responses start with expert judgment about the research questions and will set the direction for the future rounds. Okoli and Pawlowski (2004) claimed the Delphi surveys could solicit quantitative, qualitative, or both and the research then analyzes the usable responses to investigate the research questions. The qualitative judgments serve the purpose of providing empirical data for the next round and increasing the understanding of the expert's factors (Okoli & Pawlowski, 2004). Linstone and Turoff (1975) wrote that each of these surveys would indicate an index of desirability, computed by the expert responses, will favor a consensus. The first set of responses from Round 1 was deduplicated, and a recording was made of the expert's judgments. A group of factors was generated into categories to make it easier for the experts when the next round was initiated. These feedback factors are not used for analysis by the researcher. The feedback was provided to the experts in brief explanations to validate the responses. The second round asked the experts to verify the interpreted responses and that their judgments are in the proper categories. The panelists could provide additional thoughts that may not have been recorded initially. The next two rounds narrowed down the factors that reflect the judgments of the experts. The list of responses was rated by the panelists on a 6-point Likert-type scale. The responses were calculated using a group means to score. The experts were asked to rank the factors. For

each factor, the consensus level was set at 80% of expert agreement. The third round presented the completed, consolidated list of judgments to the panel and allowed for reconsiderations. During the third round, the panelists were asked to reconsider any questions where group consensus was not found.

The qualitative data collected during the three rounds were analyzed using the NVivo computer software program. Leech and Onwuegbuzie (2011) and Zamawe (2015) claimed the qualitative researcher is the main tool for analysis and computer-assisted qualitative data analysis (CAQDAS) software is only a tool for assisting the researcher by providing multiple views of the data. The CAQDAS is used so that underlying relationships can emerge and can allow the analysis to yield more details than if the analysis was conducted manually (Leech & Onwuegbuzie, 2011). Zamawe (2015) wrote that NVivo CAQDAS software, created by QRS International, is used to analyze qualitative designs such as grounded theory, ethnography, literature reviews, phenomenology, and mixed methods. NVivo allowed the data to be examined and increased the understanding of the judgments and codes reviewed in the study. NVivo was also used to manage the storage and catalog of judgment data. The NVivo features of word count and classical content analysis were used to understand underlying themes from the judgments provided by the experts (Leech & Onwuegbuzie, 2011).

Issues of Trustworthiness

Credibility, transferability, dependability, and confirmability are qualitative research concepts that describe the level of findings that represent a quality inquiry. To address these concepts, I have outlined the elements that are incorporated into this

research that met the requirements of a quality study. Each section includes how the concepts are followed by the Delphi design or my role as a researcher.

Credibility

Credibility is associated with the concept of truthfulness. Linstone and Turoff (1975) wrote that the initial Delphi qualitative questions are broad and open-ended. Extra care must be made by the researcher to ensure the initial set of qualitative questions set the proper path for the research and do not lead the panelists down a predetermined path. The researcher may see limitations in the research by not executing Delphi with a proper set of initial questions, not populating the panel with the correct expertise, and not correctly communicate the requirements of the participants. To address these limitations, I worked with the committee to refine the initial round of questions, conduct a pilot round to solidify the questions and instructions, diligently seek the proper panel members, and carefully craft communications to each participant. I expected that not all the participants will complete the multiple rounds of the Delphi design in the proposed time frame. The number of participants that were chosen amounted to a number large enough to allow for the loss of multiple panelists as well as to obtain data saturation (Day & Bobeva, 2005). Day and Bobeva (2005) and Skulmoski et al. (2007) wrote the appropriate number of participating experts helps to strengthen the credibility of the study. The Delphi data collection procedure supports the development of improvement to the disaster response from computer crimes. The participants will have the opportunity during each round to contribute to the development of the disaster recovery factors and provide suggestions on how to improve the process.

Transferability

Clibbens, Walters, and Baird (2012) claimed the most common means of increasing the validity of Delphi study is to test the instrument with a pilot test for the first round of questions. The transferability of the items in the instrument was achieved by a smaller panel of disaster recovery and cybersecurity expert chosen from my network of colleagues that do not take part in the formal study. The pilot panel reviewed the first round of content for relevance and clarity and provided feedback for improving the questions. The Delphi design can employ further construct transferability when asking the panel experts to validate the researcher's interpretation and factor variables. Linstone and Turoff (1975) claimed the validity of the combined group judgment is typically measured regarding consensus of the experts. While findings of this Delphi study may not apply to all disaster recovery programs, I made every effort to ensure the expert judgments and researcher coding from this study aligned with other research found in the literature.

Dependability

Dependability in qualitative research can be obtained from the role of the researcher in data collection, clear communication with the participants, and quality checking of the collected data (Patton, 2015). Linstone and Turoff (1975) wrote that dependability of the Delphi is demonstrated in group statistical summaries of the responses. Okoli and Pawlowski (2004) wrote that the pilot testing is also a dependability method for a Delphi study. Both the pilot panel and the formal panel should show the same direction in their qualitative data judgments for solving the disaster recovery

scenario. Skulmoski et al. (2007) highlighted that audit trails help to confirm trustworthiness of a study's findings and the methodological process of the Delphi has this attribute. I captured all questions, responses, feedback, calculations, and coding for each round of the Delphi. A clear decision trail was recorded from the beginning to the end of the study. The research was further triangulated by follow-up evaluation interviews when outliers were recorded. Day and Bobeva (2005) claimed a Delphi could maximize the quality of the outcome and confirm results with an electronic survey and evaluation interviews. The Delphi questions were clearly defined with an alignment from the review of the literature in Chapter 2 and were incorporated into the first round to improve dependability.

Confirmability

Conformability requires the researcher to be explicit about the methods executed in data gathering, data analysis, participant selection, and the forming of the conclusion (Miles, Huberman, & Saldana, 2014). In the Delphi design, the researcher is a facilitator and not a participant (Day & Bobeva, 2005). This allowed the data collection to come directly from the participants and reduce the impact of researcher bias. Linstone and Turoff (1975) claimed the Delphi design could lend a greater than objectivity than other qualitative inquiries from the methods used in the data collection and revisions by the panelists. Donohoe and Needham (2009) wrote the systematic method allows participants to express their opinions which ensure rational and reflexive opinions that are not influenced by a dominating panelist. Donohoe and Needham wrote that no study is free of bias and researchers using the Delphi design must consider critical design decisions in

pretesting and the potential for misinterpretation. Linstone and Turoff pointed out that since panelists are encouraged to suggest new questions and modify existing ones the potential for research bias is low. Statements that comprise the Delphi can reflect cultural opinions, and subjective bias from the researchers that formulate them and I will seek to remove any bias in the process of the survey creations. To enable confidence in the data, a rationale was provided to show how the initial set of questions was initially crafted. This rational combined with the audit trail assists with dependability and confirmability.

Ethical Procedures

Ethical considerations for qualitative research include the proper treatment of the participants, securing, and handling of the collected data. The topic of information technology disaster recovery activity resulting from computer crimes does not raise an ethical concern for the participants or from the organizations they are employed. The panelists were not identified with a business, even to each other, so that there could be no negative perceptions of an entity or employer. Disaster responders and technology management are not considered a traditional protected class in scientific research. The judgments made by the expert panel sought to better respond to a technology interruption caused by computer crimes. The judgment data collected from the experts was not a confidential data set. The data collected were the opinions of the experts, and all data was being stored in an encrypted format while being analyzed. After the data was analyzed and summarized, it is electronically destroyed after 5 years. Research by Goodman et al. (2012) pointed out the requirements that employees may have to protect the intellectual property of their employer. During this study, I ensured confidentiality was maintained

for both participants and their organization to protect any negative effect that could arise from participating in this study.

Summary

Disaster recovery planners, incident responders and cybersecurity experts used their knowledge and understanding of disaster recovery and computer crimes interruptions to identify strategies and mitigating controls to use when developing improved plans for responding to disasters. The Delphi design is an effective and efficient group think the approach to solving technical problems. The expert panel had the experience to provide judgments on improving disaster recovery strategies to combat emerging technology threats. The Delphi instrument provided anonymity and an efficient technique for the panelists to communicate with the researcher. Chapter 3 includes a review of the Delphi design and details on how participants were selected. This explanation supports how the panelists will collaborate and provide qualitative data to the researcher. The results of the Delphi study are discussed in Chapter 4. The study details, expert comments, coding, and scores will be included.

Chapter 4: Results

Chapter 4 includes the results and findings from the Delphi panel of experts on disaster recovery and cyber security of computer crimes interruptions. The Delphi study intended to document the expert opinion on how organizations can improve the disaster recovery process when responding to computer crimes. Data were collected using questions corresponded over electronic mail or LinkedIn messaging. For the second and third round, data were collected using a 6-point and 5-point Likert scale. The group median for the research questions was communicated to the panel to allow for feedback, additional trends, and expert analysis. With a growing threat of technology disasters that can significantly affect organizations, this study might assist in improving processes to remediate and recover business operations.

This Delphi used qualitative seed questions, developed from the literature review, to populate the first round. The following Round 1 questions guided the study and were used in the pilot:

1. What factors significantly affect the ability of disaster recovery programs in responding to computer crimes caused disasters?
2. What interruptions caused by computer crimes cause the response team to recover differently than a traditionally planned recovery?
3. In what ways can a disaster response be unsuccessful when following traditional technology disaster recovery plans to recover from computer crimes caused business interruption?

4. What steps could be an improvement from traditional disaster recovery procedures to resume the organization from a computer crimes disaster?
5. What differences can be found from a business that prepared for interruptions caused computer crimes as compared to those that do not?
6. What should organizations avoid to improve the ability to recover from computer crimes?
7. What common themes exist where the cause of the technology interruption could have been significantly reduced by modification of the information technology disaster recovery framework to align with a cybersecurity framework?
8. What type of expertise should be recruited to build a successful disaster recovery program that could better respond to computer crimes?
9. What cybersecurity processes could improve disaster response if any?
10. What advantages or disadvantages exist in specifically defining cybersecurity risk and controls in information technology disaster recovery frameworks?

The open-ended Round 1 questions focus on multiple disaster recovery themes. The first three questions presented in the first round seek to understand attributes that can positively or negatively affect the resumption of the organization. The following three questions inquired about processes or procedures that improve the response. The remaining questions collected judgments on improving an existing DR framework and opinion on needed organizational expertise for disaster recovery teams. This chapter includes a review of the pilot design, the research setting, demographics, data collection, analysis, evidence of trustworthiness, and the study results.

Pilot Study

To assist in the trustworthiness of this research, a pilot study was used. The pilot study consisted of three experts who met the eligibility criteria used to select the participants for the main study. One expert from each demographic consisting of disaster recovery researcher, disaster recovery incident responder, and cybersecurity expert was used. The purpose of the pilot was to collect feedback to verify, clarify, and refocus any directions or questions for the first round of the Delphi study. The pilot study used the predefined study directions and 10 research questions to understand how each pilot participants would navigate the returning of the first round's data. After I analyzed the pilot submissions, each expert was given feedback and the opportunity to make changes or suggestions to improve the questions and instructions that would be used in the main study. The participant's expertise provided feedback to improve the initial instructions by including a definition of information technology disaster recovery and modifying the ninth seed question to describe better the intent of the questions focus on cybersecurity.

Research Setting

The data collection for the Delphi were electronic instead of observations, focus groups, personal interviews, or action research. One advantage of the participants submitting electronic data was that the data was not being physically written down or transcribed by the researcher. The electronic data collection prohibited me from recording conditions that may have biased or influenced the participants while they contributed to the study. No other data were collected about the participants other than their initial consent to the study and the qualitative data they provided. The Delphi instrument did not

inquire about demographics, organizational conditions, or personal preferences that could have influenced the analysis of this data. Although there was a vetting process for each expert, the expertise of each participant was not recorded in this study.

Demographics

The request for expert panelists was successful in confirming 25 of 98 contacted for the study. The participant background was represented by:

- Disaster recovery researchers were recruited into the group.
- Expertise in the disaster recovery profession was recruited into the group.
- Expertise from the cybersecurity was recruited into the group.

The disaster recovery responders in the panel were selected from disaster recovery programs of businesses large enough to staff a full-time disaster recovery program, properly plan for, conduct testing, fully fund, and have experienced an interruption from computer crimes. The disaster recovery researchers had published, peer-reviewed papers on disaster recovery. The disaster recovery researchers that authored publications had their research study current trends in disaster recovery. Each participant was selected based on interviews, recommendations, or their visibility as a researcher in this subject matter. The diversity of knowledge was considered an important selection factor along with the represented field of expertise. This panel included an adequate number of experts who were interested in identifying a successful strategy for disaster recovery.

Twenty-two experts agreed to join this study. Of the 22, 17 participants completed the first two rounds of the study. Eight participants left the study after the second round, and nine participants completed the last round. Participants that were late with their

submission were contacted after a short timeframe. The participants were encouraged to complete the study but allowed to leave if necessary.

Data Collection

Recruitment

While waiting for IRB approval, I crafted a list of potential experts using multiple sources. LinkedIn and snowball sampling offered a successful source of experts for recruitment of expert participants. I planned to complete recruiting in a 3-week timeframe. The weeks provided sufficient time to confirm the requirements with the participants and requested phone calls with potential experts that wanted more detailed information about necessary expertise. Invitations were sent to roughly 96 individuals with a copy of the approved IRB consent form. Two of the prospective participants recommended additional experts that could satisfy this study's edibility requirements. Five experts were added to the participants from the snowball sampling. Twenty-two experts agreed to participate reaching an optimal target panel size. Additional participants were accepted in anticipation of a small number of participants abandoning the study before the completion of the third round. The Delphi followed the schedule found in Table 1.

Table 1

The Participant Delphi Schedule

Event	Start Date	End Date
Delphi Round 1	12/24/17	1/4/17
Round 1 analysis	1/4/18	1/6/18
Delphi Round 2	1/14/18	1/20/18
Round 2 analysis	1/20/18	1/22/18
Delphi Round 3	1/23/18	1/29/18
Round 3 analysis	1/29/18	1/30/18

Delphi Round 1

After consent was obtained, participants were provided the instructions and expectations needed to complete the study in a Microsoft Word format. Each expert was recognized for accepting to participate and for contributing to the technology community. The changes were made to the Round 1 questionnaire that was identified in the pilot test and on December 24, 2017, the first-round was initiated. The 22 participants were given a week to provide their responses to the qualitative seed questions that made up Round 1. Participants were instructed to record their responses in the document. A spreadsheet was used to record each participant's submissions. Each participant was assigned an alphanumeric number to allow for analysis of confidentiality. Statements by the participants were collected from the 10 seed questions. The statements were coded, deduplicated, and, after considering the conceptual framework, I identified several

themed statements for the second Delphi phase. The themed statements were sent back to the participants to discover if a consensus could be found in the statements.

Delphi Round 2

The codes and themed statements that can impact disaster recovery were shown in the participants' Round 1 submission. The second round provided the participants with the statements that stemmed from the first-round submissions. Linstone and Turoff (1975) provided a common 6-point Likert scale for Delphi judgments following the first round of submissions as explained in Table 2.

Table 2

Agreement Scale Used for the Round 2 Judgment

Scale	Agreement
6.	Strongly agree
5.	Agree
4.	Slightly agree
3.	Slightly disagree
2.	Disagree
1.	Strongly disagree

The participants were asked to provide a 6-point Likert scale on the themed statements. Each participant could comment on the coding that was created by their submissions to facilitate member checking. For submissions ranked at a 2 or less, it was encouraged for the participant to provide feedback for a better understanding of the

judgment. Participants were encouraged to qualify why they disagreed with the themed statement. Appendix D lists the Round 2 questions. In interpreting what a group means, a value of 3.5 is considered the natural point and anything above a 4 is an agreement by the panel. A mean value of 4.5 to 6 results in a general agreement. An 80% agreement from the participants, an interquartile range below 2.5, and a standard deviation below 1.5 are commonly used for consensus measurement (Giannariu & Zervas, 2014). The data collected from the participants were placed into a spreadsheet and analyzed for percent agreement, mean, standard deviation, and the interquartile range. The consensus statements were used to build the third round of the Delphi.

Delphi Round 3

The third round of the study was used to identify the importance of the consensus statements identified in Round 2. The participants were instructed to judge the statements on how important that statement would be for the organization to implement with the intent of improving recovery from computer crimes. For the third round of the Delphi, an importance 5-point Likert scale was used. Table 3 defined the Likert scale used for participant agreement. The third round sought to understand what importance the participants would place on applying the consensus statement collected in Round 2. The instructions with the third-round questions asked for a judgment on the importance of the presented statements in influencing the ability of the organization to respond to computer crimes. See Appendix E for a copy of the Round 3 questionnaires.

Table 3

Importance Scale Used for Likert Judgment

Scale	Agreement
5.	Very Important
4.	Important
3.	Moderately Important
2.	Slightly Important
1.	Not Important

Data Analysis

The thematic analysis in qualitative research is used to pinpoint, examine, and record patterns within the data collected (Maxwell, 2005). Thematic analysis was used in this study to create the statements used in the second round of the Delphi. The first round allowed for the participants to answer open-ended questions about disaster recovery and how organizations may better respond to an interruption. Several of the statements submitted were duplicates which were removed. I then used thematic analysis to create the statements for consensus building among the experts. After studying the participant's open-ended statements, I coded the data into categories. For this coding process, I did not bring a set of codes into the study. Multiple reviews were conducted of the statements, and the themed statements were placed into rows of a spreadsheet. Commonly used words, phrases, and acronyms were groups into themed statements. After each participant submitted responses, the themed statements were added to the Round 2 questionnaires or

modified to describe the coded themes better. This process was used to analyze down the hundreds of statements into 110 statements that were grouped by the 10 seed questions. Appendix D contains the themed statement that resulted from this process.

Linstone and Turoff (2002) claimed the objective of the original Delphi study was to obtain the most reliable consensus of a judgment from a panel of experts. Most Delphi studies include descriptive statistics put together of the median and frequencies collected from a survey of expert judgment. Giannariu and Zervas (2014) claimed that there is not a common practice in the Delphi literature to reach consensus. Giannariu and Zervas wrote that 51% of participant agreement, a specified distance from the mean, using standard deviation measurements, interquartile ranges, and coefficient of variation are all found in Delphi literature for computing consensus.

The Interquartile Range (IRQ) was described by Frankfort-Nachmias and Leon-Guerrero (2015) as a measure of variation for interval-ratio variables. Frankfort-Nachmias and Leon-Guerrero defined the IRQ as the difference between the upper and lower quartiles by showing what the width of the middle 50% is. The interquartile range score was defined as the difference between the highest data point and lowest median obtained within a given set of data. Howard (2008) pointed out that the IRQ will point out scores that are heavily dependent on extreme scores. The IRQ assists in Delphi research by identifying where participant's judgments are widely different in the distribution.

Linstone and Turoff (2002) and Giannariu and Zervas (2014) described where the standard deviation and calculated means are commonly presented for consensus in a

Delphi. The standard deviation described by Howell (2008) is the positive square root of the variance of the sample collected. The standard deviation is commonly used to understand how many of the scores in the sample fall a deviation above or below the mean. For reasonably symmetric distributions, it can be stated that two-thirds of the sample will fall within one standard deviation of the mean. This measurement allows for the researcher to understand how closely together the Delphi participants have scored a question.

For this study, the mean, standard deviation, 80% participant agreement, and interquartile score were used in combination to reach a consensus. In interpreting the group means, a value of 4 and above is considered an agreement by the panel. Consensus for this study was obtained by four measurements used in combination:

- An 80% agreement from the participants was recorded.
- An interquartile range below 2.5 was recorded (Giannariu & Zervas, 2014).
- A standard deviation below 1.5 was recorded (Giannariu & Zervas, 2014).
- A mean score of greater than 4.0

The mean scores of the round one statements falling below 4.00 were eliminated from the third round of the Delphi. The analysis of the data also recorded a strong consensus measurement among the expert panel judgments which measured an 80% or greater of 5 and 6-point Likert scale on any specific statement that reached consensus.

When a Delphi has a third round, the round is often used to evaluate data that falls outside the median or to prioritize statements (Linstone & Turoff, 2002). The third round

in this study did not continue to evaluate consensus but allowed each participant to apply their opinion of importance in implementing the consensus statements.

Evidence of Trustworthiness

Credibility

The objective of credibility is to describe the concept of truthfulness in the research findings. Linstone and Turoff (1975) wrote that Delphi questions must be carefully chosen by the researcher to allow the panelists to set the direction of the judgments instead of following a predetermined path. To address Delphi credibility limitations, I worked with the pilot participants and the committee to refine the seed questions, diligently sought the proper expert panel members, and carefully crafted communications to each participant.

Day and Bobeva (2005) and Skulmoski et al. (2007) wrote that obtaining the correct number and expertise of participants strengthens the credibility of the study. The number of expert participants in the study allowed for the loss of panelists without impacting the ability to obtain data saturation (Day & Bobeva, 2005). The data collection of this study supported the development of improvements to the disaster response from computer crimes. For each round, participants had the opportunity to contribute to the development of the disaster recovery factors and provide suggestions on how to improve the process. The feedback returned ensured the data that was coded and analyzed by the researcher had the expected intent of the participant. Before the second and third rounds were initiated, all submitted feedback was collected and confirmed for correctness if necessary.

Transferability

The most common means of increasing the transferability of a Delphi is to test the instrument with a pilot exercise for the initial round (Clibbens et al., 2012). The transferability of the items in the Delphi was achieved by a small panel of disaster recovery and cybersecurity expert. The pilot panel reviewed the Delphi first round of content for relevance and clarity. Feedback was provided for improving the questions in clarity and a better understanding of the intent of the research. Transferability was increased by asking the panel experts to validate the researcher's interpretation and factor variables. Linstone and Turoff (1975) wrote the validity of the Delphi judgment can be measured by consensus of the experts. Given the small and nonrandom sample of participants, this study may not be readily transferable. Additional studies with other participants may likely improve transferability.

Dependability

Patton (2015) claimed that dependability could be obtained by the researcher in proper data collection, providing clear communication with the participants, and attention to accuracy in the collection of data. Linstone and Turoff (1975) wrote that dependability could be found in a Delphi study by the calculation of group statistical summaries of the judgments. Okoli and Pawlowski (2004) wrote that the pilot testing is another mechanism to show dependability in a study. Skulmoski et al. (2007) claimed an audit trail could confirm dependability of a study's findings and the methodological process. Day and Bobeva (2005) wrote that a Delphi would maximize the quality of the outcome and confirm the results of a study with an electronic survey.

In this study, the pilot participants and the study participants indicated the same themes in their judgments for solving the technology disaster service interruptions, providing the correct expertise in personnel, and alignments with technology security frameworks. The audit trails retained in the Delphi technique captured all questions, responses, feedback, calculations, and coding for each round. A clear decision trail was recorded from the beginning to the end of the study. Additionally, the research was triangulated by follow-up evaluation questions with two participants. The initial 10 questions were clearly defined with an alignment from the review of the literature in Chapter 2.

Confirmability

Miles et al. (2014) wrote that conformability in a qualitative study requires the researcher to explicitly define the methods used for data gathering, analysis, selection, and conclusion. Linstone and Turoff (1975) claimed the Delphi method has clearly defined processes that are easily followed and clearly produces data that can be reviewed by additional researchers. The use of the thick description and audit trail allows for the conformability in the Delphi.

Day and Bobeva (2005) summarized that the researcher facilitating a Delphi method is not a participant. The Delphi method allows for data collection directly from the participants and minimizes researcher bias. The Delphi method will include a greater than objectivity to alternative methods because of the ability for revisions by the panelists (Linstone & Turoff, 1975). The systematic method allowed the expert participants to

express their opinions on their judgments without being influenced by a dominating participant.

It can be a difficult statement to claim a study is free of bias, and a researcher using the Delphi should place considerations on design decisions (Donohoe & Needham, 2009). The ability for the panelists to modify the questions based on their judgments lowers the potential for research bias. Linstone and Turoff (1975) wrote that Delphi panelists are encouraged to suggest new questions and modify existing ones. Researcher statements made in the Delphi were carefully crafted to remove cultural opinions and subjective bias. Confidence in the data was found by rationale provided to show how the initial set of questions are initially crafted. This rational combined with the audit trail assists with dependability and confirmability.

Study Results

Round 1

Four hundred and thirty-one statements were collected from the participants in Round 1. The collected statements fell into five significant categories related to information technology disaster recovery:

- factors that come from computer crimes
- improvement steps
- planning for computer crimes
- integrating cybersecurity
- necessary job skills

After collecting and coding the data, considering the conceptual framework, and reducing duplicate answers, several statements were developed for Round 2 consensus building. The Round 1 coding activity produced 16 themes that were used in the construction of the Round 2 statements. Most every participant provided multiple, duplicate statements to one or more of the seed questions.

Table 9

Round 1 Statements

Category	Round 1 Statements
Significant factors that come from computer crimes	107
Improving the ITDR response	94
ITDR planning for computer crimes	81
Integrating with cybersecurity	105
Necessary Skillsets for responders	44

Appendix F includes the removal of duplicate statements made. The statements were coded by being placed in a spreadsheet for sorting and a color application. 16 disaster recovery themes were generated and are listed in Table 4.

Table 4

Round 1 Codes From the Seed Questions.

Code/Category	Frequency
Lack of understanding or confusion	18
Management support	6
Prover versus poor funding	6
Skills, roles, and training	26
Lack of scope	5
Traditional playbook weakness or strength	21
Testing / Lessons learned	14
Root cause analysis	9
Aligning with cybersecurity	16
Enterprise risk assessment	15
Poor versus proper planning	26
Capacity planning	3
Co-location – data resilience	15
ITDR team cooperation with cyber	21
Toolsets	5
Policy or regulatory requirements	9

The data provided by the participants were grouped into 110 statements developed from the first round of open-ended questions. The people skills and roles, proper planning, and cyber security cooperation categories created the largest number of codes. The capacity planning, toolsets, project scoping, funding and management support categories held the least amount.

Round 2

The Round 1 data collection included 431 statements from the 10 qualitative, open-ended questions. The 431 statements were analyzed ad themed into 110 statements relating to the seed questions. The themes were broken up into multiple statement relating to the questions as described in Table 5. Appendix D contains the complete list of Round 2 questions sent to the participant panel. Participants could provide additional comments on the statements to clarify their answers better. Three participants provided additional reasoning and explanations. I did not receive any feedback on the need for a greater explanation of the statements or how the statements were generated.

Table 5

Themed Statements Created From Round 1 Analysis

Seed Questions	Themed Statements	Consensus found
Question 1	13	11
Question 2	7	5
Question 3	12	8
Question 4	13	11
Question 5	6	5

Question 6	15	12
Question 7	11	7
Question 8	12	6
Question 9	12	8
Question 10	9	6

Of the 110 statements sent to the participants, the consensus was found on 79 statements. Table 6 includes the statements that met the consensus requirements outlined in this study. Questions 7, 8, 9 and 10 recorded the most amount of statements lacking the criteria needed for consensus. The theme of Questions 7, 9, and 10 included cybersecurity frameworks that may apply to disaster recovery. Question 8 statements included perceived job skills needed for a computer crimes business interruption.

Table 6

Participant Consensus From the Round 2 Analysis

Delphi Statement	MEAN	SD	CON	IRQ
Lack of understanding of the interdependencies in IT makes it difficult to anticipate the impact of the recovery.	5.40	0.99	0.93	1.00
The organization must have adequate planning for computer crimes.	5.07	1.03	0.93	2.00
Critical IT services must be available to conduct a recovery.	4.60	1.06	0.80	1.00
A lack of management support and poor funding will negatively impact this response.	5.07	1.03	0.93	2.00
If the organization does not staff skilled resources, the response will suffer.	5.33	0.65	0.93	1.00

The untested recovery process from computer crimes will negatively impact the recovery process.	5.17	1.03	0.87	1.25
The ability to triage the incident correctly as the ITDR team comes on the scene will be an issue when the cause is computer crimes	4.71	1.20	0.80	2.00
IR teams must be trained for such a scenario.	5.07	0.73	1.00	0.75
Delphi Statement	MEAN	SD	CON	IRQ
Organizations conducting lessons learned will improve their response.	4.93	0.73	1.00	0.75
Critical data must be protected and available from an alternate source to protect from computer crimes	5.25	0.87	0.87	1.00
There must be a clear list of responsibilities in responding to this type incident.	5.17	0.83	0.93	1.25
Organizations may need to document their computer crimes recovery differently for compliance/legal/law enforcement reasons.	3.86	1.21	0.80	2.00
Computer crimes can render critical systems unable to support a recovery where traditionally it would.	5.00	1.00	0.93	0.50
It will be hard to identify compromised versus uncompromised systems for recovery.	4.57	0.98	0.87	1.00
A triage of a computer crimes attack can lead to multiple activities of containment outside of the recovery process.	4.71	1.11	0.93	1.50
Computer crime related recovery is much more variable, and it is very difficult to determine the variables effectively.	4.45	1.04	0.87	1.00
If a data backup/alternative is not available, traditional recovery will not be successful or extremely time-consuming.	4.82	1.08	0.87	1.00
If an organization finds itself in a response that it has not scoped, it will trip upon the response.	4.14	0.90	0.73	1.50

When a breach occurs, the organization may lack the ability to anticipate and quantify the damage. This would hamper the recovery.	5.14	0.90	1.00	1.50
An organization may not have outside resources available to assist with a computer crimes interruption. For example, an organization may not have an InfoSec resource on retainer.	4.63	1.30	0.87	1.25

Delphi Statement	MEAN	SD	CON	IRQ
The organization has a lack of alignment with IT goals and business goals.	4.14	0.69	0.80	0.50
A Traditional DR playbook may not eradicate the intrusion correctly.	5.09	0.70	1.00	0.50
The DR team may have a poor understanding of the attack which could cause the activation of the wrong recovery solution, delaying, or stopping the overall business resumption.	5.29	0.76	1.00	1.00
If organizations do not test for the computer crimes scenario, it will fail to recover on time.	4.86	0.90	0.93	1.50
Computer crimes are more complex and involve greater communication and collaboration outside of IT and the IT Security team.	5.00	1.07	0.87	1.50
Keep the soft copy of the DR plan offline from the main company environment so that it cannot be hacked.	4.86	1.07	0.80	1.00
Craft procedures where data is lost or corrupted and recovery have to be initiated using physical backups.	4.63	1.06	0.80	1.25
A separate set of procedures for cybercrime that takes into consideration the risks of computer crimes interruptions.	4.71	0.76	0.87	1.00
Real-time data synchronization to alternate locations would improve recovery from a computer crime interruption.	4.29	0.95	0.80	0.50

An improvement would come from lessons learned and cause analysis sessions.	5.00	0.82	0.93	1.00
Security architectures must use technology in support of business objectives, and accurately model dependencies to prioritize resources.	5.14	0.69	0.87	0.50
Organizations must focus on people, communications, tools, and facilities to improve from computer crimes interruptions.	4.71	0.76	1.00	1.00

Delphi Statement	MEAN	SD	CON	IRQ
Preventive and testing measures must be taken continuously for computer crimes.	4.71	0.95	1.00	1.50
Containment and eradication procedures for computer crimes will need to be included in playbooks.	5.29	0.76	0.93	1.00
Embed a Cybersecurity Framework into the ITDR program.	4.29	1.50	0.87	2.00
I have seen organizations struggle to recover from a typical disaster recovery effort and fail completely when attempting to recover from a computer crime event.	4.71	0.76	0.87	1.00
The prepared organization will not rely on one solution to protect everything.	4.86	0.90	0.93	1.50
Companies more heavily invested in preparing for computer crime-based interruptions have greater integration with their Information Security counterparts and have a management team that understands the risks posed by computer crimes and are willing to devote more money and attention to prevention and preparation for computer crime interruptions.	4.87	1.19	0.87	1.50
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by computer crimes.	5.13	0.99	0.87	1.00

Organizations must provide a robust awareness program to ITDR teams to help mitigate computer crimes risks.	5.00	0.82	1.00	1.00
Organizations cannot treat a computer crimes recovery as just a “technical” or “IT” led the response to better respond to computer crimes.	5.47	0.83	0.93	1.00

Delphi Statement	MEAN	SD	CON	IRQ
Organizations must avoid the knee-jerk reaction to throw money at a problem without first grasping what that problem is and then smartly coming up with the solution.	5.14	0.90	0.93	1.50
Organizations must avoid open source systems for critical business applications to better respond to computer crimes.	3.36	1.21	0.40	1.00
Organizations that do not conduct lessons learned and root cause analysis will not improve to better respond to computer crimes.	5.29	0.76	1.00	1.00
Organizations should avoid placing a low value on quality management in DR to better respond to computer crimes.	4.71	0.95	0.81	1.50
Organizations must avoid architectures that lack redundancy or resiliency attributes to better respond to computer crimes.	5.00	0.58	0.93	0.00
Organizations must avoid thinking they are protected from computer crimes.	5.43	0.53	1.00	1.00
Organizations must avoid neglecting the risk of computer crimes interruptions.	5.13	0.99	0.93	1.50
Organizations must not focus on speed but instead focus on the assessment phase to better respond to computer crimes.	4.57	0.98	0.80	1.00

Organizations must avoid having missing cybersecurity policies to better respond to computer crimes.	4.43	0.98	0.87	1.00
Organizations must avoid operating DR functions without the proper funding to better respond to computer crimes.	4.57	0.98	0.93	1.00

Delphi Statement	MEAN	SD	CON	IRQ
Organizations cannot operate ITDR and InfoSec in different silos to better respond to computer crimes.	5.53	0.64	1.00	1.00
A well-developed cybersecurity framework supports the ITDR, and the opportunity for a technical interruption is reduced.	4.80	0.77	1.00	1.00
A coordinated process alignment between Disaster Recovery and Information Security frameworks is vital to reducing the recovery of this type.	5.27	0.59	1.00	1.00
DR and InfoSec should be aligning their lifecycle processes, so that like steps are executed together, and participation is integrated.	5.29	0.76	1.00	1.00
Developing an ITDR set of practices and different playbooks will reduce the response.	4.14	0.90	0.80	1.50
Resilience efforts should be folded into dependency models to reduce the response to this interruption.	4.29	0.76	0.87	1.00
Advanced preparation will reduce a computer crimes response.	5.00	1.15	0.80	1.50
There is not much alignment between DR and InfoSec frameworks, and that is a problem.	4.73	1.10	0.80	1.50
A deep understanding of interdependencies in the IT environment will improve the response to computer crimes.	5.27	0.59	1.00	1.00

A business-focused understanding of the organization will improve the response to computer crimes.	5.00	1.15	0.87	1.50
A risk-based focus on the business will improve the response to computer crimes.	5.33	0.72	1.00	1.00
Technical, analytical, logical, and lateral thinking will improve the response to computer crimes.	4.57	0.79	0.80	1.00

Delphi Statement	MEAN	SD	CON	IRQ
A basic understanding of the layers of protection, prevention, policy management, operations, monitoring, and response will improve computer crimes recovery efforts.	4.29	0.49	1.00	0.50
Cyber Security expertise needs to exist to improve the response to computer crimes.	4.57	0.79	0.87	0.50
Enterprise Security Risk Management (ESRM) in the ITDR process	5.20	1.08	0.93	1.00
InfoSec training for ITDR teams	4.57	0.79	1.00	1.00
Organizations can integrate the RMO and CSO responsibilities into ITDR planning activities.	4.00	1.15	0.87	1.50
Formal lessons learned and future prevention, which may help lessen the severity of future incidents.	4.71	0.76	1.00	1.00
Establishing a baseline of security configurations is another cybersecurity process that extends to ITDR.	4.71	0.76	0.93	1.00
Asset inventory processes.	4.57	0.53	0.80	1.00
Penetration testing and disaster recovery testing	5.00	1.00	0.80	0.50
CAG 20 Critical Security controls would improve the recovery.	4.57	0.53	0.87	1.00
Organizations should include InfoSec risks in ITDR frameworks.	5.13	0.92	0.93	1.00

If done well, clearly following an ESRM program and linking the outcomes of the framework to the DR framework offers organizations the ability to see the interdependencies between assets and objectives.	5.00	1.00	0.87	1.00
Without cyber being a part of that plan the plan itself will be lacking.	4.86	0.69	0.93	0.50

Delphi Statement	MEAN	SD	CON	IRQ
If done properly, cybersecurity risk management will identify the DR systems as one of the most business-critical systems in the organization.	4.33	1.45	0.80	1.00
Integrating some cybersecurity risks and controls in your disaster recovery process may allow it to easier identify attacks that would otherwise be considered a "system malfunction."	4.71	0.49	0.93	0.50
A cybersecurity framework integration could provide an advantage in that it provides a 2nd or 3rd layer of risk management to the disaster recovery framework.	4.43	1.40	0.80	1.00

Round 3

In this study, 29 statements of the 110 fell below the combined measurements needed to reach consensus and were not used in the third round. Of the 79 statements that reached consensus, 71 statements could be used to understand the importance of applying that statement to an organization to improve a computer crimes response. The eight statements that were filtered out in round three were not statements that could apply to improving an disaster recovery response to computer crimes. The filtered statements pointed to important knowledge on disaster recovery but did not directly apply to an

improvement action an organization could take. Appendix E lists the entire list of Round 3 questions.

During Round 3, the participants were given the opportunity to rank the importance of the consensus questions identified in round two. Of the 71 consensus statements, 32 statements reached a consensus on the importance to the organization. Table 7 includes the statements that reach a consensus on the importance to be implemented in an organization.

Table 7

Round 3 Consensus Statements on Importance

Round 3 statements	MEAN	SD	CONS	IRQ
Lack of understanding of the interdependencies in IT makes it difficult to anticipate the impact of the recovery. Improve understanding.	4.63	0.7	.88	.025
A lack of management support and poor funding will negatively impact this response.	4.50	0.8	.88	1
The ability to triage the incident correctly as the ITDR team comes on the scene will be an issue when the cause is computer crimes.	4.25	0.7	.88	1
The organization has a lack of alignment with IT goals and business goals.	4.25	0.7	.88	.25
The DR team may have a poor understanding of the attack which could cause the activation of the wrong recovery solution, delaying, or stopping the overall business resumption.	4.63	0.7	.88	.25
Security architectures must use technology in support of business objectives, and accurately model dependencies to prioritize resources.	4.25	0.7	.88	1

Organizations must focus on people, communications, tools, and facilities to improve from computer crimes interruptions.	4	0.5	.86	0
Containment and eradication procedures for computer crimes will need to be included in playbooks.	4.38	0.7	.88	1
Embed a Cybersecurity Framework into the ITDR program.	4.5	0.8	.88	1

Round 3 statements	MEAN	SD	CONS	IRQ
The prepared organization will not rely on one solution to protect everything.	4.6	0.7	.88	.25
Companies more heavily invested in preparing for computer crime-based interruptions have greater integration with their Information Security counterparts and have a management team that understands the risks posed by computer crimes and are willing to devote more money and attention to prevention and preparation for computer crime interruptions.	4.38	0.5	1	1
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by computer crimes.	4.38	0.5	1	1
Organizations must avoid plans that do not take into consideration the current state of the systems to better respond to computer crimes.	4.13	0.6	.88	.25
Organizations that do not conduct lessons learned and root cause analysis will not improve to better respond to computer crimes.	4.25	0.7	.88	1
Organizations must avoid architectures that lack redundancy or resiliency attributes to better respond to computer crimes.	4.63	0.7	.88	.25
Organizations must avoid thinking they are protected from computer crimes.	4.75	0.7	.88	0

Organizations must avoid neglecting the risk of computer crimes interruptions.	4.5	.08	.88	1
A well-developed cybersecurity framework supports the ITDR, and the opportunity for a technical interruption is reduced.	4.5	0.5	1	1

Round 3 statements	MEAN	SD	CONS	IRQ
A coordinated process alignment between Disaster Recovery and Information Security frameworks is vital to reducing the recovery of this type.	4.75	0.5	1	.25
DR and InfoSec should be aligning their lifecycle processes so that like steps are executed together, and participation is integrated.	4.38	0.7	.88	1
Resilience efforts should be folded into dependency models to reduce the response to this interruption.	4	0.5	.88	0
There is not much alignment between DR and InfoSec frameworks, and that is a problem. Create alignment.	4.5	0.8	.88	1
A deep understanding of interdependencies in the IT environment will improve the response to computer crimes.	4.38	0.7	.88	1
A business-focused understanding of the organization will improve the response to computer crimes.	4.38	0.7	.88	1
A risk-based focus on the business will improve the response to computer crimes.	4.63	0.5	1	1
Technical, analytical, logical, and lateral thinking will improve the response to computer crimes.	4.5	0.5	1	1

A basic understanding of the layers of protection, prevention, policy management, operations, monitoring, and response will improve computer crimes recovery efforts.	4.25	0.7	.88	1
Implement Enterprise Security Risk Management (ESRM) in the ITDR process.	4.25	0.7	.88	1
Deploy InfoSec training for ITDR teams.	4.38	0.5	1	1
Round 3 statements	MEAN	SD	CONS	IRQ
Organizations should include InfoSec risks in ITDR frameworks.	4.50	0.5	1	1
If done well, clearly following an ESRM program and linking the outcomes of the framework to the DR framework offers organizations the ability to see the interdependencies between assets and objectives.	4.38	0.7	.88	1
Integrating some cybersecurity risks and controls in your disaster recovery process may allow it to easier identify attacks that would otherwise be considered a “system malfunction.”	4.38	0.5	1	1

The consensus statements made in this round provided a viewpoint on the perceived actions that an organization should consider at high importance. The 32 Round 3 statements represent only 40% of the round two statements that the participants felt were important enough to place a higher priority on implementation of the theme. Appendix G provided the analysis of the third-round submissions. In addition to the ranking of importance, the participants had the opportunity to provide feedback or comments on their submissions. Six participants submitted to the third and final round of the study. There were no comments or feedback given in this round by the participants.

Summary

Chapter 4 included the collection and analysis of three rounds of the Delphi study to understand the effects of computer crimes in the management of disaster recovery. The results of the study recapitulate the data collected from expert participants in the field of disaster recovery and cybersecurity. The results of this research communicated the insight of the experts and supported the practices that possibly could improve the response to computer crimes caused service interruption.

The qualitative statements and subsequent judgments provided by the first round of the Delphi produced 410 qualitative statements. The considerations involving planning, modification of disaster recovery playbooks, improving skills of the disaster recovery teams, and cooperation with cyber teams were identified as the top four largest coding categories as highlighted in Figure 5. Having toolsets, scoping exercises, funding, and management support were the least coded categories. The second round presented 110 themed statements for the participant's judgment. The judgments resulted in 79 consensus statements. The 79 statements focused on significant factors of computer crimes, problems of an unplanned response, improvement steps, planning for computer crimes, integrating cybersecurity into disaster recovery processes, and necessary job skills needed in the disaster recovery team.

Figure 5. Top 4 categories in the round one coding.

Round 3 was used to solicit the expert opinions on the importance of the consensus statements from Round 2. Participants considered the statements for organizations to implement to improve the disaster response from computer crimes. Of the 79 statements that reached consensus in the second round, 71 were presented to the participants in the third round. Of the 71 statements, only 32 or 45% meet the requirements for consensus to satisfy the importance for an organization to implement. The key findings of this study suggest:

- Organizations should dedicate effort to have a better understanding of the intricacies that technology has on business processes.
- Planning for computer crimes is crucial for the success of the recovery process.
- Alignment of disaster recovery and cyber security should improve the response to siloed activities.

- Cybersecurity training of disaster recovery teams will improve the planning and response to computer crimes interruptions.
- Lessons learned for computer crimes interruptions will improve the response activity for future events.
- An enterprise based risk management strategy, considering computer crimes, will improve the planning in the disaster recovery program.

Chapter 5 includes the conclusion of this research, implications, interpretations, limitations, and recommendations for this study.

Chapter 5: Discussion, Conclusions, and Recommendations

A large majority of organizations rely on technology for critical processes and service interruptions of any type may severely affect their offering. A review of the literature indicated a limited knowledge on how to effectively respond to computer crimes because of the relative newness of the attack and missing competencies needed by the disaster recovery team. The purpose of this qualitative study was to identify improvements that could be made to the resumption of an organization that experienced an interruption involving computer crime. Woods et al. (2016) described qualitative research as the combining of knowledge, experience, and understanding of a topic to allow the researcher to build an understanding of a phenomenon. A qualitative inquiry was chosen because it was the most appropriate design for gaining an understanding of the problem computer crimes interruptions cause to disaster recovery programs. The Delphi was selected over other qualitative approaches because of the desire for prediction and theory building in disaster recovery. This study allowed for the identification of controls, planning, processes, and skillsets that could be used to improve the resumption process. The Delphi allowed this study to contribute to the body of knowledge on disaster recovery as it pertains to the viewpoints of disaster recovery researchers, practitioners, and cybersecurity experts.

The results of this study included consensus statements by the panel on five central topics that described factors affecting recovery efforts from (a)computer crimes, (b) processes for improving the disaster recovery response, (c) disaster recovery planning, (d) integration with cybersecurity, and (e) desirable job skills. The key findings

of this study suggested that (a) organizations should have a better understanding of the intricacies that technology has on business processes (b) management support is essential for the recovery, (c) planning for computer crimes is crucial, (d) alignment of disaster recovery and cyber security should improve the response, (e) skillsets of responders should be considered, and (f) a risk-based focus on computer crimes will improve the planning in the disaster recovery program.

In this chapter, I explain inferences and themes that may be drawn from the Delphi results. I discuss the possible changes that can be made to a disaster recovery program to improve recovery times from a computer crimes interruption. The remaining sections of Chapter 5 are comprised of interpretations of the findings, limitations of the study, recommendations, and implications.

Interpretation of Findings

The results of this study included consensus statements by the participant panel on five central topics that produced 79 consensus statements on the effect of computer crimes in disaster recovery. Four hundred and thirty-one statements were collected in the first round of the study and themed down into 110 statements. In the second round, 31 of the original 110 statements did not reach the consensus formula that consisted of a mean of 4.0 or greater, 80% agreement, IRQ of less than 2.5 and SD less than 1.5. Table 8 contains the statements and consensus found from each round of this Delphi.

Table 8

Overall Delphi findings

Category	Round 1 Statements	Round 2 Statements	Round 2 Consensus	Round 3 Statements	Round 3 Consensus
Significant factors that come from computer crimes	107	21	16	10	5
Improving the ITDR response	94	27	19	19	7
ITDR planning for computer crimes	81	22	17	15	8
Integrating with cybersecurity	105	32	21	21	10
Necessary Skillsets for responders	44	13	6	6	5

The key findings of the study indicated that organization's disaster recovery leadership needed to focus on greater risk assessments of critical technology infrastructures outside of the traditional fire, flood, and loss of power. Planning for technology interruptions must now consider disruptions from technology vulnerabilities that could be leveraged by attackers to bring down organization's business processes. Planners and responder's skillsets must also be considered. Cybersecurity cross training on incident response and identification will improve the response to computer crime. The findings also pointed to integrating cybersecurity processes with a disaster recovery framework.

Delphi Round 1

The first round of the study provided 10 open-ended, seed questions to the participants. The original seed questions were derived from within the literature review. Seventeen participants of the 23 that agreed to join the study responded to the questionnaire. The initial 10 seed questions resulted in 431 statements corresponding to the five main themes in Table 8.

Significant factors that come from computer crimes. The first two seed questions collected factors from the participants that significantly affected the response to computer crimes and how the disaster recovery playbook may be impacted. One hundred and seven statements were submitted by the panel as factors to consider when responding to computer crimes. The panelists recorded the most references to lack of knowledge, management support, and responsibilities. The statements were coded and themed for the Round 2 judgments.

Improving the Disaster Recovery response. The third and fourth seed questions included judgments on the response aspects of recovery from computer crimes. Ninety-four statements were submitted by the participants for their viewpoints on responding to and improving the response to computer crimes. Determining the root cause of the attack, disaster recovery alignment, recovering data, and updating the playbook were the most frequently referenced.

Disaster Recovery planning for computer crimes. The fifth and sixth questions collected judgments on the planning aspects that an organization should consider when the disaster recovery team is building the playbooks. Eighty-one statements were

collected from the participants on disaster recovery planning for computer crimes and the way an organization may improve the process. Avoidance of a single solution, specific planning for computer crimes, lessons learned, and the need for information security were the highest themes analyzed for this category.

Integrating with cybersecurity. The seventh, ninth, and 10th questions focused on the integration of cybersecurity processes with disaster recovery. One hundred and five statements were submitted by the participants on the alignment of cybersecurity frameworks alignment with disaster recovery, use of cybersecurity processes, and the advantages of implementation of cyber security controls. Risk management, lessons learned, cybersecurity training, and cybersecurity frameworks recorded the highest count of themes in this category. Several participants cited information security frameworks that could be aligned with disaster recovery and pointed to the need for alignment of cyber with disaster recovery.

Necessary skillsets for responders. The eighth question focused on any skillsets that could assist disaster recovery responders or planners for the recovery of computer crimes. Forty-four statements were submitted by the panel for their viewpoints on the job skills needing to be recruited for a successful recovery from computer crimes. A risk mindset, cyber security expertise, and certifications were the highest coded responses. Several experts expressed logical thinking and cyber security knowledge as a requirement to be found in the disaster recovery team personnel. A focus on the understanding of technology in the business was also highlighted as a skill needed to understand the impact of the computer crimes.

Delphi Round 2

The second round of the Delphi presented 110 themed statements analyzed from the first round of data collection. The themed questions were broken up by the 10 seed questions so that the participants could understand the root of the statement. Of the 110 statements sent to the participants, the consensus was found on 79 (72%) of the statements.

Significant factors that come from computer crimes. For Questions 1 and 2 focusing on computer crimes factors, 21 themed statements were presented for judgment. Of the 21 statements, 16 (76%) of the statements came to a consensus agreement. The panel highlighted the need for understanding interdependencies, adequate planning for computer crimes, needed availability of critical infrastructure, management support via funding, testing a response for computer crimes, and critical data must be protected from tampering.

Improving the disaster recovery response. Questions 3 and 4, concentrating on the response aspects of recovery, provided 27 themed statements. Of the 27 statements, 19 (70%) of the statements reached a consensus agreement. Of the statements that reached a consensus, having a clear scope of the response, quantifying the damage, having external resources to assist in the recovery, needing an alignment with business goals, revising the disaster recovery playbook for new threats, and testing for computer crimes were viewed as steps the organization can take to improve the response.

Disaster recovery planning for computer crimes. The fifth and sixth questions focused on the planning aspects of the recovery and provided 22 statements for judgment.

Of the presented statements, 17 (77%) of the statements meet consensus. Specific planning for computer crimes, understanding the cyber risk, the need for awareness programs, considering the current state of technology in the organization, lesson learned activities, adequate funding, and the need for information technology disaster recovery to operate in the same business silo as information security were each identified by the panel.

Integrating with cybersecurity. The seventh, ninth, and 10th questions focused on the integration of cybersecurity processes with disaster recovery. Thirty-two statements were presented to the participants for judgment, and 21 (53%) found consensus. Alignment with a cybersecurity framework, resilience controls, the need for enterprise risk management, and lessons learned was identified as the major themes. Al Hamed and Alenezi (2016) highlighted the importance of a strong connection between information security and disaster recovery and the need for organizational improvement in business impact analysis.

Three participants provided additional feedback on the potential cost of implementing cybersecurity into disaster recovery processes. The participants felt there could be a disadvantage in that adding the cybersecurity components to the existing process would require more time, technology, and expertise. This disadvantage could be coming from a position of a leader that is already struggling to get funding for a DR program and may find it difficult to expand the scope of computer crimes.

Necessary skillsets for responders. The eighth question focused on skill sets to assist disaster recovery responders or planners for the recovery of computer crimes.

Thirteen statements were presented to the participants for judgments. Six (46%) of the proposed statements found consensus for the skillsets needed to recover from computer crimes. Business-focused understanding, risk analysis, prevention, and cybersecurity expertise were identified as necessary for the recovery effort. Toigo (1989) and Tucker (2014) claimed risk assessment was a commonly misunderstood aspect of disaster recovery planning, and without the proper cybersecurity knowledge, the risk assessment may not contain the necessary understanding to identify the risks.

Delphi Round 3

The Round 3 questionnaire carried consensus statements over from the second round of agreements. Five questions from the first category and two questions from the third category were filtered from this round because the questions did not apply to the application of control or process of an organization. Seventy-five consensus statements were presented to the participants for judgment of a 5-point importance Likert scale to the organization's disaster recovery program.

Significant factors that come from computer crimes. Fourteen statements were presented with five reaching the threshold for consensus. The participants highlighted the need for management support, a clear understanding of technology interdependencies, and the responders understand computer crimes attacks. These findings indicated that responders must have a good grasp of the environment and at the same time an understanding how computer crimes can affect that environment. This highlighted the need for cybersecurity knowledge on the planning and response side of the disaster recovery program. Statements not reaching a consensus concentrated on the availability

of critical IT services, testing recovery processes, and lessons learned. This research seems to indicate lessons learned, and testing is needed in a cyber response, but the participants placed a higher priority on implementing cybersecurity knowledge over these existing activities that may just need minor upgrading to meet the need.

Improving the disaster recovery response. Nineteen statements were presented for the panel to provide a judgment on the importance of deployment in an organization. Seven statements met the criteria for consensus. The panel highlighted the need for the technology department to alignment with the business, a need for a clear understanding of computer threats, a focus on responder's knowledge, revising playbooks for new threats, and embedding cybersecurity into disaster recovery programs. An analysis of the findings resulted in the training of the disaster recovery responders and revision of the DR playbook to respond to the emerging threat of computer crimes. The theme statements that did not reach consensus focused on data backup techniques, a focus on quantifying the damage, third-party resources, traditional disaster recovery playbooks, communication, and cause analysis

Disaster recovery planning for computer crimes. Fifteen statements were presented to the panel on planning for computer crimes. Eight statements reached a consensus of importance. The participants highlighted the importance of a diversified response to computer crimes interruptions, adequate funding, attention to risks, attention paid to understanding the current state of systems, and resiliency of technology. The concepts that did not reach a threshold of consensus focused on the computer crimes problem being an IT problem, quick decision making without understanding the problem,

and placing a low value on quality management. This research indicates knowledge of cybersecurity will improve the risk management process and deployed controls to resume the organization. Resiliency was also scored here with the intent of the participants pointing to having data available following a computer crimes attack. Feedback was provided by a participant that this might be a difficult problem to solve. Traditional redundancy of data with synchronization or a backup medium has not always mitigated computer crimes such as ransomware (Bhattacharya & Kumar, 2017).

Integrating with cybersecurity. Twenty-one statements were sent to the panel for ranking that focused on cybersecurity integration with disaster recovery. Of the 21 statements, 10 (47%) achieved consensus. The participants indicated an information security framework should integrate with disaster recovery and cybersecurity teams should be aligned, disaster recovery teams should receive infosec training, and enterprise risk management being important for organizations to consider. The themes that did not reach a consensus of importance threshold included building advanced DR playbooks, chief security officer responsibilities in disaster recovery planning, baselining security configurations, penetration testing activities, risk management identification of critical systems, and risk management. This research indicated the strong need for the integration of cybersecurity with disaster recovery.

Necessary skillsets for responders. Six themed statements were presented for ranking the skills that disaster recovery team members should exhibit. Of the six statements from the second round, five statements reached a consensus on importance. Understanding the technology environment, business-focused understanding of the

organization, risk analysis, and basic information security skills was highlighted as desirable skills for being better equipped to respond to computer crimes. This finding correlates with many sections of this research regarding the training of cybersecurity skillsets to disaster recovery planners and responders.

Limitations of the Study

This study had potential limitations. Although the Delphi participants were provided qualitative questions about information technology disaster recovery, the question attributes were limited to computer crimes by the researcher. The disaster recovery body of knowledge is far reaching beyond information technology, and this research was specifically limited to the disaster recovery of computer crimes caused interruption. This research tried to understand how organizations might better respond to computer crimes interruptions and if information technology disaster recovery alignment with cybersecurity might improve the response. The research study findings did not include the motive behind the cyber attackers, describe the type of individuals or groups that comprise cyber hackers, or developed a method for preventing the attacks. The study did not research the building of an disaster recovery team or how the team should be funded.

The findings from this research may apply to organizations that currently follow disaster recovery activities. The study would not apply to organizations that have a limited technology footprint or do not find it necessary to have processes to recover technology. The study was not focused on any organization, and the finding might have different results depending on the purpose of the organization.

This research was limited to the disaster recovery and cybersecurity participants understanding of information technology disaster recovery and cybersecurity incident response. A potential limitation might come from the recruiting of a panel that would fail to include the viewpoints of recognized experts. To avoid including participants that would not provide valuable data, I held to a strict guideline. Published disaster recovery researchers, disaster recovery practitioners, and cybersecurity expertise were confirmed from interviews and LinkedIn profiles. The snowball sampling technique provided additional experts who were also queried for applicable expertise requirements that had been set. The responses to this research may differ from experts that do not agree with the need to integrate cybersecurity knowledge into disaster recovery.

Recommendations

The following recommendations were derived from this qualitative Delphi study. The recommendations are intended to offer an improved understanding of disaster recovery teams, social change, and contribute to the information technology disaster recovery body of knowledge. This study was not confined to any organizational type or geographic locations. The researcher focused on five categories relating to significant factors, improving response, planning, integration, and skillsets. Researchers may wish to conduct similar Delphi research on different organizations such as corporate 500, nonprofits, or government agencies with a similar focus on these major categories.

A future Delphi on desirable skillsets of disaster recovery responders might yield invaluable data on the needs of an increasingly complicated cyber risk. Attacks have changed overtime and one section of industry may not see the same attacks as another.

Due to different technologies, risks to cyber-attacks, computer crimes, and available resources, a Delphi that focuses on one organizational sector, for example, finance, would represent a viable option for research on the effects of computer crimes.

For future studies, researchers might change the eligibility of the study to include potential participants from a software development background, cloud service architecture, and c-level executives to seek new views on industry-specific experience. The results of these future Delphi might provide new insight for comparison with this study on new frameworks, responses, integrations or changes to the disaster recovery team composition. There are a variety of potential avenues for Delphi studies that might provide further insight into disaster recovery as it pertains to cyber threats.

Five panelists of this study indicated a lack of understanding of technology interdependencies and how proper triage of computer crimes may be significant factors in a recovery activity. Future qualitative studies could expand on the five panelists judgement of disaster recovery responders lacking technical understanding for the response. This study would center on successful triage techniques for containment and remediation of computer crimes.

Six panelists highlighted the need for data resiliency. Another area of research might seek to understand how vital it is to have data resiliency when an entity experiences a computer crimes interruption and if the resiliency deployed is enough to overcome the intentional attack. Disaster recovery scholars may wish to understand how important it is to have defined disaster response roles when encountering a computer crimes interruption. Existing DR plans may not have clear roles when the interruption is

not conventional, and the team must leave the planner recovery procedures. Understanding how roles with a veteran cyber skillset can improve the disaster recovery process would be valuable to the body of knowledge.

Ninety three percent (93%) of this study's panel highlighted the need for enterprise risk management as it pertains to cyber risks. Guidry et al. (2015) and Ferdinand (2015) claimed that the lack of organizational understanding of how a disaster recovery program might modify measures to account for computer crimes interruptions. Future researchers may find value in qualitative studies looking at how organizations need to alter their disaster recovery planning to specifically accommodate technology black swans such as the Petya crypto locker or the DyN DDoS attack (Shuler & Smith, 2017).

An analysis of the data indicated there would be an advantage with developing cybersecurity expertise and when aligning disaster recovery frameworks with cybersecurity frameworks. Comments from the experts pointed to the need for greater visibility, monitoring, and incident response from cyber-attacks. The study did not identify existing or applicable frameworks that would meet this need. Future research should center on how to align components of a common cybersecurity framework to add value to disaster recovery framework such as the ISO 22301, ISO 17999, NIST 800-34 or BS25999 ((Bird, 2015; Brown, 2016). The cybersecurity frameworks 800-184 and CAG 20 are described as frameworks for improving policies and plans for recovering evolved threats (Montesino & Fenz, 2011). Future studies might produce a hybrid control

framework that would better position an organization to defend, identify and recover from cyber threats.

An analysis of the data indicated the participants placed importance on cybersecurity skills for responders. As expressed by the experts, there might exist a considerable gap between traditional disaster recovery skillsets and the cyber skills needed for responding to computer crimes. A potential Delphi would seek to understand the desirable skillsets of disaster recovery responders that might yield invaluable data on the increasingly complicated cyber risk response to computer crimes (McCreight & Leece, 2016). Researchers may also conduct qualitative studies for the value of penetration testing experience, encryption solutions, and security event monitoring.

Implications

The experience of disaster recovery and cybersecurity experts represents a section of information which might facilitate a change in the response and recovery from technology disasters. Technology disasters are a risk that is increasingly affecting organizational survivability. Keeping an organization immediately viable following a technology interruption will assist in the survivability or profitability of the organization. Prepared organizations are better positioned to keep employees on the payroll and remaining in the community instead of invoking evacuation plans and crisis communications (Kuo & Means, 2011). By improving the disaster recovery response to an event, a community that is relying on vital services from the affected entity will experience a reduced interruption as opposed to a prolonged disturbance. Hospitals, emergency response, local law enforcement, and transportation are examples of vital

services that can leverage an improved information technology disaster recovery response to service the local community.

Recommendations for Information Technology Disaster Recovery Teams

My research reduces a gap in the understanding of information technology disaster recovery by focusing specifically on the consensus of experts in the field of cybersecurity and information technology disaster recovery. Organizations across the globe are experiencing interruptions due to unexpected computer crimes, and researchers are predicting this trend to increase (Page, Kaur, & Waters, 2017; Liu, Li, Shuai, & Wen, 2017). Traditional disaster recovery has a significant amount of historical data to aid in the planning and resuming of a system from fire, flood, and loss of power (Ferdinand, 2015); however, newer risks to the organization must now be realized from the threat of computer crimes. Key decision makers must integrate cybersecurity efforts with disaster recovery planning and procedures. Training information technology disaster recovery planners and responders in general or specific cybersecurity techniques can improve the planning phase and conceptual awareness during a computer crimes interruption. A cybersecurity awareness can provide an insight into a risk management activity that may not have been considered otherwise (Alexander, 2015; Grigonis, 2002; Iqbal, Widyawan, & Mustika, 2016; Lam, 2002; Rittinghouse & Ransome, 2011). Organizations should explore ways to integrate more cybersecurity into the disaster recovery lifecycle to improve the ability to quickly and efficiently recover from business interruptions.

Conclusions

This qualitative Delphi research study included the viewpoints and knowledge of disaster recovery researchers, disaster recovery responders, and cybersecurity experts as a tool to understand how to improve the effects of computer crimes on disaster recovery programs. Although disaster recovery was originally founded from the principles of emergency management in responding to natural disasters (Alexander, 2015), the research participants highlighted the need to advance the disaster recovery process to include cybersecurity threats. The research pointed to the need for organizations to implement cybersecurity knowledge in the disaster recovery process for planning, risk management, lessons learned, and awareness improvement of the responders. The emerging threats from cyber-attacks pose a serious risk to organizations (Vaidya, 2015) and a building of understanding in cybersecurity should improve the disaster recovery response from a computer crimes interruption.

This research also explored the use of a cybersecurity framework integration with disaster recovery processes. The monitoring, defensive controls, and incident response procedures found in popular cybersecurity frameworks can easily augment existing information technology disaster recovery planning and response procedures. The research participants highlighted advantages in several sections of this research in combining the two concepts where it was applicable. Therefore, based on the results of this study, organizations must explore ways to build knowledge in their disaster recovery teams of cybersecurity techniques and should improve their disaster recovery programs through an integration with a cybersecurity framework.

References

Aasgaard, D., Cheung, P., Hulbert, B., & Simpson, M. (1978). An evaluation of data processing 'Machine Room' loss and selected recovery strategies. *Management Information Systems Research Center Working Papers*. Minneapolis, MN: University of Minnesota.

Alexander, D. E. (2015). *Disaster and emergency planning for preparedness, response, and recovery.* Oxford, UK: Oxford University Press.

Alhazmi, O. H., & Malaiya, Y. K. (2013). Evaluating disaster recovery plans using the cloud. In Reliability and Maintainability Symposium (RAMS), 2013 Proceedings-Annual (1-6). *IEEE*. doi:10.1109/RAMS.2013.6517700

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82,* 69-82. Retrieved from https://www.journals.elsevier.com/international-journal-of-human-computer-studies/

Al Hamed, T., & Alenezi, M. (2016). Business continuity management & disaster recovery capabilities in Saudi Arabia ICT Businesses. *International Journal of Hybrid Information Technology, 9*(11), 99-126. doi:10.14257/ijhit.2016.9.11.10

Allen, J., Crabb, G., Curtis, P. D., Fitzpatrick, B., Mehravari, N., & Tobar, D. (2015). *Structuring the chief information security officer organization*. Pittsburgh, PA: Carnegie Mellon University. Retrieved from http://www.sei.cmu.edu

Allen, J. H., & Sledge, C. A. (2002). Information Survivability: Required Shifts in Perspective. *CrossTalk*: *The Journal of Defense Software Engineering.* Retrieved from http://www.crosstalkonline.org/

Allianz (2015). Allianz Risk Barometer top business risks. Retrieved from http://www.agcs.allianz.com/

Allman, K. (2016). In focus: How to beat hackers without paying a ransom. *Law Society of NSW Journal, 28*(26). Retrieved from https://www.lawsociety.com.au/resources/journal/index.htm

Aspan, M. & Kelvin, S. (2011, June 16). Citi says 360,000 accounts hacked in May cyber attack. *Reuters*. Retrieved from http://www.reuters.com/article

Axelrod, C. (2016). Actionable security intelligence from big, midsize and small data. *ISACA Journal*. Retrieved from https://www.isaca.org/Journal/archives/2016/Volume-1/Pages/actionable-security-intelligence-from-big-midsize-and-small-data.aspx

Babbie, E. (2007). *The practice of social research* (11th ed.). Belmont, CA: Thomson Wadsworth.

Bajgoric, N. (2014). Business continuity management: a systemic framework for implementation. *Kybernetes*, 156-177. doi:10.1108/K-11-2013-0252

Barclay, C. (2014, June). Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM 2). In ITU Kaleidoscope Academic Conference: Living in a converged world-Impossible without

standards?, Proceedings of the 2014 (275-282). *IEEE*. doi:10.1109/Kaleidoscope.2014.6858466

Barber, R. (2001). Hackers profiled—who are they and what are their motivations?. *Computer Fraud & Security, 2001*(2), 14-17. Retrieved from https://www.journals.elsevier.com/computer-fraud-and-security

Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G., & Scarfone, K. (2016). Cybersecurity event recovery. *NIST Special Publication*, 800-184. doi:10.6028/NIST.SP.800-184

Benston, G. J. (1973). Required disclosure and the stock market: An evaluation of the Securities Exchange Act of 1934. *The American Economic Review, 63*(1), 132-155. Retrieved from https://www.jstor.org/journal/amereconrevi?decade=1970

Berke, P. R., Kartez, J., & Wenger, D. (1993). Recovery after disaster: achieving sustainable development, mitigation and equity. *Disasters, 17*(2), 93-109. Retrieved from http://onlinelibrary.wiley.com/journal/10.1111/(ISSN)1467-7717

Bernal-Torres, C., Thoene, U., & Giraldo, J. (2016). Sources, availability and uses of knowledge in enterprises in Bogotá, Colombia. *Intangible Capital, 12*(2), 733-754. doi:10.3926/ic.626

Bhattacharya, S., & Kumar, C. R. S. (2017, February). Ransomware: The CryptoVirus subverting cloud security. In Algorithms, Methodology, Models and Applications in Emerging Technologies. *IEEE*. Retrieved from http://ieeexplore.ieee.org/

Bhoola, V., Hiremath, S. B., & Mallik, D. (2014). An assessment of risk response strategies practiced in software projects. *Australasian Journal of Information Systems, 18*(3), 161-191. Retrieved from http://journal.acs.org.au/index.php/ajis

Bidgoli, H. (2016). Integrating real life cases into a security system: Seven checklists for managers. *American Journal of Management, 16*(4), 9. Retrieved from http://www.na-businesspress.com/ajmopen.html

Bird, L. (2015). Editorial. *Journal of Business Continuity & Emergency Planning*. 288-289. Retrieved from http://www.henrystewartpublications.com/jbcep

Bishoff, L., Breeding, M., Clareson, T., Conn, D., O'Shea, D. & Soderdahl, P. (2015). *Technology disaster response and recovery planning.* Chicago, IL: The American Library Association.

Bobko, J. P., & Kamin, R. (2015). Changing the paradigm of emergency response: The need for first-care providers. *Journal of Business Continuity & Emergency Planning, 9(*1), 18-24. Retrieved from http://www.henrystewartpublications.com/jbcep

Bortree, D. S., & Seltzer, T. (2009). Dialogic strategies and outcomes: An analysis of environmental advocacy groups' Facebook profiles. *Public Relations Review*, 35(3), 37-319. Retrieved from https://www.journals.elsevier.com/public-relations-review/

Bronk, C., & Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. *Survival, 55*(2), 81-96. doi:10.1080/00396338.2013.784468

Brooks, C. (2011, September 6). 10 years later, small businesses tell tales of 9/11 recovery. Business News Daily. Retrieved from http://www.businessnewsdaily.com/

Brown, H. S. (2016). After the data breach: Managing the crisis and mitigating the impact. *Journal of Business Continuity & Emergency Planning, 9*(4), 317-328. Retrieved from http://www.henrystewartpublications.com/jbcep

Business Continuity Institute (2013). Horizon scan 2013: Survey report. Retrieved from http://www.thebci.org/index.php/download-the-2013-horizon-scan-report

Butler, J. (1998). *Contingency planning and disaster recovery: Protecting your organization's resources.* Charleston, SC: Computer Technology Research Corporation.

Cabaj, K., & Mazurczyk, W. (2016). Using software-defined networking for ransomware mitigation: The case of CryptoWall. *IEEE Network, 30*(6), 14-20. Retrieved from http://ieeexplore.ieee.org

Cao, Y., Yegneswaran, V., Possas, P., Chen, Y. (2012) Pathcutter: Severing the self-propagation path of XSS JavaScript worms in social web networks. Proceedings of the 19th network and distributed system security symposium (NDSS). Retrieved from http://www.internetsociety.org/events/ndss-symposium-2012

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009). Challenges for securing cyber physical systems. In Workshop on future directions in cyber-physical systems security (Vol. 5). Retrieved from https://cps-vo.org/node/403/#main-content-area

Cefaratti, M., Hui, L., & Wallace, L. (2011). The information security control environment. *Internal Auditor, 68*(2), 55-59. Retrieved from https://na.theiia.org/periodicals/Pages/Internal-Auditor-Magazine.aspx

Cervone, H. F., & Cervone, H. F. (2016). Information doesn't always want to be free: An overview of regulations affecting information security. *Digital Library Perspectives, 32*(2), 68-72. Retrieved from http://www.emeraldinsight.com/2059-5816.htm

Chand, A. M., & Loosemore, M. (2016). Hospital disaster management's understanding of built environment impacts on healthcare services during extreme weather events. Engineering *Construction & Architectural Management*, *23*(3), 385-402. doi:10.1108/ECAM-05-2015-0082

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Thousand Oaks, CA: Sage.

CIS (2017). CIS controls. Center for Internet Security. Retrieved from https://www.cisecurity.org/controls/

Clark, K., Dawkins, J., & Hale, J. (2005, June). Security risk metrics: Fusing enterprise objectives and vulnerabilities. In Information Assurance Workshop. Proceedings from the Sixth Annual IEEE SMC, 388-393. *IEEE*. Retrieved from http://www.ieee.org

Clibbens, N., Walters, S., & Baird, W. (2012). Delphi research: Issues raised by a pilot study. *Nurse Researcher, 19*, 37-44. Retrieved from http://journals.rcni.com/journal/nr

CMMI (2007). Assess your organization's capability. Carnegie Mellon University. Retrieved from http://cmmiinstitute.com/

Cook, J. (2015). A six-stage business continuity and disaster recovery planning cycle. *SAM Advanced Management Journal, 80*(3), 23. Retrieved from http://samnational.org/publications/sam-advanced-management-journal/

Cooks, T. (2015). Factors affecting emergency manager, first responder, and citizen disaster preparedness (Unpublished doctoral dissertation). Walden University. Minneapolis, Minnesota.

Cross, K. (2000). Application of the NSA infosec assessment methodology. *SANS Institute InfoSec Reading Room*. Retrieved from https://www.sans.org/reading-room/

Cutter, S. L., Emrich, C. T., Mitchell, J. T., Piegorsch, W. W., Smith, M. M., Weber, L., Tierney, K., Roberts, S. & Sorell, T. (2016). Designing crisis management systems for the twenty-first-century. *Public Administration, 94*(2), 569-575. doi:10.1111/padm.12260

Cybulski, G. T. (2016). Business continuity management: Return on investment. Aon Global Risk Consulting. Retrieved from http://www.aon.com

Dahlberg, R., & Guay, F. (2015). Creating resilient SMEs: is business continuity management the answer?. *WIT Transactions on The Built Environment, 168*, 975-984. Retrieved from https://www.witpress.com/elibrary/wit-transactions-on-the-built-environment

Dalkey, N. C., & Helmer, O. (1951). The Use of Experts for the Estimation of Bombing Requirements: A Project Delphi Experiment. RAND. Retrieved from https://www.rand.org/

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207. doi:10.1016/j.cose.2009.09.002

David, A. (1969, November 27). Town topics. Princeton Newspaper, 24(39). Retrieved from http://www.towntopics.com

David, C. C., Ong, J. C., & Legara, E. F. T. (2016). Tweeting supertyphoon Haiyan: Evolving functions of Twitter during and after a disaster event. *PloS one, 11*(3). doi:10.1371/journal.pone.0150190

Davis, M., Strell, E., & Wallace, J. (2005). Environmental protection after a disaster: A right or a privilege. *Nat. Resources & Env't, 20*, 15. Retrieved from https://www.americanbar.org/publications/natural_resources_environment_home/natural_resources_environment_archive.html

Day, J., & Bobeva, M. (2005). A generic toolkit for the successful management of Delphi studies. *The Electronic Journal of Business Research Methodology, 3*(2), 103-116. Retrieved from http://www.ejbrm.com/main.html

Department of Energy (n.d.). Cybersecurity capability maturity model. Office of Electricity Delivery and Energy Reliability. Retrieved from https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program

Dietel, A. (2015). You get what you pay for: The NFIP is underwater and climate change adaptation is essential to reach dry land. *Florida A & M University Law Review, 10*(2), 8. Retrieved from http://commons.law.famu.edu

Dines, R. (2012). It's time to add hacking into your disaster recovery plans as a potential risk for downtime. Retrieved from http://blogs.forrester.com/rachel_dines

Donohoe, H. M., & Needham, R. D. (2009). Moving best practice forward: Delphi characteristics, advantages, potential problems, and solutions. *International Journal of Tourism Research, 11*(5), 415-437. doi:10.1002/jtr.709

Ee, H. (2014). Business Continuity 2014: From traditional to integrated Business Continuity Management. *Journal of Business Continuity & Emergency Planning*, 102-105. Retrieved from http://www.henrystewartpublications.com/jbcep

Elliot, D., Swartz, E. & Herbane, B. (2010). *Business continuity management: A crisis management approach*. New York, NY: Routledge.

Ericsson, G. N. (2007). Toward a framework for managing information security for an electric power utility—CIGRÉ experiences. *IEEE transactions on power delivery, 22*(3), 1461-1469. Retrieved from http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=61

Fallara, P. (2003). Disaster recovery planning. *IEEE potentials, 23*(5), 42-44. Retrieved from http://ieeexplore.ieee.org/

Fallucchi, F., Tarquini, M., & De Luca, E. W. (2016). Knowledge management for the support of logistics during humanitarian assistance and disaster relief (HADR). In *International Conference on Information Systems for Crisis Response and*

Management in Mediterranean Countries (226-233). Springer International Publishing. doi:10.1007/978-3-319-47093-1_19

Federal Reserve (2016). Compliance guide to small entities. Board of Governors of the Federal Reserve System. Retrieved from https://www.federalreserve.gov/bankinforeg

FEMA (2017). About the agency. Federal Emergency Management Agency. Retrieved from https://www.fema.gov/

Ferdinand, J. (2015). Building organisational cyber resilience: A strategic knowledge-based view of cyber security management. *Journal of Business Continuity & Emergency Planning, 9*(2), 185-195. Retrieved from http://www.henrystewartpublications.com/jbcep

Ford, R. (1999). No surprises in Melissa land. *Computers & Security, 18*(4), 300. Retrieved from https://www.journals.elsevier.com/computers-and-security/

Fowles, J. (1978). *Handbook of futures research*. Westport, CT: Greenwood Press.

Frankfort-Nachmias, C., & Leon-Guerrero, A. (2015). *Social statistics for a diverse society (7th ed.).* Thousand Oaks, CA: Sage.

Gagneja, A. S., & Gagneja, K. K. (2015, December). Incident response through behavioral science: An industrial approach. In Computational Science and Computational Intelligence (CSCI), 2015 International Conference on (36-41). *IEEE*. Retrieved from http://americancse.org/events/csci2016/Symposiums

Garner, S. A., Hutchison, P. D., & Conover, T. L. (2016). The effect of SEC disclosure regulation regarding audit committees' financial experts on foreign private issuers

cross-listed on U.S. Securities Exchanges. *Journal of International Accounting Research, 15*(2), 7-26. doi:10.2308/jiar-51375

Giannariu, L., & Zervas, E. (2014). Using Delphi technique to build consensus in practice. *Int. Journal of Business Science and Applied Management 9*(2). Retrieved from http://business-and-Management.org

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *TQM Journal, 23*(4), 367-376. doi:10.1108/17542731111139455

Goodacre, S., Irving, A., Wilson, R., Beever, D., & Challen, K. (2015). The pandemic influenza triage in the emergency department (PAINTED) pilot cohort study. *Health Technology Assessment, 19*(3). Retrieved from https://www.journalslibrary.nihr.ac.uk/HTA/#/

Goodman, K. W., Adams, S., Berner, E. S., Embi, P. J., Hsiung, R., Hurdle, J. & Winkelstein, P. (2012). AMIA's code of professional and ethical conduct. *Journal of the American Medical Informatics Association*, *20*(1), 141-143. doi:10.1136/amiajnl-2012-001035

Grant, D. (2016). Business analysis techniques in business reengineering. *Business Process Management Journal*, *22*(1), 75-88. Retrieved from http://www.emeraldinsight.com/journal/bpmj

Greene, T. (2006). SSL VPNs as a disaster recovery technology; * SSL VPNs get government backing. *Network World*. Retrieved from http://www.worldcat.org/title/network-world/oclc/13350973

Grigonis, R. (2002). *Disaster survival guide for business communications networks: Strategies for planning, response and recovery in data and telecom systems.* Gilory, CA: Cmp Books.

Guidry, P. E., Vaughn, D., Anderson, R. P., & Flores, J. (2015). Business continuity and disaster management: Mitigating the socioeconomic impacts of facility downtime after a disaster. *IEEE Industry Applications Magazine, 21*(5), 68-77. doi:10.1109/MIAS.2014.2345796

Gupta, S., & Gupta, B. B. (2017). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. *International Journal of System Assurance Engineering and Management, 8*(1), 512-530. Retrieved from http://www.springer.com/engineering/industrial+management/journal/13198

Gupta, M., Chaturvedi, A. R., & Mehta, S. R. (2011). Economic analysis of tradeoffs between security and disaster recovery. *CAIS, 28*, 1. Retrieved from http://aisel.aisnet.org/cais/

Haimes, Y., Kaplan, S., and Lambert, J. (2002). Risk filtering, ranking, and management framework using hierarchical holographic modeling. *Risk Analysis 22*(2), 383–397. Retrieved from http://onlinelibrary.wiley.com/journal/10.1111/(ISSN)1539-6924

Hall, D. (1989). Turning up the heat on disaster plans. *ABA Banking Journal, 81*(8), 35. Retrieved from http://bankingjournal.aba.com/

Harp, D. & Gregory-Brown, B. (2016). SANS 2016 State of ICS Security Survey. SANS Institute. Retrieved from http://www.sans.org

Heng, T. B., Hooi, S. C., Liang, Y. Y., Othma, A., & San, O. T. (2012). Telecommuting for business continuity in a non-profit environment. *Asian Social Science, 8*(12), 226. Retrieved from http://www.ccsenet.org/journal/index.php/ass

Henning, R. R. (1999). Security service level agreements: Quantifiable security for the enterprise?. In Proceedings of the 1999 workshop on New security paradigms (54-60). *ACM*. Retrieved from http://jacm.acm.org/

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, 25. Retrieved from http://www.tandfonline.com/loi/fbsh20

Hiatt, C. J. (Ed.). (2000). *A primer for disaster recovery planning in an IT environment*. Hersey, PA: Idea Group Publishing.

Hiller, M., Bone, E. A., & Timmins, M. L. (2015). Healthcare system resiliency: The case for taking disaster plans further – Part 2. *Journal of Business Continuity & Emergency Planning, 8*(4), 356-375. Retrieved from http://www.henrystewartpublications.com/jbcep

Holling, C. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics, 4(*1), 1-23. Retrieved from http://www.annualreviews.org/journal/ecolsys

Houston, B., Hawthorne, J., Perreault, M., Park, E., Goldstein Hode, M., Halliwell, M. R., Turner McGowen, S., Davis, R., Vaid, S., McElderry, J., & Griffith, S. A. (2015). Social media and disasters: A functional framework for social media use

in disaster planning, response, and research. *Disasters, 39*(1), 1-22. doi:10.1111/disa.12092

Howell, D. C. (2016). *Fundamental statistics for the behavioral sciences*. Toronto, ON: Nelson Education.

Hsu, C., & Sandford, B. A. (2007). The Delphi technique: Making sense of consensus. *Practical Assessment, Research & Evaluation, 12*(10), 1-8. Retrieved from http://pareonline.net/

IBM Security (2016). Reviewing a year if serious data breaches, major attacks and new vulnerabilities. 2016 Cyber Security Intelligence Index. Retrieved from http://www-03.ibm.com/security/data-breach/cyber-security-index.html

Ignatius, A. (2015). They burned the house down. *Harvard Business Review*, 7-8, 106. Retrieved from https://hbr.org/

Iguer, H., Medromi, H., Sayouti, A., & Tallal, S. (2016). Including EAS-SGR IT Risk framework in an IT GRC global framework. *In Advances in Ubiquitous Networking*. Retrieved from http://www.springer.com/us/

Inkinen, H. (2016). Review of empirical research on knowledge management practices and firm performance. *Journal of Knowledge Management, 20*(2), 230-257. doi:10.1108/JKM-09-2015-0336

Iqbal, A., Widyawan, & Mustika, I. W. (2016, June). COBIT 5 domain delivery, service and support mapping for business continuity plan. *AIP Conference Proceedings*, *1746*(1). doi:10.1063/1.4953970

ISACA (2016). State of cybersecurity: Implications for 2016. ISACA and RSA conference survey. Retrieved from https://www.isaca.org/cyber

Jain, T. N., Ragazzoni, L., Stryhn, H., Stratton, S. J., & Della Corte, F. (2015). Comparison of the sacco triage method versus START triage using a virtual reality scenario in advance care paramedic students. *CJEM*, 1-5. Retrieved from https://www.cambridge.org/core/journals/canadian-journal-of-emergency-medicine

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993. doi:10.1016/j.jcss.2014.02.005

Jedynak, P. (2013). Business continuity management: The perspective of management science. *International Journal of Contemporary Management*, 85-96. Retrieved from http://journals.indexcopernicus.com

Johansson, E., & Johnson, P. (2005). Assessment of enterprise information security-an architecture theory diagram definition. Proc. of CSER, 5. Retrieved from https://cser-consortium.org/publications

Jones, R. (2007). Survival of the fittest: Disaster recovery design for the data center. *Burton Group, 1*(45). Retrieved from http://www.burtongroup.com

Kadar, M. (2015). Development and implementation of a business continuity management risk index. *Journal of Business Continuity & Emergency Planning*. 238-251. Retrieved from http://www.henrystewartpublications.com/jbcep

Kamali, B., Bish, D., & Glick, R. (2017). Optimal service order for mass-casualty incident response. *European Journal of Operational Research, 261*(1), 355-367. doi:10.1016/j.ejor.2017.01.047

Kanapathy, K., & Khan, K. I. (2012). Assessing the relationship between ITIL implementation progress and firm size: evidence from Malaysia. *International Journal of Business and Management, 7*(2), 194. doi:10.5539/ijbm.v7n2p194

Kandel, J. & Kovacik, R. (February 12, 2016.) Hollywood hospital 'Victim of Cyber Attack'. News NBC4; Retrieved from http://www.nbclosangeles.com/news/local/Hollywood-Hospital-Victim-of-Cyber-Attack-368574071.html

Kantamaneni, K., Alrashed, I., & Phillips, M. (2015). Cost vs. safety: A novel design for tornado proof homes. *HBRC Journal*. doi:10.1016/j.hbrcj.2015.05.004

Kapucu, N., & Hu, Q. (2016). Understanding multiplexity of collaborative emergency management networks. *The American Review of Public Administration, 46*(4), 399-417. doi:10.1177/0275074014555645

Karter, M. J. (2003). Fire loss in the United States during 2002. National Fire Protection Association. Fire Analysis and Research Division. Retrieved from http://www.nfpa.org/news-and-research

Kellman, B. (2016). Disaster mitigation under law-an international legal challenge. International Seminar on Global Environment and Disaster Management: Law and Society. Retrieved from http://hdl.handle.net/123456789/15499

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015, July). Cutting the gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (3-24). Springer International Publishing. Retrieved from http://www.wikicfp.com/cfp/home

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091-2121. Retrieved from http://ieeexplore.ieee.org

Kirkpatrick, K. (2015). Cyber policies on the rise. *Communications of the ACM*, 58(10), 21-23. doi:10.1145/2811290

Koenig, T. A., Bruce, J. L., O'Connor, J., McGee, B. D., Holmes Jr, R. R., Hollins, R., Forbes, B., Kohn, M., Schellekens, M., Martin, Z., & Peppler, M. C. (2016). Identifying and preserving high-water mark data (No. 3-A24). U.S. Geological Survey. doi:10.3133/tm3a24

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296. doi:10.1016/j.cose.2006.02.008

Kuo, S. S., & Means, B. (2011). Corporate social responsibility after disaster. *Washington University Law Review 89*(973). Retrieved from http://heinonline.org/

Kweit, M. G., & Kweit, R. W. (2004). Citizen participation and citizen evaluation in disaster recovery. *The American Review of Public Administration, 34*(4), 354-373. Retrieved from http://journals.sagepub.com/home/arp

Lachlan, K. A., Spence, P. R., Lin, X., Najarian, K., & Del Greco, M. (2016). Social media and crisis management: CERC, search strategies, and Twitter content. *Computers in Human Behavior, 54*, 647-652. Retrieved from https://www.journals.elsevier.com/computers-in-human-behavior

Lainhart IV, J. W. (2000). COBIT™: A methodology for managing and controlling information and information technology risks and vulnerabilities. *Journal of Information Systems, 14*(1), 21-25. Retrieved from http://aaahq.org/ais/journal

Lam, J. (2014). *Enterprise risk management: From incentives to controls*. Hoboken, NJ: John Wiley & Sons.

Lam, W. (2002). Ensuring business continuity. *IT Professional, 4*(3). Retrieved from https://www.computer.org/it-professional/

Lanz, J. (2015). Conducting information technology risk assessments. *CPA Journal*, *85*(5), 6-9. Retrieved from http://www.cpajournal.com/

Latif, A. A., Arshad, N. H., & Janom, N. (2016). The development of infostructure maturity model for application in disaster management. *Journal of Theoretical and Applied Information Technology, 88*(1), 169. Retrieved from http://www.jatit.org

Law, M. D., & Robson, G. (2014). A case study for accounting information systems-A business continuity plan for protecting critical financial information in the NYC

financial services industry. *The Review of Business Information Systems, 18*(1), 15. Retrieved from http://www.cluteinstitute.com/

Lea, J. K., & Tippett, V. C. (2017). Mass-casualty events: How do we ensure an efficient and effective response?. *Prehospital and Disaster Medicine, 32*(S1), S234-S235. Retrieved from https://www.cambridge.org/core/journals/prehospital-and-disaster-medicine

Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the cyber-attack on the Ukrainian power grid. *SANS ICS Report*. Retrieved from https://ics.sans.org/

Leech, N. L., & Onwuegbuzie, A. J. (2011). Beyond constant comparison qualitative data analysis: Using NVivo. *School Psychology Quarterly, 26*(1), 70. doi:10.1037/a0022711

Lewis, J. A. (2013). Raising the bar for cybersecurity. Center for Strategic and International Studies. Retrieved from https://www.csis.org/

Liao, R., Balasinorwala, S., & Rao, H. R. (2017). Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests. *Information Systems Frontiers*, 1-13. Retrieved from https://link.springer.com/journal

Lindström, J., Samuelsson, S., & Hägerfors, A. (2010). Business continuity planning methodology. *Disaster Prevention and Management: An International Journal, 19*(2), 243-255. doi:10.1108/09653561011038039

Linstone, H. A., & Turoff, M. (2002). *The Delphi Method. Techniques and Applications*. Retrieved from http://www.academia.edu/download/40866077/delphibook.pdf

Liu, X., Li, Z., Shuai, Z., & Wen, Y. (2017). Cyber attacks against the economic operation of power systems: a fast solution. *IEEE Transactions on Smart Grid, 8*(2), 1023-1025. Retrieved from http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?reload=true&punumber=5165411

Logan, J. R., Issar, S., & Xu, Z. (2016). Trapped in Place? Segmented Resilience to Hurricanes in the Gulf Coast, 1970–2005. *Demography, 53*(5), 1511-1534. Retrieved from https://s4.ad.brown.edu/Projects/

Long, N., & Thomas, R. (2001). Trends in denial of service attack technology. CERT Coordination Center. Retrieved from http://www.cert.org

Lord, K. (1981). *The data center disaster consultant, Second edition*. Wellesley, MA: Prentice-Hall.

Loui, R. P., & Loui, T. D. (2016). How to survive a cyber pearl harbor. *Computer, 49*(6), 31-37. doi:10.1109/MC.2016.186

Manhart, M., & Thalmann, S. (2015). Protecting organizational knowledge: a structured literature review. *Journal of Knowledge Management, 19*(2), 190-211. doi:10.1108/JKM-05-2014-0198

Mansfield-Devine, S. (2014). Hacking on an industrial scale. *Network Security, 2014*(9), 12-16. doi:10.1016/S1353-4858(14)70092-3

Mansfield-Devine, S. (2016). Ransomware: taking businesses hostage. *Network Security, 2016*(10), 8-17. Retrieved from https://www.journals.elsevier.com/network-security

Marinescu, M. I. (2015). Cyberwar & cyberterrorism heading towards a cyber-waterloo. *Annals of University of Oradea, Series: International Relations & European Studies,* (7), 49-60. Retrieved from https://catalog.wakegov.com

Marion, C. C. (1988). Computer viruses and the law. Dick. L. Rev., 93, 625. Retrieved from http://heinonline.org/

Martin M, Lam MS (2008) Automatic generation of XSS and SQL injection attacks with goal-directed model checking. In: Proceedings of the USENIX security symposium (USENIX). Retrieved from https://www.usenix.org/conference/

Matar, S., Matar, N., Balachandran, W., & Hunaiti, Z. (2016). Social media platforms and its applications in natural disaster and crisis events–the case of Bosnia & Herzegovina. *Journal of Information & Knowledge Management.* Retrieved from http://www.worldscientific.com/worldscinet/jikm

Maxwell, J. A. (2005). *Applied Social Research Methods Series: Vol. 41. Qualitative research design: An interactive approach* (2nd ed.). Thousand Oaks, CA: Sage.

McCreight, T., & Leece, D. (2016). Physical security and IT convergence: Managing the cyber-related risks. *Journal of Business Continuity & Emergency Planning, 10*(1), 18-30. Retrieved from http://www.henrystewartpublications.com/jbcep

McLaughlin, P. (2005). NFPA 1600: ground rules for disaster-preparedness. *Cabling Installation & Maintenance,* 38-40. Retrieved from http://www.cablinginstall.com/index.html

McManus, J. (2004). A stakeholder perspective within software engineering projects. In Engineering Management Conference, 2004. *IEEE International*, 2, 880-884. Retrieved from http://ieeexplore.ieee.org

Mihut, M. (2014). SERIOS: A security model and framework for implementing information security. *Economy Informatics, 14*(1), 63-72. Retrieved from http://www.economyinformatics.ase.ro/

Million, W. (1997). Disaster recovery planning: More than boom, and gloom. *Disaster Recovery Journal, 1*(10), 44-48. Retrieved from https://www.drj.com/

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative data analysis: A Methods sourcebook* (3rd ed.). Thousand Oaks, CA: Sage.

Miura, H., Midorikawa, S., & Matsuoka, M. (2016). Building damage assessment using high-resolution satellite SAR images of the 2010 Haiti earthquake. *Earthquake Spectra, 32*(1), 591-610. Retrieved from https://www.researchgate.net/profile/Hiroyuki_Miura4/publication

Mojtahedi, M., & Oo, B. L. (2017). The impact of stakeholder attributes on performance of disaster recovery projects: The case of transport infrastructure. *International Journal of Project Management.* doi:10.1016/j.ijproman.2017.02.006

Montesino, R., & Fenz, S. (2011, August). Information security automation: how far can we go?. In Availability, Reliability and Security (ARES), 2011 Sixth International Conference on (pp. 280-285). *IEEE*. Retrieved from http://ieeexplore.ieee.org

Moore, D., Paxson, V., Savage, S., Shannon, C., Staniford, S., & Weaver, N. (2003). Inside the slammer worm. *IEEE Security & Privacy, 99(*4), 33-39. Retrieved from https://www.computer.org/security-and-privacy/

Moore, D., Shannon, C., Brown, D. J., Voelker, G. M., & Savage, S. (2006). Inferring internet denial-of-service activity. *ACM Transactions on Computer Systems (TOCS), 24*(2), 115-139. Retrieved from http://tocs.acm.org

Morgan, S. (2016). Cybercrime damages expected to cost the world $6 trillion by 2021. Retrieved from http://www.csoonline.com/article/3110467/security/

Mossburg, E. (2015). A deeper look at the financial impact of cyber attacks. *Financial Executive, 31*(3 & 4), 77-80. Retrieved from http://www.edingergroup.com/tag/financial-executive-magazine/

Mulla, G., & Ademi, A. (2015). Introduction to business continuity planning. *Science, Innovation New Technology*, 31. Retrieved from http://www.ijsint.org

NSA (2002, May 3). NSA develops INFOSEC assessment training and rating program. NSA Press Release. Retrieved from https://www.nsa.gov/news-features/press-room/

Neaga, G., Winters, B., & Laufman, P. (1997). *Fire in the computer room, what now?: Disaster recovery, preparing for business survival*. London, UK: Prentice-Hall International.

Niederman, F. (2004). IT employment prospects in 2004: a mixed bag. *Computer, 37*(1), 69-77. Retrieved from https://academic.oup.com/comjnl

Niemimaa, M. (2015). Interdisciplinary review of business continuity from an information systems perspective: Toward an integrative framework. *Communications of the Association for Information Systems, 37*(1), 69-102. Retrieved from http://aisel.aisnet.org/cais/vol37/iss1/4

Niglia, A. (2015). *Critical infrastructure protection (CEIP) with a focus on energy security*. Washington, DC: IOS Press.

Office of Management and Budget (2000). Management of federal information resources; Circular no. A-130. Retrieved from https://www.whitehouse.gov/

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management, 42*(1), 15-29. Retrieved from http://www.sciencedirect.com

Page, J., Kaur, M., & Waters, E. (2017). Directors' liability survey: Cyber attacks and data loss—a growing concern. *Journal of Data Protection & Privacy, 1*(2), 173-182. Retrieved from https://www.henrystewartpublications.com/jdpp

Pasquini, A., & Galie, E. (2013). COBIT 5 and the process capability model: Improvements provided for IT governance process. *Symposium from Young Researchers*, (67-76). Retrieved from https://www.sais-jhu.edu

Patterson, D., Brown, A., Broadwell, P., Candea, G., Chen, M., Cutler, J., Enriquez, P., Fox, A., Kieman, E., Merzbacher, M., Oppenheimer, D., Sastry, N., Telzlaff, W., Traupman, J. & Treuhaft, N. (2002). Recovery-oriented computing (ROC): Motivation, definition, techniques, and case studies. Technical Report

UCB//CSD-02-1175, UC Berkeley Computer Science. Retrieved from http://roc.cs.berkeley.edu

Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). Thousand Oaks, CA: Sage.

Pearson, E., & Bethel, C. L. (2016, April). A design review: Concepts for mitigating SQL injection attacks. In Digital Forensic and Security (ISDFS), 2016 4th International Symposium (169-169). Retrieved from http://www.ieee.org/conferences_events

Pennardt, A., Kamin, R., Llewellyn, C., Shapiro, G., Carmona, P. A., & Schwartz, R. B. (2016). Integration of tactical emergency casualty care into the national tactical emergency medical support competency domains. *J Spec Oper Med, 16*, 62-66. Retrieved from https://www.jsomonline.org/index.php

Phillips, B. D. (2015). *Disaster recovery*. Boca Raton, FL: CRC.

Pieko, E. (2005). Improving the quality of information technology (IT) security audits for federal agencies. *Digital Abstracts International*, *61*(9). Retrieved from http://www.ijdc.net/

Ponemon Institute (2016). 2016 cost of data breach study: Impact of business continuity management. Retrieved from http://pointbandbeyond.com/

Price Waterhouse Cooper (2015). US cybersecurity: Progress stalled. Key findings from the 2015 U.S. state of cybercrime survey. Retrieved from https://www.pwc.com

Quang Tran, M., Kien, N., Borcea, C., & Yamada, S. (2014). On-the-fly establishment of multihop wireless access networks for disaster recovery. *IEEE Communications Magazine, 52*(10), 60-66. doi:10.1109/MCOM.2014.6917403

Rabjohn, A. (2013). The human cost of being a 'first responder'. *Journal Of Business Continuity & Emergency Planning, 6*(3), 268-271. Retrieved from http://www.henrystewartpublications.com/jbcep

Raiyn, J. (2014). A survey of cyber attack detection strategies. *International Journal of Security and Its Applications, 8*(1), 247-256. Retrieved from http://www.sersc.org/

Randeree, K., Mahal, A., & Narwani, A. (2012). A business continuity management maturity model for the UAE banking sector. *Business Process Management Journal, 18*(3), 472-492. doi:10.1108/14637151211232650

Razvi Doomun, M. (2008). Multi-level information system security in outsourcing domain. *Business Process Management Journal, 14*(6), 849-857. doi:10.1108/14637150810916026

Razzaq, A., Latif, K., Ahmad, H. F., Hur, A., Anwar, Z., & Bloodsworth, P. C. (2014). Semantic security against web application attacks. *Information Sciences, 254*, 19-38. Retrieved from https://www.journals.elsevier.com/information-sciences/

Revesz, R. L., & Stewart, R. B. (2016*). Analyzing superfund: Economics, science and law*. Abingdon, United Kingdom: Routledge.

Ridley, G., Young, J., & Carroll, P. (2004, January). COBIT and its utilization: A framework from the literature. In System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference. *IEEE*. Retrieved from http://www.ieee.org

Rittinghouse, J., & Ransome, J. (2011*). Business continuity and disaster recovery for infosec managers*. Boston, MA: Digital Press.

Rodriguez, M. (2016). Technology triage: Assessing and managing library systems and projects. University of Connecticut. Retrieved from http://digitalcommons.uconn.edu/

Rodríguez, R., & Román, S. (2016). The influence of sales force technology use on performance: The study of mediating and moderating effects. *In Let's Get Engaged! Crossing the Threshold of Marketing's Engagement Era* (93-94). Gewerbestrasse, Switzerland: Springer International.

Ross, D. F. (2016). *Introduction to e-supply chain management: engaging technology to build market-winning business partnerships*. Boca Raton, FL: CRC.

Salini, P., & Shenbagam, J. (2015). Prediction and classification of web application attacks using vulnerability ontology. *International Journal of Computer Applications, 116*(21). Retrieved from http://www.ijcaonline.org/

Samanta, P., & Dugal, M. (2016). Basel disclosure by private and public-sector banks in India: assessment and implications. *Journal of Financial Regulation and Compliance, 24*(4). doi:10.1108/JFRC-12-2015-0065

Sarmiento, J. P., Hoberman, G., Jerath, M., & Ferreira Jordao, G. (2016). Disaster risk management and business education: the case of small and medium enterprises. *AD-minister*, (28), 73-90. doi:10.17230/ad-minister.28.4

Schmitting, R. & Munns, A. (2010). Performing a security risk assessment. *ISACA Journal* (1). Retrieved from https://www.isaca.org/journal/archives/2010

Schreider, T. (1996). The legal issues of disaster recovery planning. *Disaster Recovery Journal, 9*(2), 31. Retrieved from https://www.drj.com/

Schuba, C. L., Krsul, I. V., Kuhn, M. G., Spafford, E. H., Sundaram, A., & Zamboni, D. (1997). Analysis of a denial of service attack on TCP. In Security and Privacy, Proceedings (208-223). *IEEE*. Retrieved from http://www.ieee.org

Schultz, E. E. (2004). Malware update. *Computers & Security, 23*(5), 355-361. doi:10.1016/j.cose.2004.06.001

Schultz, E., & Shumway, R. (2001). *Incident response: a strategic guide to handling system and network security breaches*. Indianapolis, IN: New Riders Publishing.

Schwartz, M. (2017a). Another global ransomware outbreak rapidly spreads. *InfoRisk Today*. Retrieved from http://www.inforisktoday.com/another-global-ransomware-outbreak-rapidly-spreads-a-10060

Schwartz, M. (2017b). South Korean hosting firm pays 1 million ransom. *InfoRisk Today*. Retrieved from http://www.inforisktoday.com

Security Exchange Commission (n. d.). Securities Exchange Act of 1934. *SEC Docket, 49*(8). Retrieved from http://www.4tnoxu.com/

Sen, R., & Heim, G. R. (2016). Managing enterprise risks of technological systems: An exploratory empirical analysis of vulnerability characteristics as drivers of exploit publication. *Decision Sciences, 47*(6), 1073-1102. doi:10.1111/deci.12212

Sharifi, M., Ayat, M., Rahman, A. A., & Sahibudin, S. (2008) Lessons learned in ITIL implementation failure. *IEEE*, 1, 1-4. Retrieved from http://www.ieee.org

Sharma, C., & Jain, S. C. (2014, August). Analysis and classification of SQL injection vulnerabilities and attacks on web applications. In Advances in Engineering and Technology Research (ICAETR), 2014 International Conference on (1-6). *IEEE*. Retrieved from http://www.ieee.org

Shuler, R. L., & Smith, B. G. (2017). Internet of things behavioral-economic security design, actors & cyber war. *Advances in Internet of Things, 7*(02), 25. Retrieved from http://www.scirp.org/journal/ait/

Shackelford, S. J. (2009). From nuclear war to net war: Analogizing cyber attacks in international law. *Berkeley Journal of International Law, 27*(1), 192-251. Retrieved from http://scholarship.law.berkeley.edu/bjil/

Shackelford, S., Proia, A., Martell, B., & Craig, A. (2015). Toward a global cybersecurity standard of care?: Exploring the implications of the 2014 NIST Cybersecurity Framework on shaping reasonable national and international cybersecurity practices. *Texas International Law Journal, 50*(2), 303-353. Retrieved from http://www.tilj.org/

Silver, C., & Lewins, A. (2014). *Using software in qualitative research: A step-by-step guide*. Thousand Oaks, CA: Sage.

Simons, B. (1999). Melissa's Message. *Communications of The ACM, 42*(6), 25-26. Retrieved from https://cacm.acm.org/

Singer, P. W. (2015). Stuxnet and its hidden lessons on the ethics of cyberweapons. *Case Western Reserve Journal of International Law, 47*(3), 79-8

Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied Clinical Informatics, 7*(2), 624. Retrieved from https://www.ncbi.nlm.nih.gov

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education, 6*, 1. Retrieved from http://www.igi-global.com/journal/international-journal-information-communication-technology

Smith G. (2017) Involving land use planners in pre-event planning for post-disaster recovery. *Journal of The American Planning Association, 80*(4), 306-307. Retrieved from https://www.planning.org/japa/

Snyder, R. (2014). Project risk management within information systems. *ASBBS Proceedings, 21*(1), 670. Retrieved from http://asbbs.org/

Solberg Søilen, K. (2016). Economic and industrial espionage at the start of the 21st century - Status quaestionis. *Journal of Intelligence Studies in Business, 6*(3), 51-64. Retrieved from https://ojs.hh.se/index.php/JISIB

Souppaya, M., Feldman, L., & Witte, G. (2017). ITL bulletin for February 2017 guide for cybersecurity incident recovery. U.S. Department of Commerce. Retrieved from http://csrc.nist.gov/publications

Sprague, C. (2015). 21st century IT applications. *Research Starters: Business (Online Edition). EBSCOhost.* Retrieved from https://www.ebsco.com/

Srinivasan, S. (2016). Data Privacy Issues in Cloud Computing. *International Journal of Digital Society 7*(4). Retrieved from http://infonomics-society.org/ijds/

Stalans, L. J., & Finn, M. A. (2016). Understanding how the internet facilitates crime and deviance. *An International Journal of Evidence-based Research, Policy, and Practice 11*(4). doi:10.1080/15564886.2016.1211404

Stanton, R. (2005). Beyond disaster recovery: the benefits of business continuity. *Computer Fraud & Security, 2005*(7), 18-19. doi:10.1016/S1361-3723(05)70234-7

Steiner, H. (2014). Coercive instruments in the digital age: The cases of cyber-attacks against Estonia and Iran. Swedish National Defense College. Retrieved from http://www.diva-portal.org/

Stewart, K., Allen, J., Dorofee, A., Valdez, M., & Young, L. (2015). Defining a maturity scale for governing operational resilience. Carnegie-Mellon University Pittsburgh, PA: Software Engineering Institute. Retrieved from http://www.cmu.edu/

Suaybaguio, M. J. Z. (2016). Sms technology as disaster warning and alert system as perceived by selected constituents of Davao del Norte. *Researchers World, 7*(1), 38. Retrieved from http://www.researchersworld.com/

Takahashi, B., Tandoc, E. C., & Carmichael, C. (2015). Communicating on Twitter during a disaster: An analysis of tweets during Typhoon Haiyan in the Philippines. *Computers in Human Behavior, 50*, 392-398. doi:10.1016/j.chb.2015.04.020

Thejendra, B. S. (2014). *Disaster recovery and business continuity: A quick guide for small organisations and busy executives*. IT Governance Publishing, Ely, England

Tisdale, S. M. (2015). Cybersecurity: Challenges from a systems, complexity, knowledge management and business intelligence perspective. *Issues in Information Systems, 16*(3). Retrieved from http://www.iacis.org/iis/iis.php

Toigo, J. (1989*). Disaster recovery planning; Managing risk and catastrophe in information systems*. Englewood Cliffs, NJ: Yourdon Press.

Tran, H., Campos-Nanez, E., Fomin, P., & Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *Computers & Security, 61*, 19-31. Retrieved from http://www.journals.elsevier.com/computers-and-security

University of Oregon (2007). Post-Disaster Recovery Planning Forum: How-To Guide. University of Oregon Community Service Center. Retrieved from http://nws.weather.gov/nthmp/Minutes/oct-nov07

US Department of Homeland Security (2011). Presidential Policy Directive 8. Retrieved from https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

US Department of Homeland Security (2003). Presidential Policy Directive 7. Retrieved from https://www.dhs.gov/homeland-security-presidential-directive-7

Vaidya, T. (2015). 2001-2013: Survey and Analysis of Major Cyberattacks. *arXiv* retrieved from https://arxiv.org/

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372. Retrieved from http://www.tandfonline.com/toc/uism20/current

Venkatesh, J., & Das, B. (2016). A study on information technology infrastructure to improve retail business processes. *International Journal of Research in IT and Management*, *6*(1), 1-6. Retrieved from https://euroasiapub.org/

Verizon (2017). 2017 Data breach investigations report: 10th edition. Verizon. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Venkitachalam, K., & Willmott, H. (2015). Factors shaping organizational dynamics in strategic knowledge management. *Knowledge Management Research & Practice, 13*(3), 344-359. Retrieved from http://www.springer.com/business+%26+management/operations+research

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both?. *Computers & Security, 24*(2), 99-104. Retrieved from http://www.sciencedirect.com/science/journal/

Wang, X., & Zhang, W. (2016). Cross-site scripting attacks procedure and prevention strategies. *EDP Sciences*, *61*. Retrieved from https://publications.edpsciences.org/#!s=current&l=en

Weichselgartner, J., & Pigeon, P. (2015). The role of knowledge in disaster risk reduction. *International Journal of Disaster Risk Science, 6*(2), 107-116. Retrieved from https://link.springer.com/journal/13753

Wold, G. H. (2002). Disaster recovery planning process. *Disaster Recovery Journal, 5*(1), 29-34. Retrieved from https://www.drj.com/

Woods, M., Macklin, R., & Lewis, G. K. (2016). Researcher reflexivity: exploring the impacts of CAQDAS use. *International Journal of Social Research Methodology*, *19*(4), 385-403. Retrieved from http://www.tandfonline.com

Yang, T., Ku, C., & Liu, M. (2016). An integrated system for information security management with the unified framework. *Journal of Risk Research, 19*(1), 21-41. doi:10.1080/13669877.2014.940593

Yeh, F., McMullen, K. D., & Kane, L. T. (2010). Disaster planning in a health sciences library: A grant-funded approach. *Journal of the Medical Library Association, 98*(3), 259. Retrieved from http://jmla.mlanet.org/ojs/jmla

Yin, R. (2013). *Case study and research design methods* (5th ed.). Thousand Oaks, CA: Sage.

Zahidy, A. H., Azizan, N. A., & Sorooshian, S. (2016). *Organizational productivity and performance measurements using predictive modeling and analytics*. Hershey, PA: IGI Global.

Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal, 27*(1), 13-15. doi:10.4314/mmj.v27i1.4

Zimmerman, R., & Restrepo, C. E. (2009). Information technology and critical infrastructure interdependencies for emergency response. Proceedings of the 3rd International Conference on Information Systems for Crises Response and Management. Retrieved from https://iscram2017.mines-albi.fr/

Appendix A: Invitation Letter

Invitation to participate in a doctoral research project with consent

Project Title: The Effects of Computer Crimes on the Management of Disaster Recovery

Researchers:
Timothy Proffitt, doctoral candidate, Management
David Gould - Ed.D., Committee Chair, Walden University

Dear Madam/Sir,

You are invited to participate in a research project being conducted by Walden University. This information sheet describes the project. Please read this sheet carefully and be confident that you understand its contents before deciding whether to participate.

Who is involved in this research project? Why is it being conducted?

Timothy Proffitt is conducting this research as a doctoral requirement and Dr. David Gould from Walden University will be the committee chair. The Walden Institutional Review Board (IRB) has given their written support for this research. The purpose of this qualitative study is to understand how information technology disaster recovery controls and processes can be modified to improve response to a computer crime caused business interruption.

Why have you been approached?

You have been approached on the basis that you identify yourself as an expert in disaster recovery or cybersecurity. You have not been approached randomly, but rather, have been identified by one of the researchers or by one of your friends, family or acquaintances that might be aware of you being an expert in these fields.

What is the project about? What are the questions being addressed?

The purpose of this qualitative Delphi study is to understand how information technology disaster recovery controls and processes can be modified to improve response to a computer crime caused business interruption. A qualitative approach will focus on information technology disaster recovery participants to develop a new framework of response. A new model will be developed as an understanding of how the information technology disaster recovery processes could be influenced by other frameworks tailored for cyber security or computer incident response. A Delphi approach was chosen over other qualitative research approaches, such as a case study, because the aim of this study is to learn what factors affect a certain responses and to problem solve to improve the disaster response process.

If I agree to participate, what will I be required to do?

Participation will require the full completion of three rounds of a Delphi questionnaire that should take between 30 and 45 minutes of your time for each round. The initial questionnaires will ask you about factors significantly affecting the ability of disaster recovery programs in responding to computer crimes caused disasters. You are asked to answer question in your expert opinion with the understanding that the next round of questions will build on the previous answers. After each submission, you will be provided feedback to be sure that your submission was clearly understood by the researcher.

It is valuable to the study that all three rounds are completed by a participant. The last round is important in reaching consensus or identifying new areas that need further discussion.

What are the risks or disadvantages associated with participation?

There are no foreseeable risks for your participation outside your normal day-to-day activities. Each of the three rounds will ask you judgments on questions around information technology disaster recovery. The responses should be expected to take between thirty to sixty minutes depending on your responses. The study should not be a significant investment of your time.

What are the benefits associated with participation?

The results of the study will assist in improved disaster recovery planning and response to an emerging threat to any organization relying on technology for vital business functions. Billions of dollars and a number of organizations each year are lost when they are unable to recover from a disaster. Your participation may improve the resiliency of organizations around the globe.

What will happen to the information I provide?

Your completed questionnaire is anonymous and your name will be known only to the researcher. No information will be place into the dissertation that can identify you personally. Your questionnaire will be kept confidential for 15 years before being destroyed. The summarized results may be published in disaster recovery journals, made available to various technology groups, conferences, and various other sources.

What are my rights as a participant?

- You have the right to withdraw your participation at any time.
- You have the right to have any unprocessed data withdrawn and destroyed.
- You have the right to have any questions answered at any time.

Is there a payment?

There will not be any compensation for participating in the study.

Statement of Consent

I have read the above information and I feel I understand the study well enough to make a decision about my involvement. By, replying to this email with the phrase, “Yes,

I consent to this study." You understand that you are agreeing to the terms described above.

Appendix B: List of Round 1 Questions

- What factors significantly affect the ability of disaster recovery programs in responding to computer crimes caused disasters?
- What interruptions caused by computer crimes cause the response team to recover differently than a traditionally planned recovery?
- In what ways can a disaster response be unsuccessful when following traditional technology disaster recovery plans to recover from computer crimes caused business interruption?
- What steps might be an improvement from traditional disaster recovery procedures to resume the organization from a computer crimes disaster?
- What differences can be found from a business that prepared for interruptions caused computer crimes as compared to those that do not?
- What should organizations avoid to improve the ability to recover from computer crimes?
- What common themes exist where the cause of the technology interruption could have been significantly reduced by modification of the information technology disaster recovery framework to align with a cyber security framework?
- What type of expertise should be recruited to build a successful disaster recovery program that could better respond to computer crimes?
- What cyber security processes could improve disaster response, if any?

- What advantages or disadvantages exist in specifically defining cyber security risk and controls in disaster recovery frameworks?

Appendix C: List of Themes Build from Round 1

- What factors significantly affect the ability of disaster recovery programs
- What interruptions caused by computer crimes cause the response team to recover differently
- What ways can a disaster response be unsuccessful when following traditional technology disaster recovery
- What steps could be an improvement
- What differences can be found from a business that prepared
- What should organizations avoid to improve
- Where could the modification of the information technology disaster recovery framework to align with a cyber security framework?
- What type of expertise should be recruited
- What cyber security processes could improve disaster response
- What advantages or disadvantages exist in specifically defining cyber security risk

Appendix D: Consensus Building from Round 2

Question 1: What factors significantly affect the ability of disaster recovery programs in responding to computer crimes caused disasters?
Lack of understanding of the interdependencies in IT makes it difficult to anticipate the impact of the recovery.
The organization must have adequate planning for computer crimes.
Critical IT services must be available to conduct a recovery.
A lack of management support and poor funding will negatively impact this response.
If the organization does not staff skilled resources, the response will suffer.
The untested recovery process from computer crimes will negatively impact the recovery process.
The ability to triage the incident correctly as the ITDR team comes on the scene will be an issue when the cause is computer crimes
IR teams must be trained for such a scenario.
Organizations conducting lessons learned will improve their response.
Critical data must be protected and available from an alternate source to protect from computer crimes
There must be a clear list of responsibilities in responding to this type incident.
The lack of an RTO and RPO will hamper the response for computer crimes.
Replacement equipment must be available and quickly replaced
Question 2: What interruptions caused by computer crimes could force an organizations disaster response team to recover differently than a traditionally planned recovery (playbooks)?
Organizations may need to document their computer crimes recovery differently for compliance/legal/law enforcement reasons.
A compromise of the IT administrators/ IT systems will force a different response.
Computer crimes can render critical systems unable to support a recovery where traditionally it would.
It will be hard to identify compromised versus uncompromised systems for recovery.
A triage of a computer crimes attack can lead to multiple activities of containment outside of the recovery process.
Computer crime related recovery is much more variable, and it is very difficult to determine the variables effectively.
A destructive data threat might require a more focused reaction than what a traditional play book has.

Question 3: In what ways can a disaster response be unsuccessful when following traditional technology disaster recovery plans to recover from computer crimes caused business interruption?
If a data backup/alternative is not available, traditional recovery will not be successful or extremely time-consuming.
A compromise of the IT administrators system or credentials will force a different response capability than recovery from water/power/storms.
If an organization finds itself in a response that it has not scoped, it will trip upon the response.
Attackers can purposely deceive the ITDR team with decoy interruptions to increase the success of the attack.
When a breach occurs, the organization may lack the ability to anticipate and quantify the damage. This would hamper the recovery.
It will be hard to identify compromised versus uncompromised systems for recovery.
A response would be difficult without the possession of endpoints, reliable communications, or reliable utilities.
An organization may not have outside resources available to assist with a computer crimes interruption. For example, an organization may not have an InfoSec resource on retainer.
The organization has a lack of alignment with IT goals and business goals.
A Traditional DR playbook may not eradicate the intrusion correctly.
The DR team may have a poor understanding of the attack which could cause the activation of the wrong recovery solution, delaying, or stopping the overall business resumption.
If organizations do not test for the computer crimes scenario, it will fail to recover on time.
Question 4: What steps could be an improvement from traditional disaster recovery (i.e. loss of power, fire, flood) procedures to resume the organization from a computer crimes disaster (DoS, hacking, crypto locker, data destruction)?
Computer crimes are more complex and involve greater communication and collaboration outside of IT and the IT Security team.
Keep the soft copy of the DR plan offline from the main company environment so that it cannot be hacked.
Craft procedures where data is lost or corrupted and recovery have to be initiated using physical backups.
A separate set of procedures for cybercrime that takes into consideration the risks of computer crimes interruptions.
Real-time data synchronization to alternate locations would improve recovery from a computer crime interruption.
An improvement would come from lessons learned and root cause analysis sessions.
Security architectures must use technology in support of business objectives, and accurately model dependencies to prioritize resources.

implement a solution that can detect a change in data to encrypted state or data loss that will prevent existing backups from being overwritten.
Organizations must focus on people, communications, tools, and facilities to improve from computer crimes interruptions.
Preventive and testing measures must be taken continuously for computer crimes.
Containment and eradication procedures for computer crimes will need to be included in playbooks.
Embed a Cybersecurity Framework into the ITDR program.
Leverage a cloud technology for an organization so that they are better secured and recoverable.
Question 5: What differences can be found from an organization that prepares for interruptions caused computer crimes as compared to those that do not?
I have seen organizations struggle to recover from a typical disaster recovery effort and fail completely when attempting to recover from a computer crime event.
The prepared organization will not rely on one solution to protect everything.
Companies more heavily invested in preparing for computer crime-based interruptions have greater integration with their Information Security counterparts and have a management team that understands the risks posed by computer crimes and are willing to devote more money and attention to prevention and preparation for computer crime interruptions.
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by computer crimes.
Organizations may but subject to fines or lawsuits where they may not come from a traditional disaster.
Organizations must provide a robust awareness program to ITDR teams to help mitigate computer crimes risks.
Question 6: What should organizations avoid to improve the ability to recover from computer crimes interruptions?
Organizations cannot treat a computer crimes recovery as just a “technical” or “IT” led the response to better respond to computer crimes.
Organizations must place security controls on mobile phones to better respond to computer crimes.
Organizations must avoid the knee-jerk reaction to throw money at a problem without first grasping what that problem is and then smartly coming up with the solution.
Organizations must avoid plans that do not take into consideration the current state of the systems to better respond to computer crimes.
Organizations must avoid staff turnover and unclear responsibilities to better respond to computer crimes.

Organizations must avoid open source systems for critical business applications to better respond to computer crimes.
Organizations that do not conduct lessons learned and root cause analysis will not improve to better respond to computer crimes.
Organizations should avoid placing a low value on quality management in DR to better respond to computer crimes.
Organizations must avoid architectures that lack redundancy or resiliency attributes to better respond to computer crimes.
Organizations must avoid thinking they are protected from computer crimes.
Organizations must avoid neglecting the risk of computer crimes interruptions.
Organizations must not focus on speed but instead focus on the assessment phase to better respond to computer crimes.
Organizations must avoid having missing cybersecurity policies to better respond to computer crimes.
Organizations must avoid operating DR functions without the proper funding to better respond to computer crimes.
Organizations cannot operate ITDR and InfoSec in different silos to better respond to computer crimes.
Question 7: What common themes exist where the cause of the technology interruption could have been significantly reduced by modification of the information technology disaster recovery framework to align with a cybersecurity framework?
A well-developed cybersecurity framework supports the ITDR, and the opportunity for a technical interruption is reduced.
Adherence to policies and procedures will reduce the recovery from computer crimes.
A coordinated process alignment between Disaster Recovery and Information Security frameworks is vital to reducing the recovery of this type.
DR and InfoSec should be aligning their lifecycle processes so that like steps are executed together, and participation is integrated.
Developing an ITDR set of practices and different playbooks will reduce the response.
Resilience efforts should be folded into dependency models to reduce the response to this interruption.
Advanced preparation will reduce a computer crimes response.
Testing and segmentation with strict access control and secure baseline configurations will reduce the response to computer crimes.
The computer crime prevention program must include the protection from internal crimes.
Organizations must hold pre-event training processes to reduce computer crimes responses.
There is not much alignment between DR and InfoSec frameworks, and that is a problem.

Question 8: What type of expertise (job skills and/or personal) should be recruited to build a successful ITDR program that could better respond to computer crimes interruptions?
Project management will improve the response to computer crimes.
People management will improve the response to computer crimes.
A deep understanding of interdependencies in the IT environment will improve the response to computer crimes.
A business-focused understanding of the organization will improve the response to computer crimes.
A risk-based focus on the business will improve the response to computer crimes.
Do not hire millennials will improve the response to computer crimes.
Technical, analytical, logical, and lateral thinking will improve the response to computer crimes.
A basic understanding of the layers of protection, prevention, policy management, operations, monitoring, and response will improve computer crimes recovery efforts.
Certified professionals with CISSP, CISA, and CISM credentials to reduce the risk of computer crimes recovery efforts.
I don't think it's a matter of adding job skills or personnel to the equation but more about access to other teams will improve the response to computer crimes.
Cyber Security expertise needs to exist to improve the response to computer crimes.
Minor skills are needed such as Ethical Hacking, Encryption Solutions, Highly Adaptable and Collaborative skills will improve the response to computer crimes.
Question 9: What common cybersecurity processes could improve recovery effort that would not normally be found in an ITDR program?
Enterprise Security Risk Management (ESRM) in the ITDR process
Password management is important
The All-hazards approach should include InfoSec interruptions
Standards-based Information security management systems life cycle
InfoSec training for ITDR teams
Organizations can integrate the RMO and CSO responsibilities into ITDR planning activities
Formal lessons learned and future prevention, which may help lessen the severity of future incidents.
Establishing a baseline of security configurations is another cybersecurity process that extends to ITDR.
Asset inventory processes
The entire Cybersecurity Framework should be incorporated into the ITDR program
Penetration testing and disaster recovery testing
CAG 20 Critical Security controls would improve the recovery

Question 10: What advantages or disadvantages exist in specifically defining cybersecurity risk and controls in disaster recovery frameworks?
Organizations should include InfoSec risks in ITDR frameworks
If done well, clearly following an ESRM program and linking the outcomes of the framework to the DR framework offers organizations the ability to see the interdependencies between assets and objectives.
There could be a disadvantage to the organization by increasing the costs of additional InfoSec controls into ITDR processes.
A cybersecurity framework adoption into the ITDR could result in minimal, or zero interruptions to its business and could improve both productivity and brand image.
There does not appear to be any disadvantages to a cybersecurity framework integration into ITDR.
Without cyber being a part of that plan the plan itself will be lacking.
If done properly, cybersecurity risk management will identify the DR systems as one of the most business-critical systems in the organization.
Integrating some cybersecurity risks and controls in your disaster recovery process may allow it to easier identify attacks that would otherwise be considered a “system malfunction.”
A cybersecurity framework integration could provide an advantage in that it provides a 2nd or 3rd layer of risk management to the disaster recovery framework.

Appendix E: List of Round 3 Questions

Lack of understanding of the interdependencies in IT makes it difficult to anticipate the impact of the recovery. Improve understanding.
The organization must have adequate planning for computer crimes.
Critical IT services must be available to conduct a recovery.
A lack of management support and poor funding will negatively impact this response.
If the organization does not staff skilled resources, the response will suffer.
The untested recovery process from computer crimes will negatively impact the recovery process.
The ability to triage the incident correctly as the ITDR team comes on the scene will be an issue when the cause is computer crimes
IR teams must be trained for such a scenario.
Organizations conducting lessons learned will improve their response.
Critical data must be protected and available from an alternate source to protect from computer crimes. There must be a clear list of responsibilities in responding to this type incident.
If a data backup/alternative is not available, traditional recovery will not be successful or extremely time-consuming.
If an organization finds itself in a response that it has not scoped, it will trip upon the response.
When a breach occurs, the organization may lack the ability to anticipate and quantify the damage. This would hamper the recovery.
An organization may not have outside resources available to assist with a computer crimes interruption. For example, an organization may not have an InfoSec resource on retainer.
The organization has a lack of alignment with IT goals and business goals.
A Traditional DR playbook may not eradicate the intrusion correctly.
The DR team may have a poor understanding of the attack which could cause the activation of the wrong recovery solution, delaying, or stopping the overall business resumption.
If organizations do not test for the computer crimes scenario, it will fail to recover on time.
Computer crimes are more complex and involve greater communication and collaboration outside of IT and the IT Security team.
Keep the soft copy of the DR plan offline from the main company environment so that it cannot be hacked.
Craft procedures where data is lost or corrupted and recovery have to be initiated using physical backups.
A separate set of procedures for cybercrime that takes into consideration the risks of computer crimes interruptions.

Real-time data synchronization to alternate locations would improve recovery from a computer crime interruption.
An improvement would come from lessons learned and root cause analysis sessions.
Security architectures must use technology in support of business objectives, and accurately model dependencies to prioritize resources.
Organizations must focus on people, communications, tools, and facilities to improve from computer crimes interruptions.
Preventive and testing measures must be taken continuously for computer crimes.
Containment and eradication procedures for computer crimes will need to be included in playbooks.
Embed a Cybersecurity Framework into the ITDR program.
The prepared organization will not rely on one solution to protect everything.
Companies more heavily invested in preparing for computer crime-based interruptions have greater integration with their Information Security counterparts and have a management team that understands the risks posed by computer crimes and are willing to devote more money and attention to prevention and preparation for computer crime interruptions.
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by computer crimes.
Organizations cannot treat a computer crimes recovery as just a “technical” or “IT” led the response to better respond to computer crimes.
Organizations must avoid the knee-jerk reaction to throw money at a problem without first grasping what that problem is and then smartly coming up with the solution.
Organizations must avoid plans that do not take into consideration the current state of the systems to better respond to computer crimes.
Organizations that do not conduct lessons learned and root cause analysis will not improve to better respond to computer crimes.
Organizations should avoid placing a low value on quality management in DR to better respond to computer crimes.
Organizations must avoid architectures that lack redundancy or resiliency attributes to better respond to computer crimes.
Organizations must avoid thinking they are protected from computer crimes.
Organizations must avoid neglecting the risk of computer crimes interruptions.
Organizations must not focus on speed but instead focus on the assessment phase to better respond to computer crimes.
Organizations must avoid having missing cybersecurity policies to better respond to computer crimes.
Organizations must avoid operating DR functions without the proper funding to better respond to computer crimes.

Organizations cannot operate ITDR and InfoSec in different silos to better respond to computer crimes.
A well-developed cybersecurity framework supports the ITDR, and the opportunity for a technical interruption is reduced.
A coordinated process alignment between Disaster Recovery and Information Security frameworks is vital to reducing the recovery of this type.
DR and InfoSec should be aligning their lifecycle processes so that like steps are executed together, and participation is integrated.
Developing an ITDR set of practices and different playbooks will reduce the response.
Resilience efforts should be folded into dependency models to reduce the response to this interruption.
Advanced preparation will reduce a computer crimes response.
There is not much alignment between DR and InfoSec frameworks, and that is a problem. Create alignment.
A deep understanding of interdependencies in the IT environment will improve the response to computer crimes.
A business-focused understanding of the organization will improve the response to computer crimes.
A risk-based focus on the business will improve the response to computer crimes.
Technical, analytical, logical, and lateral thinking will improve the response to computer crimes.
A basic understanding of the layers of protection, prevention, policy management, operations, monitoring, and response will improve computer crimes recovery efforts.
Cyber Security expertise needs to exist to improve the response to computer crimes.
Implement Enterprise Security Risk Management (ESRM) in the ITDR process
Deploy InfoSec training for ITDR teams
Organizations can integrate the RMO and CSO responsibilities into ITDR planning activities
Formal lessons learned and future prevention, which may help lessen the severity of future incidents.
Establishing a baseline of security configurations is another cybersecurity process that extends to ITDR.
Implement Asset inventory processes
Deploy Penetration testing and disaster recovery testing
Implementing the CAG 20 Critical Security controls would improve the recovery effort.
Organizations should include InfoSec risks in ITDR frameworks
If done well, clearly following an ESRM program and linking the outcomes of the framework to the DR framework offers organizations the ability to see the interdependencies between assets and objectives.

Without cyber being a part of that plan, the plan itself will be lacking.
If done properly, cybersecurity risk management will identify the DR systems as one of the most business-critical systems in the organization.
Integrating some cybersecurity risks and controls in your disaster recovery process may allow it to easier identify attacks that would otherwise be considered a “system malfunction.”
A cybersecurity framework integration could provide an advantage in that it provides a 2nd or 3rd layer of risk management to the disaster recovery framework.

Appendix F: Removal of duplicate statements

Question 1:
What factors significantly affect the ability of disaster recovery programs in responding to computer crimes caused disasters?

Lack of understanding of the interdependencies in IT
The organization must have adequate planning for computer crimes
Critical services must be available to conduct a recovery
poor funding will negatively impact this response
executive complacency to the computer crimes threat
response capability to computer crimes is cost-prohibitive
Management support
The organization does not staff skilled resources
untested recovery process will negatively impact the recovery process
ability to triage the incident correctly as the ITDR team comes on the scene
IR team training for such a scenario
management support
conducting lessons learned
The organization must have adequate planning for computer crimes
The organization does not staff skilled resources
executive complacency to the computer crimes threat
The organization must have adequate planning for computer crimes
Critical data must be protected and available from an alternate source
The organization must have adequate planning for computer crimes
There must be a clear list of responsibilities in responding to an incident
untested recovery process will negatively impact the recovery process
Critical data must be protected and available from an alternate source
The lack of a RTO and RPO will hamper the response
The organization must have adequate planning for computer crimes
With computer crime, it is much more difficult to anticipate the impact.
poor funding will negatively impact this response
untested recovery process will negatively impact the recovery process
There must be a clear list of responsibilities in responding to an incident
The organization must have adequate planning for computer crimes
Replacement Equipment must be quickly replaced
Critical services must be available to conduct a recovery
The lack of a RTO and RPO will hamper the response
Untested recovery process will negatively impact the recovery process
The organization must have adequate planning for computer crimes
executive complacency to the computer crimes threat will negatively impact this response

Duplicates removed

Lack of understanding of the interdependencies in IT make it difficult to anticipate the impact
The organization must have adequate planning for computer crimes
Critical services must be available to conduct a recovery
A lack of management support and poor funding will negatively impact this response
executive complacency to the computer crimes threat will negatively impact this response
If the organization does not staff skilled resources the response will suffer
Untested recovery process will negatively impact the recovery process
ability to triage the incident correctly as the ITDR team comes on the scene
IR team training for such a scenario
Organizations conducting lessons learned will improve their response
Critical data must be protected and available from an alternate source
There must be a clear list of responsibilities in responding to an incident
The lack of a RTO and RPO will hamper the response
Replacement Equipment must be quickly replaced

Question 2
What interruptions caused by computer crimes could force an organizations disaster response team to recover differently than a traditionally planned recovery (playbooks)?
Organizations may need to document their computer crimes recovery differently for compliance/legal reasons
A compromise of the IT administrators will force a different response
Computer crimes can render systems unable to support a recovery that traditionally it would.
It will be hard to identify compromised versus uncompromised systems for recovery
Computer crimes can render systems unable to support a recovery that traditionally it would.
It will be hard to identify compromised versus uncompromised systems for recovery
Computer crimes can render systems unable to support a recovery that traditionally it would.
A triage of a computer crimes attack can lead to multiple activities of containment outside of the recovery process.
Computer crimes can render systems unable to support a recovery that traditionally it would.
Organizations may need to document their computer crimes recovery differently for compliance/legal reasons
It will be hard to identify compromised versus uncompromised systems for recovery
A triage of a computer crimes attack can lead to multiple activities of containment outside of the recovery process.

Computer crimes can render systems unable to support a recovery that traditionally it would.
Computer crimes can render systems unable to support a recovery that traditionally it would.
Computer crime related recovery is much more variable and it is very difficult to determine the variables effectively.
It will be hard to identify compromised versus uncompromised systems for recovery
Computer crimes can render systems unable to support a recovery that traditionally it would.
It will be hard to identify compromised versus uncompromised systems for recovery
Computer crimes can render systems unable to support a recovery that traditionally it would.
A destructive data threat might require a more focused reaction that what a traditional play book has.
A triage of a computer crimes attack can lead to multiple activities of containment outside of the recovery process.
A compromise of the IT administrators/ IT systems will force a different response than traditionally

Duplicates removed
Organizations may need to document their computer crimes recovery differently for compliance/legal reasons
A compromise of the IT administrators/ IT systems will force a different response
Computer crimes can render critical systems unable to support a recovery where traditionally it would.
It will be hard to identify compromised versus uncompromised systems for recovery
A triage of a computer crimes attack can lead to multiple activities of containment outside of the recovery process.
Computer crime related recovery is much more variable and it is very difficult to determine the variables effectively.
A destructive data threat might require a more focused reaction than what a traditional play book has.

Question 3
In what ways can a disaster response be unsuccessful when following traditional technology disaster recovery plans to recover from computer crimes caused business interruption?
Organizations may need to document their computer crimes recovery differently for compliance/legal reasons
If a data backup/alternative is not available, traditional recovery will not be successful
If a data backup/alternative is not available, traditional recovery will not be successful
If a data backup/alternative is not available, traditional recovery will not be successful
A compromise of the IT administrators will force a different response

If an organization finds itself in a response that it has not scoped, it will trip up the response.
Attackers can purposely deceive the ITDR team with decoy interruptions to increase the success of the attack
If an organization finds itself in a response that it has not fully scoped, it will trip up the response.
when a breach occurs the organization may lack the ability to anticipate and quantify the damage is impaired.
If a data backup/alternative is not available, traditional recovery will not be successful
It will be hard to identify compromised versus uncompromised systems for recovery
A response would be difficult without the possession of endpoints, reliable communications, or reliable utilities
An organization may not have outside resources available to assist with a computer crimes interruption
The organization has a lack of alignment with IT goals and business goals.
Traditional disaster recovery may not eradicate the intrusion correctly
The DR team may have a poor understanding of the attack which would could cause the activation of the wrong recovery solution, delaying or stopping overall business resumption
If an organization finds itself in a response that it has not fully scoped, it will trip up the response.
If organizations do not test for this scenario it will fail to recover on time.
Organizations may not account for the time need to restore massive amounts of data to recover systems.
If an organization finds itself in a response that it has not scoped, it will trip up the response.
If an organization finds itself in a response that it has not scoped, it will trip up the response.

Duplicates removed
Organizations may need to document their computer crimes recovery differently for compliance/legal reasons
If a data backup/alternative is not available, traditional recovery will not be successful or extremely time consuming
A compromise of the IT administrators system or credentials will force a different response capability
If an organization finds itself in a response that it has not scoped, it will trip up the response.
Attackers can purposely deceive the ITDR team with decoy interruptions to increase the success of the attack
when a breach occurs the organization may lack the ability to anticipate and quantify the damage is impaired.
It will be hard to identify compromised versus uncompromised systems for recovery

A response would be difficult without the possession of endpoints, reliable communications, or reliable utilities
An organization may not have outside resources available to assist with a computer crimes interruption
The organization has a lack of alignment with IT goals and business goals.
Traditional disaster recovery may not eradicate the intrusion correctly
The DR team may have a poor understanding of the attack which would could cause the activation of the wrong recovery solution, delaying or stopping overall business resumption
If organizations do not test for this scenario it will fail to recover on time.

Question 4
What steps could be an improvement from traditional disaster recovery (i.e. loss of power, fire, flood) procedures to resume the organization from a computer crimes disaster (DoS, hacking, crypto locker, data destruction)?
computer crime are more complex and involved greater communication and collaboration outside of IT and the IT Security team.
Keep the soft copy of the DR plan offline from the main company environment so that it can't hacked.
Craft procedures where data is gone or corrupted and recovery has to be initiated using physical backups.
a separate set of procedures for cyber crime that takes into consideration the insidious nature of the cyber attacker.
Real-time data synchronization to alternate locations
Conduct lessons learned and root cause analysis sessions
Security architectures must use technology in support of business objectives, and accurately model dependencies to prioritize resources.
Craft procedures where data is gone or corrupted and recovery has to be initiated using physical backups.
implement a solution that can detect a change in data to encrypted state or data loss that will prevent existing backups from being overwritten.
focus on people, communications, tools, and facilities.
preventive and testing measures must be taken continuously
preventive and testing measures must be taken continuously
Conduct lessons learned and root cause analysis sessions
Containment and eradication procedures will need to be included in playbooks.
Embed a Cybersecurity Framework into the DR program.
Leverage a cloud technology for an organization so that they are better secured and recoverable
Preventive and testing measures must be taken continuously
Computer crime are more complex and involved greater communication and collaboration outside of IT and the IT Security team.
Embed a Cybersecurity Framework into the DR program.

Preventive and testing measures must be taken continuously

Duplicates removed
computer crime are more complex and involved greater communication and collaboration outside of IT and the IT Security team.
Keep the soft copy of the DR plan offline from the main company environment so that it can't hacked.
Craft procedures where data is gone or corrupted and recovery has to be initiated using physical backups.
A separate set of procedures for cyber crime that takes into consideration the risks of computer crimes interruptions.
Real-time data synchronization to alternate locations
Conduct lessons learned and root cause analysis sessions
Security architectures must use technology in support of business objectives, and accurately model dependencies to prioritize resources.
implement a solution that can detect a change in data to encrypted state or data loss that will prevent existing backups from being overwritten.
Organizations must focus on people, communications, tools, and facilities.
preventive and testing measures must be taken continuously
Containment and eradication procedures will need to be included in playbooks.
Embed a Cybersecurity Framework into the DR program.
Leverage a cloud technology for an organization so that they are better secured and recoverable
Organizations may need to document their computer crimes recovery differently for compliance/legal reasons

Question 5:
What differences can be found from an organization that prepares for interruptions caused computer crimes as compared to those that do not?
I have seen organizations struggle to recover from a typical disaster recovery effort, and fail completely when attempting to recover from a computer crime event.
Don't rely on one solution to protect everything.
companies more heavily invested in preparing for computer crime-based interruptions have greater integration with their Information Security counterparts and have a management team that understands the risks posed by computer crimes and are willing to devote more money and attention to prevention and preparation for computer crime interruptions.
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by cyber attacks
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by cyber attacks
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by cyber attacks

Organizations may but subject to fines or law suits where they may not from a traditional disaster.
organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by cyber attacks
A prepared organization will have a realistic recovery plan that has multiple options for recovery scenarios and reduced downtime from computer crimes.
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by cyber attacks
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by cyber attacks
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by cyber attacks
A prepared organization will have a realistic recovery plan that has multiple options for recovery scenarios and reduced downtime from computer crimes.
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by cyber attacks
Organizations must provide a robust awareness program to help mitigate computer crimes risks

Duplicates removed
I have seen organizations struggle to recover from a typical disaster recovery effort, and fail completely when attempting to recover from a computer crime event.
The prepared organization will not rely on one solution to protect everything.
companies more heavily invested in preparing for computer crime-based interruptions have greater integration with their Information Security counterparts and have a management team that understands the risks posed by computer crimes and are willing to devote more money and attention to prevention and preparation for computer crime interruptions.
organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by cyber attacks
Organizations may but subject to fines or law suits where they may not from a traditional disaster.
A prepared organization will have a realistic recovery plan that has multiple options for recovery scenarios and reduced downtime from computer crimes.
Organizations must provide a robust awareness program to help mitigate computer crimes risks

Question 6:
What should organizations avoid to improve the ability to recover from computer crimes interruptions?
Organizations cannot treat a computer crimes recovery as just a “technical” or “IT” led response.
Organizations must place security controls on mobile phones

avoid the knee-jerk reaction to throw money at a problem without first grasping what that problem is and then smartly coming up with the solution.
Organizations must avoid plans that do not take into consideration the current state of the systems
Organizations must avoid staff turnover and unclear responsibilities
Organizations must avoid open source systems for critical business applications
Organizations that do not conduct lessons learned and root cause analysis will not improve.
Organizations should avoid placing a low value on quality management in DR
Organizations must avoid architectures that lack redundancy or resiliency attributes
Organizations must avoid thinking they are protected from computer crimes
Organizations must avoid neglecting the risk of computer crimes interruptions
Organizations must avoid staff turnover and unclear responsibilities
Organizations must avoid architectures that lack redundancy or resiliency attributes
Organizations must not focus on speed but instead focus on the assessment phase
Organizations must avoid having missing cyber security policies
Organizations must avoid staff turnover and unclear responsibilities
Organizations must avoid plans that do not take into consideration the current state of the systems
avoid the knee-jerk reaction to throw money at a problem without first grasping what that problem is and then smartly coming up with the solution.
Organizations must avoid operating DR functions without the proper funding
Organizations cannot operate ITDR and InfoSec in different silos
Organizations cannot operate ITDR and InfoSec in different silos

Duplicates removed
Organizations cannot treat a computer crimes recovery as just a “technical” or “IT” led response.
Organizations must place security controls on mobile phones
avoid the knee-jerk reaction to throw money at a problem without first grasping what that problem is and then smartly coming up with the solution.
Organizations must avoid plans that do not take into consideration the current state of the systems
Organizations must avoid staff turnover and unclear responsibilities
Organizations must avoid open source systems for critical business applications
Organizations that do not conduct lessons learned and root cause analysis will not improve.
Organizations should avoid placing a low value on quality management in DR
Organizations must avoid architectures that lack redundancy or resiliency attributes
Organizations must avoid thinking they are protected from computer crimes
Organizations must avoid neglecting the risk of computer crimes interruptions
Organizations must not focus on speed but instead focus on the assessment phase

Organizations must avoid having missing cyber security policies
Organizations must avoid operating DR functions without the proper funding
Organizations cannot operate ITDR and InfoSec in different silos

Question 7:
What common themes exist where the cause of the technology interruption could have been significantly reduced by modification of the information technology disaster recovery framework to align with a cybersecurity framework?
a well-developed cybersecurity framework supports the ITDR, and the opportunity for a technical interruption is reduced.
Adherence to policies and procedures
coordinated process alignment between Disaster Recovery and Information Security frameworks is vital
DR and InfoSec should be aligning their lifecycle processes so that like steps are executed together and participation is integrated.
DR and InfoSec should be aligning their lifecycle processes so that like steps are executed together and participation is integrated.
developing an ITDR set of practices and different playbooks
Resilience efforts should be folded into dependency models.
DR and InfoSec should be aligning their lifecycle processes so that like steps are executed together and participation is integrated.
Advanced Preparation
Testing and segmentation with strict access control and secure baseline configurations.
DR and InfoSec should be aligning their lifecycle processes so that like steps are executed together and participation is integrated.
DR and InfoSec should be aligning their lifecycle processes so that like steps are executed together and participation is integrated.
The computer crime prevention program must include the protection from internal crimes.
Organizations must hold pre-event training processes
coordinated process alignment between Disaster Recovery and Information Security frameworks is vital
There is not much alignment between DR and InfoSec frameworks and that is a problem.

Duplicates removed
a well-developed cybersecurity framework supports the ITDR, and the opportunity for a technical interruption is reduced.
Adherence to policies and procedures
coordinated process alignment between Disaster Recovery and Information Security frameworks is vital
DR and InfoSec should be aligning their lifecycle processes so that like steps are executed together and participation is integrated.
developing an ITDR set of practices and different playbooks
Resilience efforts should be folded into dependency models.

Advanced Preparation
Testing and segmentation with strict access control and secure baseline configurations.
The computer crime prevention program must include the protection from internal crimes.
Organizations must hold pre-event training processes
There is not much alignment between DR and InfoSec frameworks and that is a problem.

Question 8:
What type of expertise (job skills and/or personal) should be recruited to build a successful ITDR program that could better respond to computer crimes interruptions?
project management
people management
deep understanding of interdependencies in the IT environment
business focused understanding of the organization
Risk Based focus on the business
Do not hire millennials
Technical, analytical, logical, and lateral thinking
basic understanding of the layers of protection, prevention, policy management, operations, monitoring, and response
Certified professionals with CISSP, CISA, and CISM credentials to reduce the risk
Technical, analytical, logical, and lateral thinking
Analytical, logical, and lateral thinking
I don't think it's a matter of adding job skills or personnel to the equation but more about access to other teams
Technical, analytical, logical, and lateral thinking
Cyber Security expertise needs to exist
Cyber Security expertise needs to exist
I don't think it's a matter of adding job skills or personnel to the equation but more about access to other teams
Technical, analytical, logical, and lateral thinking
Minor skills are needed such as Ethical Hacking, Encryption Solutions, Highly Adaptable and Collaborative
Cyber Security expertise needs to exist
Cyber Security expertise needs to exist
Certified professionals with CISSP, CISA, and CISM credentials to reduce the risk
business focused understanding of the organization
Cyber Security expertise needs to exist
basic understanding of the layers of protection, prevention, policy management, operations, monitoring, and response

Duplicates removed
project management
people management

deep understanding of interdependencies in the IT environment
business focused understanding of the organization
Risk Based focus on the business
Do not hire millennials
Technical, analytical, logical, and lateral thinking
basic understanding of the layers of protection, prevention, policy management, operations, monitoring, and response
Certified professionals with CISSP, CISA, and CISM credentials to reduce the risk
Analytical, logical, and lateral thinking
I don't think it's a matter of adding job skills or personnel to the equation but more about access to other teams
Cyber Security expertise needs to exist
Minor skills are needed such as Ethical Hacking, Encryption Solutions, Highly Adaptable and Collaborative

Question 9:
What common cybersecurity processes could improve recovery effort that would not normally be found in a ITDR program?

Enterprise Security Risk Management (ESRM) in the ITDR process would improve the planning process
Password management
Computer crimes risks should be incorporated into an All-Hazard approach
Standards based Information security management systems life cycle
InfoSec training for ITDR teams would improve the program
Organizations can integrate the RMO and CSO responsibilities into ITDR planning activities
Enterprise Security Risk Management (ESRM) in the ITDR process would improve the planning process
formal lessons learned and future prevention, which may help lessen the severity of future incidents.
Enterprise Security Risk Management (ESRM) in the ITDR process would improve the planning process
Establishing a baseline of security configurations is another cybersecurity process that extends to ITDR.
Asset inventory processes
The entire Cybersecurity Framework should be incorporated in the ITDR program.
Penetration testing and disaster recovery testing
InfoSec training for ITDR teams would improve the program
CAG 20 Critical Security controls would improve the recovery
The entire Cybersecurity Framework should be incorporated in the ITDR program.

Duplicates removed

Enterprise Security Risk Management (ESRM) in the ITDR process would improve the planning process
Password management
Computer crimes risks should be incorporated into an All-Hazard approach
Standards based Information security management systems life cycle
InfoSec training for ITDR teams would improve the program
Organizations can integrate the RMO and CSO responsibilities into ITDR planning activities
formal lessons learned and future prevention, which may help lessen the severity of future incidents.
Establishing a baseline of security configurations is another cybersecurity process that extends to ITDR.
Asset inventory processes
The entire Cybersecurity Framework should be incorporated in the ITDR program.
Penetration testing and disaster recovery testing
CAG 20 Critical Security controls would improve the recovery

Question 10:
What advantages or disadvantages exist in specifically defining cybersecurity risk and controls in disaster recovery frameworks?
Organizations should include InfoSec risks in ITDR frameworks
If done well, clearly following an ESRM program and linking the outcomes of the framework to the DR framework offers organizations the ability to see the interdependencies between assets and objectives.
There could be a disadvantage by increasing costs to the organization by the addition of InfoSec controls into ITDR
If done well, clearly following an ESRM program and linking the outcomes of the framework to the DR framework offers organizations the ability to see the interdependencies between assets and objectives.
There could be a disadvantage by increasing costs to the organization by the addition of InfoSec controls into ITDR
The organization could have minimal or zero interruptions to its business and could improve both productivity and brand image
There does not appear to be any disadvantages
There could be a disadvantage by increasing costs to the organization by the addition of InfoSec controls into ITDR
There does not appear to be any disadvantages
Without cyber being a part of that plan the plan itself will be lacking.
There could be a disadvantage by increasing costs to the organization by the addition of InfoSec controls into ITDR

If done properly, cybersecurity risk management will identify the DR systems as one of the most business-critical system.
integrating some cybersecurity risks and controls in your disaster recovery process may allow it to easier to identify attacks that would otherwise be considered a “system malfunction”.
A Cybersecurity advantage is that it provides a 2nd or 3rd layer of risk management to the disaster recovery framework
There could be a disadvantage by increasing costs to the organization by the addition of InfoSec controls into ITDR
Organizations should include InfoSec risks in ITDR frameworks

Duplicates removed
Organizations should include InfoSec risks in ITDR frameworks
If done well, clearly following an ESRM program and linking the outcomes of the framework to the DR framework offers organizations the ability to see the interdependencies between assets and objectives.
There could be a disadvantage by increasing costs to the organization by the addition of InfoSec controls into ITDR
The organization could have minimal or zero interruptions to its business and could improve both productivity and brand image
There does not appear to be any disadvantages
Without cyber being a part of that plan the plan itself will be lacking.
If done properly, cybersecurity risk management will identify the DR systems as one of the most business-critical system.
integrating some cybersecurity risks and controls in your disaster recovery process may allow it to easier identify attacks that would otherwise be considered a “system malfunction”.
A Cybersecurity advantage is that it provides a 2nd or 3rd layer of risk management to the disaster recovery framework

Appendix G: Analysis of the third round of data

Round 3 statements	mean	STNDV	INQ	Consensus
Lack of understanding of the interdependencies in IT makes it difficult to anticipate the impact of the recovery. Improve understanding.	4.63	0.74	0.25	0.88
The organization must have adequate planning for computer crimes.	4.13	0.83	1.25	0.75
Critical IT services must be available to conduct a recovery.	4.00	0.93	2.00	0.63
A lack of management support and poor funding will negatively impact this response.	4.50	0.76	1.00	0.88
If the organization does not staff skilled resources, the response will suffer.	3.75	0.89	1.25	0.50
The untested recovery process from computer crimes will negatively impact the recovery process.	3.88	0.83	1.25	0.63
The ability to triage the incident correctly as the ITDR team comes on the scene will be an issue when the cause is computer crimes	4.25	0.71	1.00	0.88
IR teams must be trained for such a scenario.	3.88	0.83	1.25	0.63
Organizations conducting lessons learned will improve their response.	3.75	1.04	1.25	0.63
Critical data must be protected and available from an alternate source to protect from computer crimes. There must be a clear list of responsibilities in responding to this type incident.	4.25	0.89	1.25	0.75
If a data backup/alternative is not available, traditional recovery will not be successful or extremely time-consuming.	4.38	0.92	1.25	0.75
If an organization finds itself in a response that it has not scoped, it will trip upon the response.	3.25	0.71	1.00	0.38
When a breach occurs, the organization may lack the ability to anticipate and	4.00	0.76	0.50	0.75

quantify the damage. This would hamper the recovery.				
An organization may not have outside resources available to assist with a computer crimes interruption. For example, an organization may not have an InfoSec resource on retainer.	3.38	0.92	1.25	0.63
The organization has a lack of alignment with IT goals and business goals.	4.25	0.71	1.00	0.88
A Traditional DR playbook may not eradicate the intrusion correctly.	3.63	0.74	1.00	0.43
The DR team may have a poor understanding of the attack which could cause the activation of the wrong recovery solution, delaying, or stopping the overall business resumption.	4.63	0.74	0.25	0.88
If organizations do not test for the computer crimes scenario, it will fail to recover on time.	3.88	0.83	1.25	0.63
Computer crimes are more complex and involve greater communication and collaboration outside of IT and the IT Security team.	3.88	0.83	1.25	0.63
Keep the soft copy of the DR plan offline from the main company environment so that it cannot be hacked.	3.50	0.53	1.00	0.50
Craft procedures where data is lost or corrupted and recovery have to be initiated using physical backups.	4.00	0.76	0.50	0.75
A separate set of procedures for cybercrime that takes into consideration the risks of computer crimes interruptions.	3.25	1.16	2.00	0.50
Real-time data synchronization to alternate locations would improve recovery from a computer crime interruption.	3.50	0.93	1.00	0.57
An improvement would come from lessons learned and root cause analysis sessions.	4.13	0.99	2.00	0.63
Security architectures must use technology in support of business objectives, and accurately model dependencies to prioritize resources.	4.25	0.71	1.00	0.88

Organizations must focus on people, communications, tools, and facilities to improve from computer crimes interruptions.	4.00	0.53	0.00	0.86
Preventive and testing measures must be taken continuously for computer crimes.	4.13	0.83	1.25	0.75
Containment and eradication procedures for computer crimes will need to be included in playbooks.	4.38	0.74	1.00	0.88
Embed a Cybersecurity Framework into the ITDR program.	4.50	0.76	1.00	0.88
The prepared organization will not rely on one solution to protect everything.	4.63	0.74	0.25	0.88
Companies more heavily invested in preparing for computer crime-based interruptions have greater integration with their Information Security counterparts and have a management team that understands the risks posed by computer crimes and are willing to devote more money and attention to prevention and preparation for computer crime interruptions.	4.38	0.52	1.00	1.00
Organizations that are not prepared to deal with computer crimes in their ITDR are opening themselves up to additional risks, and interruptions caused by computer crimes.	4.38	0.52	1.00	1.00
Organizations cannot treat a computer crimes recovery as just a “technical” or “IT” led the response to better respond to computer crimes.	4.13	0.83	1.25	0.75
Organizations must avoid the knee-jerk reaction to throw money at a problem without first grasping what that problem is and then smartly coming up with the solution.	3.88	1.13	2.00	0.63
Organizations must avoid plans that do not take into consideration the current state of the systems to better respond to computer crimes.	4.13	0.64	0.25	0.88
Organizations that do not conduct lessons learned and root cause analysis will not	4.25	0.71	1.00	0.88

improve to better respond to computer crimes.				
Organizations should avoid placing a low value on quality management in DR to better respond to computer crimes.	3.88	0.64	0.25	0.75
Organizations must avoid architectures that lack redundancy or resiliency attributes to better respond to computer crimes.	4.63	0.74	0.25	0.88
Organizations must avoid thinking they are protected from computer crimes.	4.75	0.71	0.00	0.88
Organizations must avoid neglecting the risk of computer crimes interruptions.	4.50	0.76	1.00	0.88
Organizations must not focus on speed but instead focus on the assessment phase to better respond to computer crimes.	4.13	0.83	1.25	0.75
Organizations must avoid having missing cybersecurity policies to better respond to computer crimes.	3.75	1.28	2.25	0.63
Organizations must avoid operating DR functions without the proper funding to better respond to computer crimes.	4.00	0.76	0.50	0.75
Organizations cannot operate ITDR and InfoSec in different silos to better respond to computer crimes.	4.25	0.89	1.25	0.75
A well-developed cybersecurity framework supports the ITDR, and the opportunity for a technical interruption is reduced.	4.50	0.53	1.00	1.00
A coordinated process alignment between Disaster Recovery and Information Security frameworks is vital to reducing the recovery of this type.	4.75	0.46	0.25	1.00
DR and InfoSec should be aligning their lifecycle processes so that like steps are executed together, and participation is integrated.	4.38	0.74	1.00	0.88
Developing an ITDR set of practices and different playbooks will reduce the response.	3.38	1.19	1.00	0.63
Resilience efforts should be folded into dependency models to reduce the response to this interruption.	4.00	0.53	0.00	0.88

Advanced preparation will reduce a computer crimes response.	4.25	0.89	1.25	0.75
There is not much alignment between DR and InfoSec frameworks, and that is a problem. Create alignment.	4.50	0.76	1.00	0.88
A deep understanding of interdependencies in the IT environment will improve the response to computer crimes.	4.38	0.74	1.00	0.88
A business-focused understanding of the organization will improve the response to computer crimes.	4.38	0.74	1.00	0.88
A risk-based focus on the business will improve the response to computer crimes.	4.63	0.52	1.00	1.00
Technical, analytical, logical, and lateral thinking will improve the response to computer crimes.	4.50	0.53	1.00	1.00
A basic understanding of the layers of protection, prevention, policy management, operations, monitoring, and response will improve computer crimes recovery efforts.	4.25	0.71	1.00	0.88
Cyber Security expertise needs to exist to improve the response to computer crimes.	4.25	0.89	1.25	0.75
Implement Enterprise Security Risk Management (ESRM) in the ITDR process	4.25	0.71	1.00	0.88
Deploy InfoSec training for ITDR teams	4.38	0.52	1.00	1.00
Organizations can integrate the RMO and CSO responsibilities into ITDR planning activities	3.75	0.46	0.25	0.75
Formal lessons learned and future prevention, which may help lessen the severity of future incidents.	3.75	0.71	1.00	0.63
Establishing a baseline of security configurations is another cybersecurity process that extends to ITDR.	3.88	0.83	1.25	0.63
Implement Asset inventory processes	3.25	0.89	1.25	0.50
Deploy Penetration testing and disaster recovery testing	3.75	0.71	1.00	0.63
Implementing the CAG 20 Critical Security controls would improve the recovery effort.	3.88	0.83	1.25	0.63
Organizations should include InfoSec risks in ITDR frameworks	4.50	0.53	1.00	1.00
If done well, clearly following an ESRM program and linking the outcomes of the	4.38	0.74	1.00	0.88

framework to the DR framework offers organizations the ability to see the interdependencies between assets and objectives.				
Without cyber being a part of that plan, the plan itself will be lacking.	3.88	0.99	0.50	0.71
If done properly, cybersecurity risk management will identify the DR systems as one of the most business-critical systems in the organization.	4.00	1.07	1.25	0.75
Integrating some cybersecurity risks and controls in your disaster recovery process may allow it to easier identify attacks that would otherwise be considered a “system malfunction.”	4.38	0.52	1.00	1.00
A cybersecurity framework integration could provide an advantage in that it provides a 2nd or 3rd layer of risk management to the disaster recovery framework.	4.00	0.76	0.50	0.75