Charlotte Community ToolBank

Risk, Response and Recovery Guide

UNC CHARLOTTE
College of Liberal Arts & Sciences

Gerald G. Fox Master of Public Administration

Gricelda de la Cruz
Samuel Hopkins
Cameron Joyce
Megan McClelland
Donna Sofsky
Kelly Weston

Supervised by Dr. James Douglas and Mr. Douglas Bean

Table of Contents

Executive Summary

Overview

Charlotte Community ToolBank (CCTB) is a locally-run affiliate of ToolBank USA, a national nonprofit organization that lends tools and equipment to other nonprofit and charitable organizations. In Fall 2019, CCTB contracted with the Gerald G. Fox Master of Public Administration (MPA) program at the University of North Carolina at Charlotte to develop an emergency planning guide for the organization. The MPA Team conducted a Risk Identification and Assessment to identify and prioritize the threats most likely to have an adverse impact on CCTB.

This report documents the steps involved in preparing the Risk Identification and Assessment and describes potential risks to CCTB. Additionally, the report recommends strategies to mitigate, respond to, and recover from disasters resulting from the identified risks. CCTB can use the report to guide in its planning activities. Other nonprofit organizations should be able to replicate or adapt the processes and strategies documented in the report to meet their planning needs.

Methodology

The MPA Team used various methods to conduct the Risk Identification and Assessment, including:

- Extensive literature review of risk assessments and emergency management best practices
- Interviews with the CCTB Executive Director and other local non-profit officials
- Site visit to CCTB and analysis of current procedures and possible risks
- Qualitative ranking of potential risks on the Risk Assessment Matrix

Key Findings

Through the Risk Identification and Assessment, the MPA Team found 10 potential risks that could threaten CCTB's operations and assets. The MPA Team considered frequency, financial impact, and operational disruption when assessing the likelihood and impact of each risk. Ranked from highest to lowest likelihood, the identified risks are:

1. Power Outage
2. Property Crime
3. Personnel Loss
4. Fire
5. Loss of Space
6. Revenue Loss
7. Severe Weather
8. Workplace Violence
9. Water Intrusion
10. Cybersecurity

The Risk Identification and Assessment also revealed that CCTB is currently using several best practices to mitigate risks. Some of these strategies include:

- Installed security and fire suppression systems
- Safety assessments performed by Charlotte Mecklenburg Police Department and Charlotte Fire Department
- Real-time crime alerts received through mobile devices and email
- Chair of Board of Directors retaining a key to the Executive Director's office
- Annual review of financial reports
- Building's gutters and downspouts cleaned each spring and fall
- Annual roof inspections
- Third-party IT analyst that administers an antivirus program, monitors IT activity, and can troubleshoot or remediate issues as they arise
- Manual offline inventory management process in case of IT shutdown

The MPA Team commends CCTB for taking these steps to protect the organization from various threats and prepare for harmful incidents.

Recommendations-at-a-Glance

Mitigation

For each identified risk, the MPA Team recommends several additional preparedness measures CCTB can implement to augment its mitigation efforts. Examples include:

- Assemble an emergency supply kit
- Conduct fire, hurricane, and tornado drills
- Ensure power poles located on or near the property are visually in good working order and report any problems
- Create and regularly update desk manuals for the Executive Director and Warehouse Coordinator positions
- Diversify revenue sources
- Create contracts, mutual agreements or memorandums of understanding with agencies that have the capacity to hold CCTB's inventory temporarily
- Conduct employee training on cybersecurity

Response

The Response Plan presented in this report lists 12 items to consider when creating a disaster response plan. Reporting, evacuation, employee accountability, and communications are among these considerations.

The Response Plan also lists general guidelines for developing a plan. These steps include creating checklists, summarizing risks, organizing actions, and making the plan accessible.

Recovery

The MPA Team identified four areas of recovery that should serve as the focus of CCTB's recovery activities:

- People
- Money
- Equipment/Inventory
- Building

The Recovery Plan recommends actions for each of these areas to help the organization regroup, restore, and continue serving the community after experiencing a disaster.

Conclusion

CCTB has proven its resilience in handling disasters such as property crime, loss of facilities, revenue loss, and cyberthreats. The recommendations included in this report can enhance the organization's disaster preparedness, response, and recovery capabilities in the future.

Introduction

Charlotte Community ToolBank (CCTB) enlisted the assistance of the Gerald G. Fox Master of Public Administration program at the University of North Carolina at Charlotte in developing an emergency response plan for CCTB and a template to distribute to other members of their national organization and other nonprofits to assist and prepare for potential risks. In response, members of the MPA Team conducted research using government, trade and academic sources.

Based on these sources, the information presented will help the organization determine and mitigate risk, as well as respond to and recover from significant events that would negatively impact personnel, operations, or assets. Mitigation, as described by FEMA is the effort to reduce loss of life and property by lessening the impact of disasters. Specifically, this assessment attempts to identify key risks that would directly affect the organization, determine risk mitigation best practices that are applicable to CCTB's current location, and provide a general framework for response and recovery. Furthermore, pertinent documents, such as templates, checklists, and guidelines for emergency planning, adaptable for use by other small not-for-profit organizations, is included.

This report is divided into five sections:

1. **Charlotte Community ToolBank Profile** provides pertinent background information and descriptions of current operations.
2. The **Risk Assessment Methodology** section describes the methods the MPA Team used to determine those risks considered likely and impactful to CCTB as well as how to mitigate each risk.
3. The **Risk Identification and Assessment** section describes each identified risk relevant to CCTB and the methodology used to assess each specific risk. This section also includes details of CCTB's current risk mitigation efforts.
4. The **Response Plan** section includes guidelines and recommendations on building a response plan for general and specific threats.
5. The **Recovery Plan** section provides an outline of considerations for replacement of resources crucial to the long-term operation of the business.

In addition, **Appendices** include the MPA Team's scope of work (Appendix I), a risk identification, response and recovery template developed for CCTB and similarly-sized organizations and not-for-profits (Appendix II), and a guide from the Colorado Small Business Development Network (Appendix III). Additional supporting documentation is also included in this section. The **References** section lists the sources used and referenced in the report.

Charlotte Community ToolBank Profile

Mission

CCTB is an agency with a mission to provide charitable community-based organizations with the tools, equipment and expertise to help them achieve their most ambitious goals. Its tool lending program provides qualifying organizations with year-round access to tools and equipment for volunteer projects, facility and grounds maintenance, and special events. By providing an inventory of tools and other types of durable assets, CCTB helps to enhance the charitable sector's capacity to serve, facilitating hands-on volunteerism in the greater Charlotte area.

History

CCTB officially opened its doors to the community in March of 2011. The CCTB is the local affiliate of ToolBank USA, the Atlanta-based parent organization of the national network of ToolBanks. ToolBanks in Charlotte, Richmond, Baltimore, Cincinnati, Houston, and Phoenix are modeled after the highly successful Atlanta Community ToolBank, which has served the greater Atlanta's charitable community for more than 27 years. Each ToolBank affiliate is governed by a local Board of Directors. The ToolBank network also includes ToolBank Disaster Services, a program of ToolBank USA, comprised of three mobile trailers which respond to disasters and large-scale volunteer projects throughout the country.

Location

CCTB maintains an 8,000 square-foot warehouse in Charlotte's South End with an inventory comprised of more than 275 different types of tools and equipment in volumes large enough to equip thousands of volunteers at a time. Access to CCTB tools eliminates the need for agencies to incur the expense of purchasing, repairing and storing tools, which reduces costs associated with service projects and allows these agencies to focus crucial resources on their mission.

Tool and Special Event Equipment Lending Program

The heart of CCTB is the tool lending program. Charitable organizations have year-round access to CCTB's inventory of tools and equipment for a nominal fee. CCTB has an extensive inventory of tools and special event equipment that includes common items such as work gloves, shovels and hammers, to more expensive items like tents, projectors, and 5500w/240v generators.

Borrowing tools from CCTB is inexpensive, convenient, and fully functional, which maximizes agencies' ability to improve community engagement and achieve greater impact for those they serve. CCTB tools are only available to member organizations, such as:

- Nonprofit/Charitable/Tax exempt organizations
- Schools and parent-teacher organizations
- Neighborhood associations
- Faith-based groups
- Civic organizations
- Government agencies

Since opening its doors in 2011, CCTB has served more than 600 charitable partners with over $7 million dollars in tools and special event items for their 258,250 volunteers working on 11,190 projects.

Tool Rush Fundraiser

In 2019, CCTB introduced the Tool Rush Program. The Tool Rush is a tool sale open to the public. Through the generous donations of corporate and individual donors, new and gently used tools are sold at a 50% or more discount off retail price. Individuals, organizations, and companies are welcome to purchase.

Hammers & Ales Fundraiser

CCTB has an annual fundraiser that provides approximately 15% of its annual revenue.

Staff

Maureen Krueger, *Executive Director*
Lex Yelerton, *Warehouse Coordinator*

Board Members

Sarah Mitchell Board President *Turner Construction Company*	**Ned Cox** *Sunseeker Power Equipment*	**Merissa Hannah** *Cobra Legal Solution*
Adam Nicholson Board Vice President *Deloitte & Touche LLP*	**Stephanie Dillon** *Community Volunteer*	**Preston Hurrell** *McGuireWoods LLP*
Mike Tropsha Board Secretary *Carolina CAT*	**Tim Dugan** *The Home Depot*	**Thomas Karlsson** *Barringer Construction*
Dan Stewart Board Treasurer *PNC Bank*	**Andrew Foos** *Messer Construction*	**Todd Linerode** *Mears Construction*
Meganne Price *Duke Energy*	**Logan Pavkov** *Atrium Health*	**William Munkres** *Stanley Black & Decker*
Beth Bjorlo *Ingersoll Rand*	**AJ Jobe** *Carolina CAT*	**Allie Alu** *Turner Construction*

Sponsorships account for approximately 70% of CCTB's revenue. Past sponsors include:

TIAA CREF	Turner Construction	Carolina CAT
Duke Energy Progress	Piedmont Natural Gas	Barringer Construction
Rodgers Builders	Deloitte US	Nucor
Messer Construction	Atrium Health	Google Fiber

Risk Assessment Methodology

The MPA Team took the following steps to complete a comprehensive risk assessment for CCTB:

1. Compiled a list of common risks relevant to small businesses and nonprofit organizations such as natural disasters, human-error factors, technology events, and operational risks for further research and risk assessment.
2. Reviewed disaster recovery, risk assessment and emergency management information from the Federal Emergency Management Agency (FEMA), Department of Homeland Security (DHS) at Ready.gov, the American Red Cross, the National Council of Nonprofits, the Council of Foundations, and the Occupational Safety and Health Administration (OSHA) for national relevance.
3. Reviewed disaster recovery, risk assessment and emergency management information from the Charlotte Mecklenburg Emergency Management Office (CMEMO), and North Carolina Emergency Management for local relevance.
4. Performed an extensive literature review on risks with the highest likelihood to occur and have an impact on CCTB. The MPA Team conducted a literature review of emergency management principles and best practices to identify the risks explored in this analysis. This literature review included scholarly journals, local, state and federal government reports, and internet sources. Internet resources came from sites maintained by relevant government agencies, professional organizations, and other experts with extensive knowledge of the risks discussed in this report.
5. Conducted interviews with the Executive Director of CCTB, a representative of the Houston Community ToolBank, an employee of CMEMO and an employee of the Charlotte Fire Department.
6. Made a site visit to CCTB to view and analyze current emergency preparedness and location risk factors.
7. Incorporated benchmark criteria from multiple sources in order to identify the likelihood of each risk occurring at CCTB.
8. Rated likely potential risks with Risk Assessment Matrix.
9. Created a template of the risk assessment process for future use.

Risk Assessment and Benchmarks

After the analysis and risk assessment, the MPA Team identified a wide range of risks that organizations often confront. The MPA Team used information from the interviews and site visit to determine which of these risks are most likely to threaten CCTB (a broader list of potential risks to organizations can be found in Appendix II). The risks most relevant to CCTB are:

- Power Outage
- Property Crime
- Personnel Loss
- Fire
- Loss of Space
- Revenue Loss
- Severe Weather
- Workplace Violence
- Water Intrusion
- Cybersecurity

Each of the risks was rated on likelihood and impact. ***Likelihood*** estimates the likely probability of the potential occurrence for a particular risk. ***Impact*** estimates the likely damage to or loss of equipment or infrastructure, injuries, death, and/or economic damage for a particular risk. Risks were given ratings of **Low**, **Moderate**, or **High**. Tables 1 and 2 provide basic guidelines used by the MPA Team when assigning these risk levels. It is important to note that the rating criteria used in these tables apply generally to most risks but is not conclusive. Each risk comes with unique characteristics that do not always fit neatly within these general criteria. Full analysis and explanations of how the ratings for each risk were derived can be found in the Risk Assessment and Identification section of the report. Readers should also note that the impact ratings are based upon the MPA Team's assessment of the most likely outcome should the event occur. It is always possible that risks could produce impacts of greater or lesser severity.

Table 1: Likelihood Rating

Likelihood Criteria	
High	• Frequent occurrence; greater than 50% chance annually • High local relevance; has happened to CCTB, has occurred in local area • Specific risk(s) not accounted for, mitigation not in place
Moderate	• Moderate frequency; greater than 10%, but less than 50% chance annually • Moderate local relevance; has not happened to CCTB, but has occurred in area • Specific risk(s) accounted for, but mitigation not in place
Low	• Infrequent; less than 10% chance annually • Low local relevance; does not happen near CCTB • Specific risk(s) currently accounted for; mitigation in place

Table 2: Impact Rating

Impact Criteria	
High	• Severe damage; greater than 50% loss annually • Extended downtime; shut down for more than 4 days • Major employee injury or death
Moderate	• Moderate damage; greater than 10%, but less than 50% loss annually • Moderate downtime; business up and running within 2-4 days • Moderate employee injury
Low	• Minor damage; less than 10% loss annually • Little downtime; business up and running in less than 24 hours • Minor or no employee injury

Risk Assessment Matrix

The MPA Team built upon a risk vulnerability and impact assessment scale and matrix from the Colorado Small Business Development Center's *Disaster Recovery and Continuity Guide for Colorado Businesses* (see Appendix III) to develop a Risk Assessment Matrix. The Risk Assessment Matrix (Table 3) plots relevant risks and determines mitigation actions. Its primary value to CCTB is in ranking and prioritizing risks and showing how each risk is rated within each dimension. There are, however, limitations to assessing risk in such a value system. In particular, events that have a low likelihood of occurring that could pose significant risk to CCTB if they occurred may receive high rankings, while events that occur regularly but do not threaten severe, widespread or long-term damage may be ranked lower. Readers should keep those limitations in mind when reviewing assessed risks.

Table 3: Risk Assessment Matrix

	Low Impact	Moderate Impact	High Impact
High Likelihood	Property Crime	Power Outage	
Moderate Likelihood		Loss of Space Revenue Loss Severe Weather Violence Water Intrusion	Personnel Loss
Low Likelihood		Cyber Security	Fire

Risk Identification and Assessment

Organizations are always exposed to risks. For organizations, risks are generally thought of as factors that have the potential to reduce the organization's ability to achieve its goals. In the case of a small non-profit organization such as CCTB, risks can be anything from cyber-attacks to severe weather damage. Not-for-profit organizations are particularly susceptible to risk due to funding and budget constraints and reduced personnel. This is why it is particularly important for small organizations to proactively plan for and mitigate known risks.

The MPA Team identified and analyzed ten potential risks as being of particular concern for CCTB. The remainder of this section provides detailed assessments of these risks. The discussion of each risk is organized in the following manner:

Background
Describes and provides general information about the risk.

Relevance to Charlotte Community ToolBank
Details how each risk pertains to CCTB and provides relevant data to show why the risk is likely to affect and impact CCTB.

Likelihood
Estimates the likely probability of the potential occurrence for a particular risk, relevant to CCTB.

Impact
Estimates the likely damage to or loss of equipment or infrastructure, injuries, death, and/or economic damage for a particular risk, relevant to CCTB.

Mitigation
Describes activities CCTB can do to mitigate the risk. This section is broken into two parts: Current Practices and Other Best Practices. Current practices are activities CCTB is currently engaged in to mitigate risk. Other best practices are additional things the MPA Team identified that CCTB can do to mitigate risk.

Power Outage

High Likelihood | Moderate Impact

Background

A power outage or interruption is the unexpected loss of electrical power or service. Extended outages can impact the community and economy through disruption of communications, water and transportation; retail business, grocery stores, gas stations and similar businesses closures; food spoilage and contamination; and prevent the use of medical devices. According to FEMA, about 70% of businesses in the U.S. will be affected by a power outage within the next 12 months (Department of Homeland Security, 2019). As reported in the 2017 Annual Report, Eaton Power Management Company, which tracks annual blackouts and power outages in the U.S., the average duration of a power outage is 81 minutes nationwide while in North Carolina, the average duration of an outage is 157 minutes. North Carolina comes in at number seven for the greatest number of outages (Eaton, 2017).

Relevance to Charlotte Community ToolBank

Unfortunately, power outages can be costly and long-lasting for businesses. Small nonprofits such as CCTB are especially susceptible. Power outages in the United States are most often caused by: storm- or weather-related events, fallen trees (not associated with weather), vehicular collisions, earthquakes, animals, equipment failure/human error, and high-power demand.

Likelihood

Power outages are measured by the total number of outages, average duration of outages, and the average number of people affected. Further, with each season, the threat of inclement weather changes. Based upon geographical location, observations on site, and statistical data analysis, the causes of power outage most likely to occur at CCTB are:

Storm- or Weather-Related Events

These outages constitute 44% of all power outages and North Carolina's rank in overall outages is consistently in the top ten. In 2017, weather-related outages made up 35% of all power outages in North Carolina (Eaton, 2017).

Fallen Trees (not necessarily due to storms)

North Carolina was ranked in the top ten for outages caused by a fallen tree or limb from 2012-2015 (Eaton, 2015). Based on observations on-site, CCTB has a few trees, but none so big as to pose a major threat.

Vehicular Collisions

North Carolina was ranked in the top ten in overall collisions causing power outages from 2012-2105 (#2 in 2015) (Eaton, 2015). The City of Charlotte has mostly exterior overhead power lines and CCTB is located on a busy, main artery into uptown Charlotte.

Equipment Failure/Human Error

North Carolina was ranked in the top ten for outages caused by an equipment failure or human error from 2012-2015, constituting ⅓ of all outages (Eaton, 2015).

These four interruptions makeup over 40% of all power outages (Eaton, 2012, 2015) and often occur simultaneously or as a result of each other. Based upon state rankings, statistics, and on-site observations, **the MPA Team has rated the likelihood of a power outage as High.**

Impact

The impact of power outage or loss depends on the cause of the outage, duration of outage, and any damage or loss incurred while the power is out, which could be minimal or catastrophic. Accordingly, the impact from power outages is more likely to affect CCTB because of the higher than national average of duration of an outage and data from the City of Charlotte and Mecklenburg County notes that inclement weather has the greatest impact on local businesses. The impact of an outage caused by any means could mean significant downtime and financial or inventory loss for CCTB and **as a result, the MPA Team has rated the impact of power outage as Moderate.**

Mitigation

Current Practices. CCTB is well-prepared for a Low to Moderate impact power outage. They have access to first alert systems and emergency items like generators and flashlights, on-site. Businesses can internally prepare only so much for these kinds of outages. Due to the nature of its business, CCTB maintains multiple portable generators on-site which could be used in case of an emergency.

Other Best Practices. The MPA Team identified additional best practices in the literature that CCTB can follow to reduce the impact of prolonged power loss.

Back-up Power

In any storm- or weather-related event, it is necessary to have a backup power system available. Given the average number and duration of power outage, service may be off for some time. CCTB should monitor inventory and keep generators on hand if severe weather is forecasted.

General Preparedness

No matter the cause of the power outage, there are general preparedness tips that are essential to protect people and assets during an outage. These best practices from FEMA (2019b) include:

- Create an emergency kit including water, flashlights and batteries
- Develop a plan to turn off or disconnect equipment, electronics or appliances in the face of impending severe weather (including restart when power is restored)
- Install and maintain emergency lighting, surge protectors and exit signs
- Train staff on emergency and safety procedures and conduct practice drills
- Keep hard copies of all emergency plans in a central location

Power Outage Toolkit

Information and planning assistance provided by the Department of Homeland Security (2019) at Ready.gov gives best practice advice and procedures for power outages including the Ready Business Power Outage Toolkit. This planning packet has table templates to store all pertinent information for a power-related outage or emergency.

Property Crime

High Likelihood | Low Impact

Background

Property crime is identified as arson, burglary, larceny theft, and motor vehicle theft (Crime Data Explorer, n.d.). In 2017, property crimes resulted in an estimated $15.3 billion loss nationwide (Federal Bureau of Investigation [FBI], 2018). The general effects of property crime can go beyond the direct cost of property loss but can also generate a climate of fear and anxiety that can affect organizational performance (Gibbons, 2004).

Relevance to Charlotte Community ToolBank

At CCTB, the impact of property crime varies based on the type of crime. The major variation is dependent on the cost of replacing items such as office equipment, tools, or repairing building damage. Regular crime incidents could result in unforeseen or unbudgeted costs for CCTB if the agency regularly needs to replace stolen items or repair damages due to vandalism.

Likelihood

CrimeMapping (n.d.) provides property crime data for a 30-day period within a two-mile radius of CCTB's location. The data for October 2019 are listed in Table 4. During this timeframe, a total of 224 records of property crime were reported. The data show that larceny is the most prevalent property crime threat in the area immediately surrounding CCTB, whereas arson is unlikely. Overall, CCTB finds itself in a neighborhood with an above average property crime rate. The Quality of Life Explorer, a neighborhood data tool provided by the City of Charlotte Housing and Neighborhood Services, shows the neighborhood profile area where CCTB is located experiences approximately 35.6 reported property crimes per 1,000 residents, which is higher than the County average of 33.4 crimes per 1,000 residents annually (Charlotte/Mecklenburg Quality of Life Explorer, 2018).

Table 4: Crime Mapping within a 30-day period

Crime Statistics from 10/01/2019 – 11/01/2019

Crime Category	Total Crime Reports
Arson	0
Burglary – Commercial	21
Larceny – Theft Total	191
Vehicle Theft Total	12

CCTB has experienced two incidents of property crime in the last five years; an attempted break-in and theft from a vehicle. The MPA Team, therefore estimates that there is a greater than 50% chance that CCTB will experience a property crime event on an annual basis. **As a result, the MPA Team has rated the likelihood of property crime as High.**

Impact

The impact of property crime depends on the type of crime that occurs and the damage incurred. Larceny accounted for the majority of crimes reported and the FBI estimates the average value of the property taken during larceny thefts was approximately $1,007 per incident in 2017 (Federal Bureau of Investigation, 2018). Burglary was the second-highest category in the area. The FBI estimates the average dollar loss per burglary incident was approximately $2,416 in 2017. The data show that these are the most likely events to threaten CCTB. Because such events tend to result in losses of less than 10% of CCTB's annual budget**, the MPA Team has rated the impact of property crime as Low**.

Mitigation

Current Practices. CCTB has employed the following security measures and practices for mitigating property crime:

- Installed security systems
- Charlotte Mecklenburg Police Department (CMPD) completed a walk-through of the facility, providing recommendations for the CCTB to implement to deter crime
- Front entrance doors remain locked at all times

Other Best Practices. The MPA Team identified several additional best practices in the literature and recommends that CCTB take these additional steps to decrease both the likelihood and impact of property crime.

Secure Access to Property

CMPD and FEMA recommend that business owners identify areas of easy access, open gates, or shared space, and utilize additional preventative measures. The Houston Police Department (2019) offers additional steps to help reduce vulnerability to crime on commercial property including updated locks and ample outdoor lighting. CCTB should identify methods to secure more expensive tools or office equipment. Further, CCTB should consider relocating items that an intruder could use to gain access into the building, such as ladders, tables, or chairs. CMPD (2018) suggests businesses provide employees with a place to adequately secure personal items during work hours. Additionally, staff should avoid leaving items in easy view within their vehicles.

Business Watch Program

The National Crime Prevention Council (NCPC) (2017) suggests Business Watch Programs as a strategy to prevent and reduce opportunities for crime. Business Watch is a neighborhood watch program for commercial areas that help reduce many types of crimes including theft, burglary, and vandalism. For example, since the Detroit Police Department (DPD) implemented

the Business Watch Program, the department has seen reduced crime rates in Business Watch areas (National Neighborhood Watch, 2019). A Business Watch would help CCTB continue to develop a good working relationship with local law enforcement while offering staff training through the police department (National Neighborhood Watch, 2019). Considering the Executive Director has a good relationship with the police officers in the area, this might be a viable mitigation step that could benefit the entire community.

Identify Temporary Agencies to Aid with Stolen Inventory

Wayland (2015) recommends identifying community organizations that can provide assistance in the event of theft. CCTB could develop partnerships and memorandums of understanding with such organizations to provide access to tools and other equipment on a short-term, as-needed basis in the event that inventory is stolen.

Personnel Loss

Moderate Likelihood | High Impact

Background

An organization's staff is one of its strongest and most valuable assets. In many nonprofits that operate with a small team of key personnel, employees play multiple roles. Suddenly losing one of these employees could create major disruptions for an organization. According to the Society for Human Resource Management (Allen, 2008), replacing a lost employee can cost an organization 50-60% of the employee's salary. This cost can be significant for small nonprofit organizations.

Relevance to Charlotte Community ToolBank

CCTB has two employees, so personnel loss is a concern. Both the Warehouse Coordinator and Executive Director provide critical support to the organization. The sudden absence of one or both employees would reduce CCTB's capacity to serve its member agencies.

Likelihood

At CCTB, one of the organization's two employees could be forced to take an extended leave of absence due to illness or injury. The untimely death of an employee is another occurrence that could leave the organization short-staffed and incurring related costs associated with recruitment, onboarding, and the loss of institutional knowledge (Byerly, 2012, p.42). According to the Nonprofit Employment Practices Survey, the overall turnover rate in the nonprofit sector is 19% (Nonprofit HR, 2016). This rate is higher than the average turnover rate across all employment sectors, which is 3.8% (Bureau of Labor Statistics, 2019). **Because of the turnover rate for nonprofit organizations**, **the MPA Team assigned personnel loss a likelihood rating of Moderate.**

Impact

The Warehouse Coordinator assists with the lending program, maintains the organization's extensive inventory, and oversees general warehouse operations (Charlotte Community ToolBank, 2018). His sudden absence could cause tool lending delays as the Executive Director may be forced to juggle this role along with her other duties. The Executive Director manages CCTB's daily operations, major business functions, development efforts, and Board activity. Her sudden absence would have an impact on the overall management of the organization and interaction with stakeholders. Without her fundraising efforts, Board engagement, donor relations, and partnerships with other community organizations would suffer.

As researchers have noted, a nonprofit executive's departure can create organizational instability and uncertainty (Gibelman and Gelman, 2002, p. 66). CCTB's small staff and potential loss of expertise and social capital resulting from the Executive Director's sudden absence could lead to several days of extended downtime. **Considering these factors, the MPA Team assigned personnel loss an impact rating of High.**

Mitigation

Current Practices. CCTB already uses some best practices to minimize the impact of personnel loss. Currently, the Chair of the Board of Directors has a key to the Executive Director's office. In the past, the individual in this position has served as Interim Executive Director, a recommended practice (Federal Reserve Bank of Kansas City, n.d.). CCTB also has a committee structure it can initiate to lead the organization if the interim period between Executive Directors must be extended. Additionally, the current Executive Director explained that staff at ToolBank USA and other affiliates can serve as her backups when needed.

Other Best Practices. The MPA Team identified additional best practices in the literature that CCTB can follow to reduce the impact of losing an employee even further.

Develop a Succession Plan

Human resource organizations such as the Society for Human Resource Management (Day, 2007) and the U.S. Office of Personnel Management (n.d.) consider succession planning a best practice for managing personnel loss at any level. A succession plan outlines the steps for identifying employee replacements with limited disruption to business operations (Day, 2007). In addition to guiding the process for finding a new leader, creating a formal succession plan can prompt a review of leadership structures and job responsibilities (Federal Reserve Bank of Kansas City, n.d.). Research suggests an effective succession plan consists of four elements: leadership development, organizational assessment, a clear vision of the organization's direction, and strategies that align with organizational goals (Gothard and Austin, 2013, p. 276).

CCTB has expressed interest in working with its Board of Directors to develop a succession plan. As an initial step, the organization can create an emergency succession plan to manage the Executive Director's unexpected absence. The plan should include guidelines for convening an emergency Board of Directors' meeting. The Board should use the meeting to select a spokesperson, create a plan for communicating with stakeholders, identify an interim Executive Director, decide on a process for hiring the next Executive Director, and form a task force to lead the hiring process (Federal Reserve Bank of Kansas City, n.d.).

Train the Board Chair in the Executive Director's Responsibilities

If the organization decides to designate interim duties as an official Chair responsibility, the Executive Director should always provide basic training to the Chair as soon as that individual is elected to office. This training could be part of an orientation program that educates Board members on their roles and responsibilities (National Council of Nonprofits, 2019).

Create and Regularly Update Desk Manuals for Each Staff Position

As the Federal Reserve Bank of Kansas City (n.d.) recommends, the Executive Director and Warehouse Coordinator can create and regularly update desk manuals for their positions. The manuals should include login credentials, contact lists, a job description, and instructions for essential functions and tasks (Federal Reserve Bank of Kansas City, n.d.). To preserve CCTB's

social capital, the Executive Director's manual should also contain a description of relationships with key stakeholders and suggested strategies for continuing to nurture those relationships.

Fire

Low Likelihood High Impact

Background

Fires in the United States have serious consequences due to injury, substantial property damage, and death (Charlotte/Mecklenburg Quality of Life Explorer, 2018). According to the U.S. Fire Administration (USFA, 2019), nonresidential building fires in the U.S. showed a 20% increase in the overall trend during a ten-year period from 2008 to 2017. Nationwide, 105 civilians died in nonresidential structure fires, a decrease of 30% from the year before (NFPA, 2019). Additionally, 1,250 civilians were injured in nonresidential structure fires in 2017, a decrease of 24% from the year before (Evarts, 2018). With appropriate education and attention, fire incidents could be largely prevented (Charlotte/Mecklenburg Quality of Life Explorer, 2018).

Relevance to Charlotte Community ToolBank

At CCTB, the significance of fire is important because fires could easily spread and cause significant damage. A single fire damaging the property or equipment could severely impact business operations for CCTB. Without tools and equipment available to lend, community agencies would also be impacted.

Likelihood

Fire incidents are relatively low in the area surrounding the CCTB facility. According to the Quality of Life Explorer (2018), the neighborhood profile area where CCTB is located experienced a total of 21.7 fire calls per 1,000 people in 2018. This is a decrease from the previous year's, 26.3 fire calls per 1,000, and lower than Mecklenburg County's average of 33.2 fire calls per 1,000 people (Charlotte/Mecklenburg Quality of Life Explorer, 2018).

CCTB has a fire suppression system in place and has had no reported fire incidents. As a result of the low incident rate of fires in CCTB's neighborhood combined with the facility's fire suppression system **the MPA Team assigned a Low rating for likelihood of fire**.

Impact

The National Fire Protection Association (NFPA) (2019) reported that commercial or business properties averaged $46,000 in losses per fire annually in the United States. Additionally, according to the U.S. Fire Administration (2019), North Carolina reported 2.0 deaths per 1,000 fires in 2017, which was below the national average of 2.3 deaths per 1,000 fires. In North Carolina, an average of 9.7 injuries occurred per 1,000 fires (United State Fire Administration, 2019). Since January 2019, Mecklenburg County has had nine deaths, reported by the Office of State Fire Marshal (North Carolina Department of Insurance, 2019). The cost to replace or repair damage to property could be considerable, however, the fire sprinkler system installed in the CCTB facility decreases the likelihood of large-scale loss (it is important to note that water damage due to activation of the sprinkler system could occur in the event of a fire). **Based on these factors, the MPA Team assigned fire a High impact rating.**

Mitigation

Current Practices. CCTB follows best practices for mitigating the risk of fire, recommended by the Charlotte Fire Department (CFD) (n.d) and the Federal Emergency Management Agency (FEMA), that of using a fire suppression sprinkler system including smoke detectors and smoke alarms.

Other Best Practices. The MPA Team identified several additional best practices in the literature that can be used by CCTB to further mitigate the threat of fire.

Proper Education and Attention

FEMA recommends establishing emergency plans, policies, and procedures as well as written plans for evacuation as low-cost measures. Plans should identify all critical resources including the nearest hospitals and fire and police stations. After written plans are created, the CCTB should conduct fire drills on a regular basis (Department of Homeland Security, n.d.b).

The current electrical system was installed by the previous owner and may need attention for safety. Poor electrical wiring or cable insulation could produce an electrical fire (FEMA, 2019a). The fire suppression sprinkler system will reduce the risk of injury or death if caused by the current exposed electrical wiring (FEMA, 2019a) but CCTB should contact a professional electrician for an electrical safety inspection of the building.

Loss of Space

Moderate Likelihood | Moderate Impact

Background

Loss of space occurs when access to the place of business has ended through mutual agreement, breach of contract, or uninhabitability of space. Rental price increases, changes in ownership, expiration of a lease agreement, catastrophic property damage, eminent domain, or foreclosure can lead to a disruption in operations.

Relevance to Charlotte Community ToolBank

Currently CCTB rents its building, creating some potential for loss of space. Without an adequate plan in place to relocate its operations, there could be a delay in services as the organization searches for and relocates to another facility.

Likelihood

In the SouthEnd Development Report, Charlotte Center City Partners (2018) found that more than half of all new residential construction is within three miles of the city's center and notes that at this time, almost two and a half million square feet in office and retail space is either planned or under construction in the area. CCTB's warehouse is in close proximity to Uptown and is therefore a prime location for future development.

In the past, CCTB was forced to relocate to its current location due to lease termination. The current lease agreement is effective until August 2021. If the property were sold, the lease's buy-out clause gives CCTB a six-month notification. In an interview with the Executive Director, she indicated that the relationship with the landlord is good and she does not anticipate a change in the lease arrangement. It is likely that this relationship offsets any immediate risk posed by future development of the site. **As a result, the MPA Team rates the likelihood for loss of space as Moderate.**

Impact

CCTB has access to a large box truck and can enlist volunteers to help relocate inventory and assets in the event of a loss. Thus, the cost of relocating operations and assets to a similar location is estimated at less than 10% of revenue and to last between one to four days. **As a result, the MPA Team assigned loss of space an impact rating of Moderate.**

Mitigation

Current Practices. If the organization were forced to relocate, CCTB maintains contacts in the local commercial real estate market who could assist in finding a new location.

Other Best Practices. According to *Negotiate the Best Lease for your Business* (Portman & Steingold, 2005), the following practices are recommended to maintain the lease agreement and to prepare for the possibility of relocating operations.

<u>Know the Terms of the Lease</u>

Abiding by the terms of a lease ensures that there is no breach of contract and provides clarity about the expectation of performance for both tenant and landlord. When considering moving to

a new location, lease terms contain information on renewal, buy-out and subletting options that may affect the timing of the move (Portman & Steingold, 2005).

Create a Needs Checklist

Business needs dictate location and facility characteristics. An assessment of current and future needs should be made in advance. Creating a checklist listing location, security system and access, minimum square footage, and budget requirements are some aspects that should be thought out ahead of time before a move becomes necessary.

Special consideration should be given to locating in an area outside a zone prone to flooding and other risks associated with the location and type of facility. Crime statistics, signs of building damage, environmental concerns associated with previous use of the building, zoning, permits, and sign ordinances should also be considered (Portman & Steingold, 2005).

If CCTB's facility were damaged or found uninhabitable, a prior arrangement with another organization to share space until normal operations can resume or another arrangement can be made is highly recommended (Robinson, 2003).

Create a Memorandum of Understanding with Partner Organizations

Establish a written agreement or memorandum of understanding between organizations to indicate description, limitations, and use of space. Insurance requirements and coverage should be considered as well as rules pertaining to the space, equipment and internet use, and safety procedures (Herman, n.d.).

Revenue Loss

Moderate Likelihood | Moderate Impact

Background

Revenue loss is defined as the loss of a key funding source. Non Profit organizations that do not have a fee-for-service funding model which fully funds the organization must rely on various funding sources to provide their products and services. Potential funding sources include fees for goods and services, individual donations and major gifts, bequests, corporate contributions, foundation grants, government grants and contracts, interest from investments, loans and program-related investments (PRI), tax revenue, membership dues and fees, or various other models of funding (Ibrisevic, 2018).

Relevance to Charlotte Community ToolBank

Organizations that are overly dependent on one form of funding are considered to have a higher risk of failure than organizations with “mixed funding,” defined as multiple revenue streams to support the operation of the organization. Therefore, finding the best mix of resources is key to ensuring sustainability (Kim, Perreault, & Foster, 2011). A review of the revenue of an organization can determine the funding mix and dependency of the organization on a single source. A general rule of thumb in the nonprofit industry is to ensure that no single funding source makes up more than 30% of the organization's revenue (Renz & Herman, 2016).

Likelihood

CCTB’s total revenue for 2017 was $198,071 and its expenses were $163,366. CCTB claims $231,603 in current assets with no outstanding liabilities. The organization maintains healthy financial stability and does not show financial risk in its public disclosures. The total contribution to CCTB was $140,212, of which a net of $21,307 came from its annual fundraising efforts. The program service revenue was $28,434. Table 5 illustrates the revenue for 2017. The organization currently receives no grants from local, state, or federal government. More than 30% of the revenue comes from donations, which does indicate a potential higher risk. The Executive Director of CCTB expressed confidence that revenues from donations are stable over time. **The risk of funding loss was set as a Moderate likelihood.**

Table 5: Charlotte Community Toolbank 2017 Revenue Chart

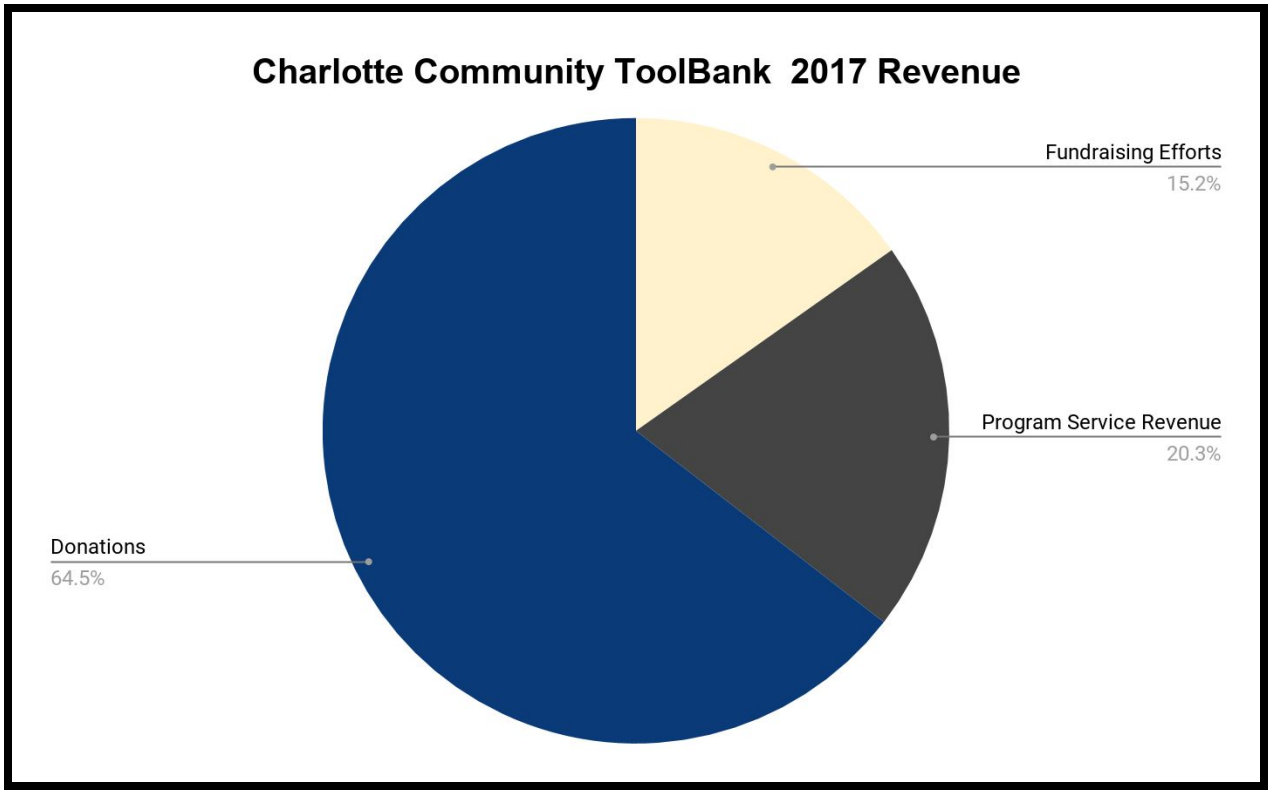


Table 5

Impact

CCTB's current funding is strong for its size and operation. Financial records show that there is an adequate mix of funding from donations and fundraising. Also, CCTB has experience overcoming the loss of a key revenue source in the past when two major donors merged and the organization was given short notice that a large revenue source would be ending. The Executive Director and Board of Directors worked successfully to find an alternative source of revenue to replace the lost revenue source, showing resilience and giving the organization experience with this risk. For these reasons, **the impact of revenue loss was set at Moderate impact**.

Mitigation

Current Practices. CCTB follows these best practices that address the risk of revenue loss:

- Annual review of financial documents, including revenue sources.
- Holding three months of operational funding in cash reserves to prepare for a potential financial crisis.

Other Best Practices. CCTB would benefit from following the following practices from the field:

- Ensure that no single funding source makes up more than 30% of the organization's revenue (Renz & Herman, 2016). The fund distribution was not provided to the MPA Team and should be reviewed by CCTB to ensure that they meet this threshold.
- Analyze historical data to get a clear picture of current and future revenue streams.

- Expand or increase reserve funds to be held in a restricted reserve fund.
- Create guiding documents to implement specific actions during a financial crisis. These actions can include a reduction of staff or services that might be necessary to overcome a financial shortfall (Kim, Perreault, & Foster, 2011).

Severe Weather

Moderate Likelihood **Moderate Impact**

Background

Unlike other natural disasters such as earthquakes and wildfires, severe weather is often forecasted. Despite forecasts and the lead time afforded for planning, weather conditions are subject to change. For this reason, it is necessary to remain prepared for potential severe weather that can affect a community's transportation and utilities systems for several days. Some of the severe weather events that occur most frequently in North Carolina include hurricanes, tornadoes, severe thunderstorms, and winter storms (Charlotte Mecklenburg Emergency Management [CMEMO], 2015).

Wind Damage

One source of wind damage is a hurricane: a rotating, low-pressure storm system with winds in excess of 74 miles per hour (National Ocean Service, n.d.). There are multiple hazards associated with hurricanes, including heavy rainfall, inland flooding, high winds, and tornadoes (National Hurricane Center, n.d.). These hazards can damage buildings, roadways and public infrastructure; cause power outages; and lead to personal injuries and deaths.

Tornadoes are a second source of wind damage. A tornado is a rotating funnel of air that can produce wind speeds of over 200 mph and, according to the National Weather Service, is one of the most destructive atmospheric phenomena (2009).

Winter Storms

North Carolina's winter storms often feature multiple types of precipitation, including snow, sleet, and freezing rain (North Carolina Climate Office, n.d.b).

Relevance to Charlotte Community ToolBank

The high-speed winds of a hurricane, tornado, or severe thunderstorm could uproot some of the trees lining the back and side of CCTB's lot. Depending on how the trees fall, they could damage the building's roof, the fencing along the perimeter of the property, or the organization's trucks. Flying debris could also cause property damage. Because CCTB is not located in a floodplain, it is unlikely the heavy rains associated with a hurricane, tornado, or severe thunderstorm could cause flooding on the property. There is, however, the potential that rainwater could enter the building if a storm damages the roof or front doors. This water intrusion could damage the tools stored in the warehouse. Since all of CCTB's tools are insured, however, the financial impact should be minimal. CCTB could experience an operational impact if the inventory is damaged, leaving the organization without enough tools to fulfill clients' lending requests.

Flooding in major roadways as the result of a hurricane, tornado, or severe thunderstorm could make it impossible for staff and clients to travel to the CCTB. If the facility is inaccessible and

unable to provide its services to the community, it would have to temporarily suspend its operations.

Heavy snow accumulations could cause damage to CCTB's roof. Ice on tree limbs could result in power outages to the facility. Ice on roadways can create hazardous driving conditions. As a result, CCTB may be forced to suspend its operations and delay service delivery during and in the days after a winter storm.

Likelihood

According to the North Carolina Department of Public Safety, the state's annual probability of experiencing a hurricane is between 33.4 and 66.6 percent (2018, p. 3-33). Charlotte is located roughly 200 miles from the coast, but has experienced the devastating effects of major hurricanes in the past. In 1989, the powerful Hurricane Hugo struck the city with damaging 87 mile per hour wind gusts and heavy rainfall (CMEMO, 2015). Between 2000 and 2018, 48 hurricanes and tropical storms affected North Carolina (North Carolina Climate Office, n.d.a). This count includes Hurricane Michael in 2018, which caused massive power outages across Mecklenburg County, as well as flooding and downed trees that resulted in road closures in parts of Charlotte.

Although North Carolina is not located within the U.S.'s principal tornado area, the state experiences an average of 31 tornadoes annually (National Oceanic and Atmospheric Administration, n.d.). In 2012, an EF-2 tornado with 130 mph winds struck Mecklenburg County, damaging 132 homes. This tornado was the result of low-level storm systems that are difficult for the National Weather Service to predict (Lyttle, Penland, & Cooke, 2012).

Between 2000 and 2018, there were four presidential disaster declarations for winter weather events in North Carolina (North Carolina Department of Public Safety, 2018). Mecklenburg County was affected by 77 winter weather events between 1996 and 2017 (North Carolina Department of Public Safety, 2018).

These data and records of past occurrences suggest severe weather meets the criteria for a Moderate annual frequency as shown in Table 1. Additionally, tornadoes can occur anywhere at any time of year, following an unpredictable path (National Weather Service, 2009). In Mecklenburg County, the annual probability of a tornado occurrence is 41% (CMEMO, 2015). CMEMO projects that high winds from storms passing through the Atlantic will also remain a threat for Charlotte in the future (2015). Winter storms will continue to occur, though local officials predict they will produce small amounts of wintry precipitation (CMEMO, 2015). **As a result, the MPA Team assigned severe weather a likelihood rating of Moderate.**

Impact

The potential for weather-related property damage could be severe. Both Hurricane Hugo and a 2002 ice storm caused road closures and millions of dollars in property damage in Charlotte (CMEMO, 2015). These events also caused massive power outages, leaving parts of the city without electricity for more than two weeks (CMEMO, 2015). This history suggests that future

severe weather events could disrupt CCTB's operations for two to four days. **Based on these factors, the MPA Team assigned severe weather an impact rating of Moderate.**

Mitigation

Current Practices. CCTB recognizes that preparation can help reduce the impact of a severe weather event. As FEMA recommends, the organization cleans the building's gutters and downspouts each spring and fall to minimize damage from heavy rains (2017a).

Other Best Practices. There are other best practices CCTB can follow to prepare for any type of severe weather.

Create a Crisis Communications Plan

The Department of Homeland Security (n.d.b) recommends creating a crisis communications plan to communicate with staff and other stakeholders during and after a weather emergency. The first step in the plan should be to identify and collect contact information for the audiences the organization must reach (Department of Homeland Security [DHS], n.d.b). For CCTB, that step will involve compiling phone numbers and email addresses for staff, Board Members, agency clients, volunteers, donors, ToolBank USA and affiliates, local partners, landlord, utility providers, insurance company, and IT contractor.

A second suggested step in the crisis communications plan is to redirect incoming phone calls to maintain contact with clients (DHS, n.d.b.). CCTB can forward the organization's phone calls to ToolBank USA or one of its affiliates.

Another recommended step in the crisis communications plan is to provide updates regarding the organization's operational status online (DHS, n.d.b.). CCTB can develop a dark site to replace the organization's website temporarily. The organization can also draft messages for its social media platforms to keep followers updated on changes to CCTB's operations or location during and immediately after a severe weather event. The dark site and social media posts can contain similar messages.

Shelter-In-Place

FEMA (2018a) recommends sheltering-in-place during hurricanes and tornadoes, and advises that a small, interior room without windows will provide the best protection against a storm. For this reason, CCTB should designate the restroom as the safe room for gathering during a hurricane or tornado. There should also be an emergency supply kit available. FEMA (2014a) advises stocking the kit with blankets, drinking water, non-perishable food, flashlights, first aid supplies, a whistle, and dust masks.

Conduct Severe Weather Preparedness Training

DHS (n.d.c.) and the National Weather Service (2009) suggest that businesses conduct training exercises to prepare for severe weather. There are two types of preparation exercises CCTB should conduct with staff, Board Members, and volunteers, and remote participation from

ToolBank USA affiliates. The first type is a hurricane or tornado drill. The second type is a tabletop exercise designed by FEMA to simulate a hurricane, tornado, or winter storm and the appropriate response scenario for each event.

Prepare the Property for Severe Weather

In advance of an approaching winter storm, staff should apply a de-icing agent to the parking lot, front steps, driveways, and other paved areas on the property to make them safe for walking (FEMA, 2017a). Staff should also move shopping carts and other items stored outside to a location inside the warehouse.

Identify a Temporary Operations Location

Additionally, staff should identify a partner organization that will allow CCTB to use its facility as a temporary location in the event the building is severely damaged or inaccessible. Neighboring nonprofit Beds for Kids may be able to provide CCTB with temporary storage space if the warehouse is damaged and the organization is in need of a safe place to store some of its inventory.

Monitor Weather Conditions

When severe weather warnings and watches are in effect, CCTB should closely monitor weather conditions using a weather app on a mobile device or a National Oceanic and Atmospheric Administration weather radio (FEMA, 2014a).

Workplace Violence

Moderate Likelihood | Moderate Impact

Background

Workplace violence is defined as any act or threat of violence, ranging from verbal abuse to physical violence directed toward persons at work or on duty (National Institute of Occupational Safety and Health, 2018). Violence may occur from within the workplace by a disgruntled or mentally unstable employee. Violence can also spill over from outside the organization through community violence or from targeted violence by an unknown outside source. Gun violence is a growing threat in the United States and the gun death rate in the U.S. is much higher than in other industrialized countries (Gramlich, 2019). In 2016, NC gun violence reached the highest levels in the past 35 years; and at 57 homicides in 2019, Charlotte is on track for its deadliest year since the highest recorded year for gun violence in 1993 (Wester, 2019).

Relevance to Charlotte Community ToolBank

Workplace violence threatens the life and well-being of employees and volunteers. Furthermore, violence threatens the reputation of an organization that is not prepared for an incident of violence and responds inappropriately to acts of violence. Organizations that experience violence can lose employee morale.

Likelihood

The risk of workplace violence is measured by the crime statistics recorded by local law enforcement made accessible to the public online through CrimeMapping. This information can be compared to local, state, and national incidents to assess the relative level of crime in a neighborhood. The CCTB warehouse is located in an area where violent crime is above the city's average. Crime statistics show that in the 180 days before September 12, 2019, there were 2 homicides, 21 firearm violations, and 524 recorded assaults within a 2-mile radius of CCTB (CrimeMapping, n.d.). Thus, there is the possibility that violence could spillover from the surrounding community onto the CCTB facility. **The likelihood of violence occurring at CCTB is rated as Moderate because of these factors.**

Impact

Violent actions can negatively impact an organization via psychological issues, physical injury, or even death. In 2016, approximately 16,890 workers in U.S. private industry experienced trauma from nonfatal workplace violence that kept the employees from returning to work and another 500 employees were a victim to workplace homicide (Centers for Disease Control, 2018). Workplace violence threatens the life and well-being of employees and volunteers. Furthermore, violence threatens the reputation of an organization that is not prepared for an incident of violence and responds inappropriately to acts of violence. Employee morale and funding are likely to be affected after an occurrence of workplace violence (Coombs, 2007). **The MPA Team rated the potential impact of workplace violence at CCTB as Moderate.**

Mitigation

Current Practices. Preparation and training to potential violence is the primary mitigating factor to avoid the negative impacts of this risk. CCTB currently has the following best practices in place:

Real-time warning mechanism

The Executive Director receives local crime alerts through her digital devices and email. There is a communication plan to alert staff and volunteers of threats.

Safety Training / Emergency response plan

CCTB staff is trained to maintain vigilance and are prepared for threats to the staff or facility. There is an emergency response plan that establishes an off-site safety zone for emergencies in the warehouse. This plan is introduced to staff and volunteers during onboarding.

Other Best Practices. National best practices to mitigate workplace violence also include the following:

No Tolerance Policy

The Occupational Safety and Health Administration (OSHA) (2015) provides best practices to address potential internal workplace violence. OSHA encourages establishing a strong Human Resource “no tolerance” policy to ensure any act of violence is immediately reported to executive management and HR for follow up and review. There should be a documentation process of internal acts of violence and the subsequent removal of potentially violent staff or volunteers to help mitigate this risk (OSHA, 2015).

However, for the volunteers that enter the organization, there is little to no process available to efficiently determine the possible risk of workplace violence from these individuals. Volunteer onboarding should include a way for volunteers to alert the Executive Director or Board of acts of violence or intimidation that could be a red flag for a potential threat of violence. A “no tolerance” policy should cover and apply to CCTB volunteers and can be integrated in the waiver for volunteers to review and sign.

“Hide, Run, Fight” Training

CCTB should also reference the national safety guidelines from the Department of Homeland Security (2019) for gun violence. “Hide, Run, Fight.” trains staff and volunteers to react to gun violence in a three-tiered approach. First, safely secure oneself in a place hidden from the shooters’ view and bunkered if possible by securing doors and windows while waiting for authorities to release you from the location. The next step is to run for safety with hands up, if there is no possibility of hiding in place or the gunman penetrates your location. Finally, if there is no other option, engaging a shooter with any potential weapon with the intent to disarm or remove the threat. These guidelines can be reviewed with staff and volunteers during the onboarding process (Department of Homeland Security, n.d.c).

Enhanced Warning Signals

CCTB could install an audible warning signal that can be activated by staff during a threat to alert staff and volunteers to seek shelter and alerts local authorities of an emergency (Occupational Safety and Health Administration, 2001).

Continuous Factual Communication

Mirza (2012) noted that communication is critical during an incident of violence. A point person should be established to share information within the organization to alert anyone that might have been impacted. It is also important to communicate with stakeholders to ensure that they are up to date with accurate information (Mirza, 2012). This can be provided through the intranet, hotline, or direct email or phone calls. CCTB should also assign a media contact who is trained or experienced in public communication. Social media posts and statements from the organization help to address any confusion or chaos that might ensue during an act of violence. These statements should be brief and only give the facts of the incident.

TOOL RUSH

Water Intrusion

Moderate Likelihood | Moderate Impact

Background

Water intrusion may result from a number of causes such as floods, prolonged rain, snow melt, blocked storm drains, faulty plumbing, and sewer line backups. Verisk Analytics ISO unit (a leading data analytics provider serving customers in the insurance service industry) reported that water intrusion and damage claims in the United States increased significantly between 2013 and 2017 and caused $13 billion in damage claims for insurance companies (Scism, 2019).

Relevance to Charlotte Community ToolBank

Water intrusion may damage or destroy motorized tool inventory, as well as electronic and computer equipment resulting in the replacement of high-dollar inventory items, such as generators and IT hardware. Water damage to IT infrastructure and crucial inventory may limit CCTB's response and service to local agencies reliant on CCTB's Tool Lending Program.

Likelihood

The CCTB facility does not lie within a floodplain, an indication that the risk of flood damage is low (FEMA, (2017b). The Hartford, a Connecticut-based property and casualty insurer, issued a report on damage claims made from 2009 to 2015. Weather-related damage from rain and melting snow accounted for 11% of insurance claims and plumbing and appliance failure accounted for 19% of claims (Bronson, 2016). **The risk of water intrusion is assessed as a Moderate likelihood.**

Impact

Water damage restoration costs range widely based on the water source. Water damage from a broken water pipe costs less to remediate than water damage resulting from a sewage backup. According to Home Advisor, a digital marketplace that provides average project and service costs to consumers CCTB could sustain damages between $14,000 to $28,000 (HomeAdvisor.com, n.d.). Based on this estimate **the impact of water intrusion is rated as Moderate.**

Mitigation

Current Practices. CCTB has taken steps to mitigate the risk of water intrusion, such as clearing gutters of debris and performing facility maintenance as needed. Furthermore, roof inspections are performed annually.

Other Best Practices. The MPA Team identified several additional best practices in the literature that should be followed to mitigate water intrusion damage:

Critical Equipment and High-Value Inventory

An assessment of areas posing the greatest risk to high-value inventory and critical equipment should be performed. Identification of water sources to determine ways to minimize water damage to critical assets should be assessed. Removing assets to areas with the least exposure to water sources should be considered (CNA Financial Corporation, 2018).

Water Shut-off Valve Identification Plan

A broken 2-inch water supply line can gush out 125 gallons of water per minute. It is important to know the location of the water disconnect valve and cut-off points to minimize damage. Use a highly visible valve identification tag and lubricate the valve periodically to ensure proper operation. Determine when the fire protection control valves can be shut off in consultation with the local fire department and advise and train employees on proper procedures. Shutting off the water as quickly as possible can save inventory and significantly lower cleanup costs. (CNA Financial Corporation, 2018).

Cold Weather Preparation

It is important to protect pipes from freezing temperatures to reduce the probability of a pipe break. Evaluate the exterior and interior of the facility and develop a checklist that includes insulating pipes vulnerable to freezing temperatures. In case of a power outage, have a reliable power backup source to heat the building during severe cold weather. (CNA Financial Corporation, 2018).

Surface Water Run-off

Although CCTB is not located in a FEMA flood zone, surface water runoff could still pose a water intrusion threat. Routine inspection of drainage systems ensures water is funneled away from the building. It is recommended that a regular preventive maintenance schedule include inspection of drainage systems such as exterior drains and downspouts (CNA Financial Corporation, 2018).

Leak Response Kit

Create a leak response kit with absorbent mops and pads, wet/dry vacuums, squeegees, and wet floor signs. Establish an agreement with a water damage restoration firm. Authorize staff to engage outside resources when needed for immediate, emergency response (CNA Financial Corporation, 2018).

Cybersecurity

Low Likelihood **Moderate Impact**

Background

Cybersecurity is defined as the practice of implementing controls and tools in place that ensure information stored by an organization maintains integrity standards, is confidential, and is readily available. This practice utilizes tools, risk management procedures, technology, and training to keep all systems and information technology equipment safe and functioning correctly (Forcepoint, 2011). Forcepoint (2011) identifies four common types of cybersecurity attacks. These include:

- Malware - Malicious software such as viruses, Trojan horses, and keyloggers that block or attack user's use of a server or computer
- Ransomware - Specific type of malware that locks or hijacks user profile and is often held hostage until a ransom is paid
- Phishing - Obtaining personal or confidential email through sending a message or link deceptively
- Social Engineering - Psychological manipulation of individuals that allows a hacker to obtain personal or confidential information.

Cybersecurity is an important topic of interest for organizations across the public and private sectors. It is estimated that by 2027, there will be over $10 billion spent on implementing procedures and best practices (Powell, 2019). With the rapid growth of technology and the dependent use of internet and data in everyday business operations, organizations have been affected by data breaches and hacking that have exposed millions of consumer records and incurred large fines of recovery for the organization. A data breach on Facebook resulted in over 90 million users being logged out of their accounts with no ability to reset passwords. Small businesses make up over 43% of cyber-attacks; public serving organizations often make up less than 20% of cyber-attacks. Also, these types of organizations often have the smallest budgets for cyber security (Strawbridge, 2018).

Relevance to Charlotte Community ToolBank

CCTB uses an online cloud system for the storing of transactions and files for business operations. The cloud system could be vulnerable to attacks as CCTB takes on a third-party risk when they outsource the hosting of their IT systems. Presently, the organization has experienced one virus incident that was able to be remediated through a board member's employer. The Board of Directors also utilize their own personal or business accounts when emailing or conducting business. This opens CCTB to cybersecurity risk since it is unable to mitigate or remediate a cybersecurity event like it would for an event where the infrastructure was owned by CCTB.

Likelihood

Ninety-two percent of malware attacks are sent by email and a ransomware attack occurs every 14 seconds (Powell, 2019). Public organizations also experience 1 in 302 emails that may be corrupt (Powell, 2019). Fortunately, CCTB now has antivirus protection and a third party directly involved with mitigation of these events. As a result, **the MPA Team has rated the likelihood of a cyber security incident as Low.**

Impact

The average cost of a cyberattack is $3 million (Crowe, 2019), and recovery from a cyberattack can negatively affect small business operations for up to 6 months (Mansfield, 2019). Given the CCTB's current mitigation practices and its lower scale of transactions, the impacts on its business operations and the costs of recovery are likely to be lower than those seen in other organizations. As a result, **the MPA Team has rated the impact of a cyber security incident as Moderate**.

Mitigation

Current Practices

CCTB does currently have programs and activities in place that help mitigate the risk of a cybersecurity attack. Current activities identified include:

- Utilizes a third-party IT analyst that administers an antivirus program, monitors IT activity, and can troubleshoot or remediate issues as they arise. Many nonprofits do not have a committed resource that can monitor cyber activity (NonProfit Times, n.d.)
- Maintains passwords for accounts and a cloud program where two members have access
- Keeps a back-up offline inventory management tool manually in case of IT shutdown

Other Best Practices

The MPA Team identified several additional best practices in the literature and recommends that CCTB take these actions:

<u>Perform an Analysis of Third-Party IT Antivirus Program</u>

Metivier (2018) identifies multiple areas of risk an organization is susceptible to when a third party manages a function within the organization. If a vendor experiences a cyberattack this will also put the data controlled by the vendor for the organization at risk. Gaps or inadequacies in the vendor's controls to mitigate cybersecurity risk could interfere with CCTB's strategy, compliance, transactions, and reputation.

<u>Set Up a Firewall</u>

Segal (n.d.) recommends establishing a firewall that sets up a barrier between the organization and the external world. This separates the data collected by the organization and provides an extra layer of security for the internal infrastructure. This will also help mitigate any risk by using other Wi-Fi networks which CCTB may use if they experience connectivity issues at the warehouse (Segal, n.d.).

Implement Employee Training Program

A training program can help educate CCTB employees on the different types of cybersecurity events and how to participate in the mitigation of cybersecurity risk. The training program should also focus on what the current programs and activities the organization participates in to prevent a cybersecurity event from occurring (Segal, n.d.).

Maintain a Password-protection Program

If a hacker or a former associate of CCTB knows a password to access any accounts or infrastructure, the organization is easily opened up to cybersecurity attacks. A password program that maintains who should have access and is routinely updated will help mitigate this risk (Segal, n.d.).

Routinely Backup all Data

Currently, CCTB uses a server to maintain all transaction and organization data. There are manual offline spreadsheets that can be used if needed. A regular routine that backs up all the data on the server can help make the reconciliation of transactions easier if the primary server is attacked (Segal, n.d.).

Response Plan

The president of Agile Recovery Solutions, Bob Boyd, stated that 75% of employees did not think their organization or employer were prepared for a disaster (Colorado Small Business Development Center, 2013). Ready.gov states the initial response during a crisis or emergency can save lives, control the event, and prevent damage to the organization or facility. When responding to an event, the Ready.gov prioritizes the safety of people within the organization. This could be Board Members, employees, or clients. Second, the organization's response should focus on the stabilization of the organization's assets and resources (DHS, n.d.a).

ScienceDirect magazine discusses the importance of a flexible emergency response plan. Since no one plan can be a solution for all emergencies, it is important to implement a response plan that accounts for any potential natural, technological, and man-made threats that could harm or damage the organization. A response plan provides the framework for officers or employees to plan and think critically to reduce loss and provide safety for multiple situations. The response plan also provides a program that must be routinely practiced for effective implementation (Vendrell and Watsonl, 2010).

The Colorado Small Business Development Center's *Disaster Continuity and Recovery Guide* provides a template that effectively outlines the requirements for an emergency response plan. The template can be found online on the Colorado Small Business Development Center website. It has been approved by OSHA and considers a full landscape of how to respond. Their template provides a step-by- step walk-through of how to create a guide for an organization.

In their template, a Response Plan should consider the following:

1. Reporting emergencies
2. Evacuation procedures and escape routes
3. Critical shutdown procedures
4. Employee accountability procedures
5. Medical duties
6. Contact information (employees, customers, emergency responders, stakeholders, media)
7. Description of emergency alarm systems
8. Alternate communication center
9. Location of critical records
10. Communication methods
11. Responsibility and authority
12. Shelter, lockdown, medical emergencies, utility outage, visitor procedures (Colorado Small Business Development Center, 2013)

Recommendation

It is the MPA Team's recommendation that CCTB create, implement, and provide training for an emergency response plan. The emergency response plan should follow the guidelines provided by the Colorado Small Business Development Center. These guidelines are comprehensive and thorough in helping organizations respond quickly in the event of a crisis. A recent FEMA survey found that 60 percent of adults are not prepared or practiced for a disaster. Of the respondents, only 39 percent have a developed emergency plan. (FEMA, 2015)

Some general guidelines from the Colorado Small Business Center for creating the plan that can also be considered are as follows:

- Create checklists
- Create a one-page summary for different risks identified
- Organize actions into People and Things, stating who should be doing an action and what items they should be responsible for
- Make the plan easily accessible for employees and stakeholders to locate
- Practice the plan routinely to commit the process steps to memory for stakeholders and employee (Colorado Small Business Development Center, 2013).

Recovery Plan

After CCTB has addressed the organization's immediate needs through its disaster mitigation and response procedures, its next step is to begin the recovery process. In its *National Disaster Recovery Framework*, the U.S. Department of Homeland Security (2017) describes recovery as the continuation and restoration of critical services that support the physical, emotional, and financial well-being of those impacted by a disaster. The recovery phase involves activities that will enable the organization to return to its regular routine or create a new sense of normalcy for the future. Since recovery is the longest part of the disaster management process (Colorado Small Business Development Center, 2013), this phase focuses on long-range planning efforts. These activities should be implemented in the weeks, months, and years after an incident has occurred.

To advise CCTB in business continuity planning, the MPA Team identified two main aspects of recovery that apply to the hazards described in the Risk Identification and Assessment section. The first is operations. This category includes people and money, two functional elements that keep the organization running. The second aspect of recovery is assets. This category includes tangibles such as equipment and the building.

The following recovery plan provides a set of recommended actions CCTB can take to regroup, restore, and continue serving the community after a disaster. The plan is organized into four major recovery focus areas: people, money, equipment/inventory, and building. CCTB should review its recovery plan regularly to ensure it continues to meet the organization's needs (Department of Homeland Security, 2017). Staff, Board Members, and other stakeholders can be involved in updating the plan. Together, they can examine the lessons learned from local and national incidents that can inform and improve CCTB's plan (Department of Homeland Security, 2017).

Operations: People

CCTB's people are the most essential element of its operations. Following an event, the organization must take steps to replace any human and social capital it may have lost. These long-term strategies will help the organization build internal resilience in the aftermath of a disaster.

<u>Provide Support to Staff to Ensure a Smooth Transition and Return to Operations</u>
Like any other organizational change, personnel-related recovery efforts require a balance between strategy and sensitivity. CCTB can support its employees, Board Members, and other stakeholders by staying focused on the organization's mission and strategic vision during the recovery period (Gothard & Austin, 2013, p. 280). This focus will provide consistency at a time when employees may feel uncertain as they continue to navigate post-disaster changes.

Monitor the Emotional Well-being of Staff and Stakeholders, and Provide Access to Mental Health Resources

After a disaster, CCTB should observe the emotional response of the staff, volunteers, and Board Members impacted by the incident, noting any signs of disaster-related stress (Department of Homeland Security, n.d.a). For incidents involving workplace violence, holding a listening session will allow employees and other stakeholders to communicate their safety concerns to the organization. At the same time, leadership can reinforce that safety is a priority and that all necessary protocols are in place to keep everyone safe. The organization should reassure and remind employees of available counseling services (Miller, 1999). FEMA recommends individuals contact the Disaster Distress Helpline, a national, toll-free crisis counseling hotline (2015).

Hold a Transition Meeting to Hand-off Executive Director Responsibilities

If the Executive Director returns from a short-term absence, the first recovery action should be for the Interim Executive Director to transition responsibilities back to the Executive Director. The two should hold a transition meeting where they discuss issues that emerged during the interim period. The Interim Executive Director should also update the Executive Director on any changes that may have occurred and provide a briefing on service delivery during her absence.

Implement the Succession Plan

To identify a replacement for the Executive Director, CCTB should proceed with the steps outlined in the succession plan created during the mitigation stage. Succession planning should be an ongoing process, so the organization should regularly assess the succession plan and make improvements as needed (Day, 2007).

Conduct Orientation Sessions to Educate and Support the New Executive Director

Since a new Executive Director will have a learning curve, the organization should conduct orientation sessions to educate the new leader on its history and culture (Gothard & Austin, 2013, p. 278). Communication between the Board of Directors and the Executive Director should remain open to ensure they are in agreement on the organization's direction. The Executive Director may also need the Board's support in maintaining and building CCTB's network of community partners. Board Members could serve as facilitators in strengthening existing relationships and establishing new ones.

Operations: Money

There are financial responsibilities to consider during the recovery process of nearly every emergency. Insurance, recovery, negotiations, savings, and seeking assistance may be appropriate steps in addressing the long-term effects of a crisis.

Insurance Collection

Much of the financial considerations involved following up with insurance providers to address the recovery efforts for crises including: cyber theft/damage, power outages, water damage, fire, or any weather-related damage. These steps might include filing a claim and working with the insurance company to complete necessary documentation to receive a final payout.

Theft Recovery

In instances of theft, some relief might come from official investigations into the theft that result in the recovery of stolen property or money. Working with local, state, and federal agencies in their investigations and following up to ensure that there is action could assist in the recovery of stolen property.

Lease Negotiations

When the physical location of the space is threatened it might be necessary to renegotiate a lease agreement. Reaching out to the property owner and discussing potential options for payment or requesting a grace period for payments. If a negotiated repayment is not an option, a search committee should begin to identify a more affordable location and start the process of securing a new lease (Day, 2007).

Access Savings and Seek Assistance

In a funding crisis, the organization should have available savings or emergency funds that can cover the cost of three months of operations. It might also be necessary to target additional major funders to request assistance. If there are emergency grants that the organization could apply to receive, this option should be reviewed. CCTB may also seek out or tap into their current network of organizations and corporations who may be able and willing to assist in operation at reduced or no cost (Wayland, 2015, p. 114-115).

Assets: Equipment/Inventory

If a crisis or disaster were to occur, damage to inventory could prevent Charlotte Community ToolBank from continuing its regular business operations. It is critical for CCTB to plan on how to replace its inventory quickly. Recovery plans for equipment and inventory should include the following:

Maintain a Manual Physical Inventory Tracking System

CCTB should maintain a tracking log of all equipment and tools. This log should show the quantity available, the quality of the equipment, the last day of maintenance, next day of required maintenance; and if there is any insurance or warranty protection for that item. This log should be maintained for each tool, IT system infrastructure, and equipment that would be vulnerable during an emergency. Having an asset log can be critical when performing a damage assessment that would be performed after an event (Wayland, 2015).

The damage assessment that utilizes a kept record of equipment and inventory will help CCTB prioritize what should be replaced immediately, what can be replaced at a later date, and what need not be replaced at all. It will also prioritize what items will need to be repurchased and what items may have a warranty or insurance claim that can be leveraged for repurchase (Wayland, 2015). CCTB can also use the physical inventory to identify undamaged inventory that would still be available for client use. After the equipment has been inventoried and a

damage assessment performed, CCTB should come up with a prioritized list of items to be recovered. The next decision should focus on how these items can be recovered. If any items do not have a warranty protection or are covered through a mutual agreement, the organization will need to evaluate its current inventory and see what can be liquidated and budgeted to purchase the needed items.

To repurchase the items, CCTB will need to file all claims with insurance companies and execute all warranty agreements. The organization could then hold a garage sale or liquidate any non-prioritized or excess items to secure funding for repurchasing the prioritized items. In parallel, CCTB will need to look at its budget to see what expenses can be frozen until the revenues are secured (Wayland, 2015).

Utilize Relationships with Local Retailers

CCTB can reach out to local retailers and service providers to implement mutual aid agreements where tools and inventory could be provided at reduced costs. These relationships will need to be formally documented and a contact established that can be immediately reached after an event. Once these agreements have been made, the contact information and materials covered in the agreement should be kept in an easily accessible location to be actioned during the recovery phase (Wayland, 2015).

Assets: Building

Every day that operations are out of service due to building damage or loss, CCTB is unable to provide vital tools to community organizations. Following incidents, the organization must implement a recovery plan to repair any damage to its building. Long-term strategies including an analysis of insurance, a building assessment, and a plan for a temporary work location will help to prepare the organization to resume business operations at the same level prior to the incident (Wallace & Webber, 2011; Wayland, 2015).

Insurance

After any incident, CCTB should be ready to follow up with their insurance company. CCTB should verify what the insurance policy will and will not cover. The American Red Cross (ARC) (2015) recommends maintaining detailed information and any documents that the insurance may need for the claim. ARC recommends keeping all paperwork to ensure proper payouts for damages incurred to buildings.

Building Assessment

CCTB should initially check with the Charlotte Fire Department to ensure the building is safe to enter. ARC offers steps to complete an assessment, including checking the exterior and interior for building damage, evaluating the building to determine if the impact of damage requires structural repair, or if the area is unsafe for staff to work from (American Red Cross, 2015).

Temporary Work Location

If the building has damage only affecting the office area, CCTB should focus on acquiring a

temporary work location for the two staff members. If damage is major or the building is unstable, a temporary work location must include space to house tools and a workspace for staff (Wayland, 2015). The final decision on where the team or equipment will be relocated to resume operations depends on the level of damage, the length of time the building will be unstable, and the cost of a temporary work location (Wayland, 2015).

A temporary work location must meet the basic needs to continue operations. Another option is having policies for teleworking or work from home procedures in the event that a recovery site is unable to be attained. The alternative solution of telework requires preparation and planning in advance (Wallace & Webber, 2011). Additionally, CCTB will need to provide a secure network for communication and handling confidential items when teleworking (Wallace & Webber, 2011).

It is also advisable for CCTB to establish mutual agreements with other agencies to utilize space for inventory storage or other business operations until the damaged facilities can either be repaired or replaced.

Conclusion

All businesses hope to never experience a disaster; however, at some point most organizations will face a difficult event. Charlotte Community ToolBank was proactive and tasked the MPA Team to complete a comprehensive risk assessment which identified the following risks: Power Outage, Property Crime, Personnel Loss, Fire, Loss of Space, Revenue Loss, Severe Weather, Workplace Violence, Water Intrusion, and Cybersecurity. The report outlines the highest likelihood and impact of these risks on CCTB's operations.

The organization currently follows many of the best practices to mitigate the identified risks. The MPA Team commends CCTB for taking these steps to protect the organization from various threats and to prepare for harmful incidents. Further, the report recommends best practices for the organization to implement. The MPA Team identified 12 areas to consider when creating a response plan and lists general guidance for plan development. The MPA Team identified four areas of recovery: people, money, equipment/inventory, and building. These should serve as the focal point of CCTB's long term recovery plan.

A proactive approach to prepare for disaster is the best way to reduce or avoid potential personnel, assets, property, or operational losses. Risk reevaluation and mitigating actions should be scheduled annually or as circumstances change. Most importantly, following through with the current and recommended best practices will increase CCTB's chances of survival and long-term viability when confronting adversity.

Acknowledgements

The MPA Team would like to thank the following individuals for their time, assistance, and contributions:

Maureen Krueger - Executive Director, Charlotte Community Toolbank
Lex Yelerton - Warehouse Coordinator, Charlotte Community Toolbank
Hannah Sanborn - Emergency Management Planner, Char-Meck Emergency Management Office
Phil Bosche - Battalion Chief, Charlotte Fire Department
Erika Hornsey - Executive Director, Houston Community ToolBank

Appendix I - Scope of Work

UNC CHARLOTTE

Scope of Work

Background:
The Charlotte ToolBank is a nonprofit organization that provides nonprofits and public-serving entities with access to the tools and equipment needed to complete community projects and stage special events. Client organizations often have restricted budgets that limit their ability to purchase or rent tools and equipment at market rates. ToolBank serves as a depository for these organizations from which they can inexpensively attain the implements they need, enabling them to maximize the use of their limited resources. The Charlotte ToolBank is an affiliate of a broader network of tool bank organizations.

Goals:
The Charlotte ToolBank's leadership and executive board have identified a need for the creation of an emergency management program. They are interested in acquiring information that can help the organization to mitigate risk and recover from crisis situations. The executive team has resources and current models that they would like to use as a reference. They have tasked students at the Gerald G. Fox Master of Public Administration Program at the University of North Carolina at Charlotte (hereafter referred to as "the MPA Team") to accomplish the following:

1. Examine best practices in the field for creating an emergency response plan
2. Identify key risks that directly affect the organization
3. Create controls to mitigate identified risks
4. Develop a recovery plan for crisis situations

Tasks
The UNC-Charlotte MPA student group will create a comprehensive emergency response plan by completing the following tasks:

1. Conduct a risk assessment of current emergency preparedness environment
2. Interview organization leadership; affiliate resources; and field practitioners
3. Research emergency risks, mitigation, and recovery best practices
4. Provide recommendations for mitigation risk and controls
5. Provide emergency management plans for crisis recovery
6. Deliver a final report and presentation to organization leadership

Boundaries

1. Limited Full Time Staff and Financial Resources
2. Project is restricted to Fall 2019 semester
3. Enterprise agreements or obligations that local affiliate must adhere to
4. Donor expectations and obligations must be considered

Timelines

Event	Date
Client presents to MPA Group	Aug. 20
Scope of Work Presented to Client	Sept. 10
Send Draft to Client	Nov. 26
Final Report Due	Dec. 10
Final Presentation and Report	Dec. 10

Deliverables

1. Draft Report
2. Final Report
3. Presentation

Client Signature: Maureen Kruger

MPA Student Signature Aricelda de la G
Samuel J Hopkins
Donna M. Ashley
Megan McClellan
Kelly Weston
Cameron Dog

Appendix II - Risk Identification Template

The Risk Identification Template outlines the process the MPA Team executed to identify likely risks which pertain to an organization. After risks have been identified, the organization must evaluate the likelihood and impact of each risk. Assessed risks should then be prioritized in a High, Moderate, or Low category for the likelihood and impact of each risk.

This template can be used as a guideline for the risk identification process. Various sources were used to compile a list of risks and tools the MPA Team used to finalize the risks identified in this report. The template includes:

- **Identify Risks** shows a comprehensive list of risks documented by the Colorado Small Business Network (2013). These are broken out into the following categories: Natural Risks; Human Related Risks; Technology Risks; Operation Risks. A step by step procedure is provided. Extra space is provided to include additional risks.
- **Consolidate Risks** provides an assessment tool the organization can use to determine which risks from the first step are applicable/not applicable to the organization.
- **Assess Risks** evaluates each relevant risk for possible scenarios, mitigation plans, probability, and impacts. FEMA (2014c) designed a resource that provides a matrix on how these can be documented and how to execute the evaluation.
- **Prioritize Risks** provides a space to rate each risk on a matrix comparing the likelihood and impact of each risk. The Colorado Small Business Network (2013) designed a matrix that each risk can be categorized.
- **Finalize Risks** consolidates all relevant risks. The organization should define each risk and example scenarios for the final risks.

1. Identify Risks

Procedure	Identify certain events that if occurred would result in the loss of business operations or personnel; negatively impact organization's financial health or reputation; or affect clients or your local community. List any potential risks that an organization would be susceptible to. (Note: in this step you are not deciding what may or may not be applicable to your organization. You are brainstorming what types of risks or events may exist for any organization

Natural Risks	**Human Related Risks**	**Technology**	**Operation**
Fire	Explosion	System Failure	Donor Loss
Flood	Chemical Spills	Cyber Attack	Facility Damage
Drought	Workplace Violence		Water Intrusion
Earthquake	Power Outage		Personnel Loss
Extreme Heat	Pollution		Loss of Space
Winter Storms	Pandemic Disease		
Tornados	Government Shutdown		
Hurricanes	Stock Market Crash		
Landslides	Nuclear Threat		
Thunderstorms	Terrorism		
Volcanos	War		
Tsunamis	Crime		
Avalanche			

2. Consolidate Risks

Procedure	**List all risks and assess if it is applicable for your organization. Provide justification if any risk is deemed out of scope in this initial phase**

Risk Event	**Internal or External**	**Applicable (Y/N)**	**Rationale**
Fire			
Flood			
Drought			
Earthquake			
Extreme Heat			
Winter Storms			
Tornados			
Hurricanes			
Landslides			
Thunderstorms			
Volcanos			
Tsunamis			
Avalanche			
Explosion			
Chemical Spills			
Workplace Violence			
Power Outage			
Pollution			
Pandemic Disease			
Government Shutdown			

3. Assess Risks

Procedure	Identify all applicable risks and measure using the following matrix to assess what impacts each risk may have on your organization

Risk	Asset or operation at risk	Scenario	Opportunity for Mitigation	Probability	People	Property	Operations	Environment	Entity	Overall Hazard Rating

INSTRUCTIONS

Column 1: Compile a list of assets (people, facilities, machinery, equipment, raw materials, finished goods, information technology, etc.) in the left column.

Column 2: For each asset, list hazards (review the "Risk Assessment" page from Ready Business) that could cause an impact. Since multiple hazards could impact each asset, you will probably need more than one row for each asset. You can group assets together as necessary to reduce the total number of rows, but use a separate row to assess those assets that are highly valued or critical.

Column 3: For each hazard consider both high probability/low impact scenarios and low probability/high impact scenarios.

Column 4: As you assess potential impacts, identify any vulnerabilities or weaknesses in the asset that would make it susceptible to loss. These vulnerabilities are opportunities for hazard prevention or risk mitigation. Record opportunities for prevention and mitigation in column 4.

Column 5: Estimate the probability that the scenarios will occur on a scale of "L" for low, "M" for medium and "H" for high.

Columns 6-10: Analyze the potential impact of the hazard scenario in columns 6 - 10. Rate impacts "L" for low, "M" for medium and "H" for high.

Column 8: Information from the business impact analysis should be used to rate the impact on "Operations."

Column 10: The "entity" column is used to estimate potential financial, regulatory, contractual, and brand/image/reputation impacts.

Column 11: The "Overall Hazard Rating" is a two-letter combination of the rating for "probability of occurrence" (column 5) and the highest rating in columns 6 – 10 (impacts on people, property, operations, environment, and entity).

Carefully review scenarios with potential impacts rated as "moderate" or "high." Consider whether action can be taken to prevent the scenario or to reduce the potential impacts.

4. Prioritize Risks

Procedure	Categorize each risk from Step 3 into this chart to identify which risks should be prioritized for mitigation, response, and recovery planning		
	LOW IMPACT	MODERATE IMPACT	HIGH IMPACT
LOW LIKELIHOOD			
MODERATE LIKELIHOOD			
HIGH LIKELIHOOD			

Step 1	Place all risks in appropriate box
Step 2	Discuss all higher risks (in orange) first
Step 3	Discuss all medium risks (in beige) second
Step 4	Discuss all low risk (In pink) last
Step 5	Organization signs off on prioritized risks that will be addressed in emergency management program

5. Finalize Risks

Procedure	List all risks to be considered for program with specific definition, examples of events that may occur, and justification for why the organization should be prepared for this risk		
Risk	**Risk Definition**	**Example Scenarios**	**Justification**

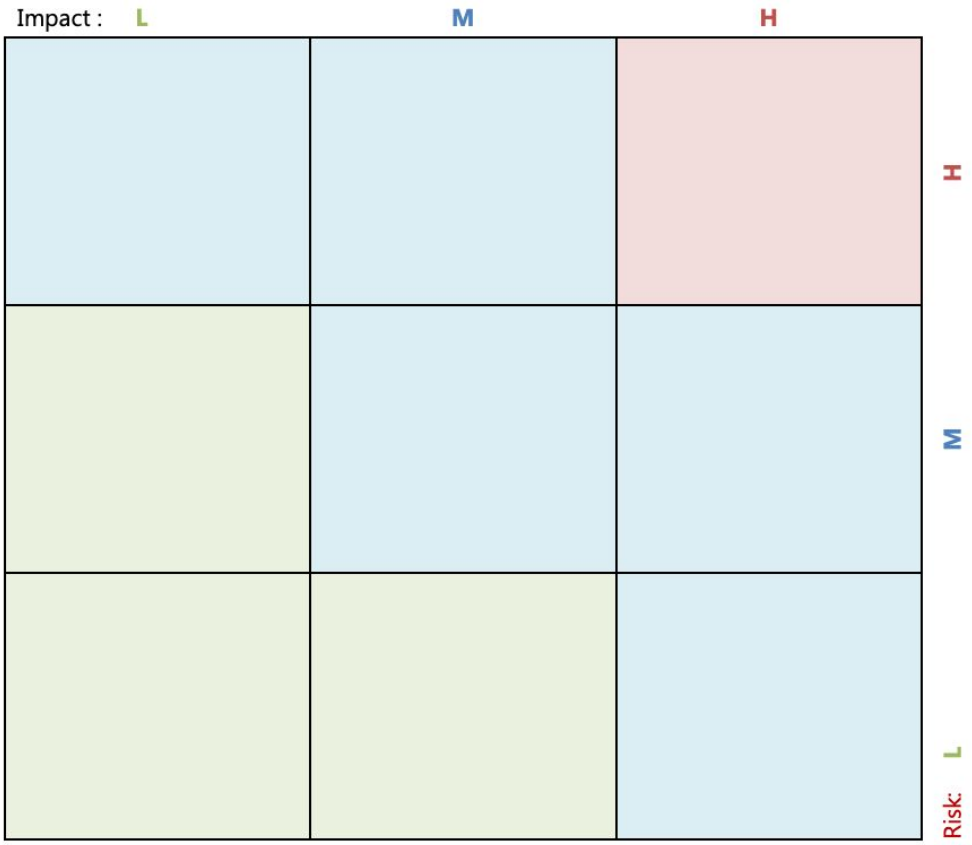
Appendix III - Colorado Small Business Network Risk Worksheets

Worksheet 1 | Prepare: Risk Assessment Table

	Threat (hazard, emergency, crisis, disaster)	Likelihood (L-M-H)	Impact (L-M-H)			Mitigation To-Do	By When	Cost ($)
			People	Places	Things			
NATURAL-ENVIRONMENTAL								
1	Fire							
2	Flood							
3	Drought							
4	Earthquake							
5	Extreme Heat							
6	Winter Storms/Extreme Cold							
7	Tornadoes							
8	Hurricanes							
9	Landslides and Debris Flow							
10	Thunderstorms and Lightning							
11	Volcano Eruptions							
12	Tsunamis							
13	Avalanche							
14	Other Severe Weather							
15	Other Natural Hazards							
16	Other							
17	Other							
HUMAN-RELATED								
18	Explosion							
19	Chemical Spills and Pollution							
20	Workplace Violence							
21	Utility Outage							
22	Pollution (water, air, soil)							
23	Pandemic Disease							
24	Supplier Failure							
25	Government Shutdown							
26	Stock Market Crash							
27	Nuclear Threat							
28	Terrorism							
29	War							
30	Other							
31	Other							
TECHNOLOGY								
32	Mechanical Breakdown							
33	Cyber Attack							
34	All Backups Fail (incl. cloud)							
35	Other							
OTHER								
36	Heart Attack							

Worksheet 2 | Prepare: Risk Assessment Matrix

After you have completed the Risk Assessment Table, take your L(ow), M(edium) and H(igh) marks for both Risk and Impact and plot them into this Risk Assessment Matrix. You can then see how many items are in the High/High section. You should be paying the most attention to them, your "low hanging fruit."



References

Allen, D. (2008). SHRM Foundation's effective practice guidelines series: Retaining talent: A guide to analyzing and managing employee turnover. Retrieved from https://www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/Documents/Retaining-Talent.pdf.

American Red Cross. (2015). Disasters and financial planning. Retrieved from https://www.redcross.org/get-help/disaster-relief-and-recovery-services/recovering-financially.html.

Bronson, C. (2016). The five most common causes of homeowners insurance claims: Report. Retrieved from https://www.insurancebusinessmag.com/us/news/breaking-news/the-five-most-common-causes-of-homeowners-insurance-claims-report-30232.aspx

Bureau of Labor Statistics. (2019). Job openings and labor turnover. Retrieved from https://www.bls.gov/news.release/pdf/jolts.pdf.

Byerly, B. (2012). Measuring the impact of employee loss. *Performance Improvement, 51(5)*, 40-47.

Centers for Disease Control. (2018). Occupational violence: Fast facts. Retrieved from https://www.cdc.gov/niosh/topics/violence/fastfacts.html

Charlotte Center City Partners. (2018). Southend development report. Retrieved from https://historicsouthend.com/wp-content/uploads/2018/06/South-End-Development-Report-May-2018-REDUCED.pdf.

Charlotte Community ToolBank. (2018). Warehouse coordinator job description. Retrieved from http://charlotte.toolbank.org/wp-content/uploads/2018/09/Warehouse-Coordinator-Position-9-18-2018.pdf.

Charlotte Fire Department. (n.d.). Smoke alarms and carbon monoxide alarm. Retrieved from https://charlottenc.gov/Fire/KeepingYouSafe/FireandLifeSafetyEducation/Pages/Smoke Alarms and Carbon Monoxide Alarms.aspx.

Charlotte-Mecklenburg Emergency Management Office. (2015). Charlotte-Mecklenburg multi-jurisdictional hazard mitigation plan. Retrieved from https://charlottenc.gov/EmergencyManagement/Plans/HazardMitigationPlans/2015Plan/Pages/default.aspx.

Charlotte-Mecklenburg Police Department. (2018). CMPD crime prevention tips. Retrieved from https://charlottenc.gov/CMPD/Safety/Pages/Safety-Tips.aspx

Charlotte/Mecklenburg Quality of Life Explorer. (2018). Quality of life explorer. Retrieved from https://mcmap.org/qol/.

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, *10*(3), 163–176.

CNA Financial Corporation. (2018). Water damage mitigation - A guide for emergency planning. Retrieved from https://www.cna.com/web/wcm/connect/2ca5fe78-fee1-4738-b6e3-bd01d151abc5/RC_Property_Guide_WaterDamage_CNA.pdf?MOD=AJPERES.

Colorado Small Business Development Center. (2013). Disaster recovery and continuity guide for small businesses. Retrieved from https://www.coloradosbdc.org/wp-content/uploads/sites/4/2019/01/CSBDC-Business-Recovery-Guide.pdf.

Crime Data Explorer. (n.d.). Retrieved November 7, 2019, from https://crime-data-explorer.fr.cloud.gov/explorer/state/north-carolina/crime.

CrimeMapping. (n.d.). Mecklenburg county crime map. Retrieved from https://www.crimemapping.com/map/agency/65

Crowe, J. (2019). 7 eye opening cyber security statistics every small business needs to know. Retrieved from https://www.ninjarmm.com/blog/small-business-cybersecurity-statistics-2019.

Day, D. (2007). SHRM Foundation's effective practice guidelines series: Developing leadership talent: A guide to succession planning and leadership development. Retrieved from https://www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/Documents/Developing-Leadership-Talent.pdf.

Department of Homeland Security. (n.d.a). Coping with disaster. Retrieved from https://www.ready.gov/coping-with-disaster.

Department of Homeland Security. (n.d.b). Crisis communications plan. Retrieved from https://www.ready.gov/business/implementation/crisis.

Department of Homeland Security. (n.d.c). Emergency response plan. Retrieved from https://www.ready.gov/business/implementation/emergency.

Department of Homeland Security. (2017). National disaster recovery framework. Retrieved from https://www.fema.gov/media-library-data/1466014998123-4bec8550930f774269e0c5968b120ba2/National_Disaster_Recovery_Framework2nd.pdf.

Department of Homeland Security. (2019). Ready business power outage toolkit. Retrieved from https://www.ready.gov/power-outages.

Eaton. (2012). Blackout tracker. United States annual report 2012. Retrieved from www.eaton.com.

Eaton. (2015). Blackout tracker. United States annual report 2015. Retrieved from www.eaton.com.

Eaton. (2017). Blackout tracker. United States annual report 2017. Retrieved from www.eaton.com.

Evarts, B. (2018). Fire loss in the United States. Retrieved from https://www.nfpa.org/News-and-Research/Data-research-and-tools/US-Fire-Problem/Fire-loss-in-the-United-States.

Federal Bureau of Investigation. (2018). Property crime. Retrieved from ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017/topic-pages/property-crime.

Federal Emergency Management Agency. (2019a). After the fire. Retrieved from https://www.usfa.fema.gov/downloads/pdf/publications/fa_46.pdf?utm_source=website&utm_medium=pubsapp&utm_content=After%20the%20Fire&utm_campaign=R3D.

Federal Emergency Management Agency. (2018a). Be prepared for a tornado. Retrieved from https://www.fema.gov/media-library-data/1522342356541-54bd8d92d0d0d07bca4c1250ebde2b21/Tornadoes_508.pdf.

Federal Emergency Management Agency. (2014a). Emergency supply list. Retrieved from https://www.fema.gov/media-library-data/1390846764394-dc08e309debe561d866b05ac84daf1ee/checklist_2014.pdf.

Federal Emergency Management Agency. (2017a). How to prepare for a winter storm. Retrieved from https://www.fema.gov/media-library-data/1408633655071-32caae446efef4ab2f4fcccdb55f725c/PrepareAthon_WINTER%20STORMS_HTG_FINAL_508.pdf.

Federal Emergency Management Agency. (2019b). Power outage information sheet. Retrieved from https://www.fema.gov/media-library/assets/documents/162056.

Federal Emergency Management Agency. (2014b). Prepare your organization for a hurricane playbook. Retrieved from

https://www.fema.gov/media-library-data/1409933369110-5d82e4e75ba272f6cefd656ff190c422/prepareathon_playbook_hurricane_final_090414_508.pdf.

Federal Emergency Management Agency. (2017b). Recovering from the storms within. Retrieved from https://www.fema.gov/blog/2017-05-11/recovering-storms-within.

Federal Emergency Management Agency. (2018b). Residential building electrical fires (2014-2016). Retrieved from https://www.usfa.fema.gov/downloads/pdf/statistics/v19i8.pdf

Federal Emergency Management Agency. (2014c). Risk Assessment Table. Retrieved from https://www.fema.gov/media-library/assets/documents/89542

Federal Emergency Management Agency. (2015). Sixty percent of Americans not practicing for disaster: FEMA urges everyone to prepare by participating in National PrepareAthon! Day on April 30th. Retrieved from https://www.fema.gov/news-release/2015/04/28/sixty-percent-americans-not-practicing-disaster-fema-urges-everyone-prepare.

Federal Reserve Bank of Kansas City. (n.d.). Nonprofit executive succession-planning toolkit. Retrieved from https://www.kansascityfed.org/publicat/community/nonprofit-executive-succession-planning-toolkit.pdf.

Forcepoint. (2011). What is cybersecurity? Retrieved from https://www.forcepoint.com/cyber-edu/cybersecurity.

Gibbons, S. (2004). The costs of urban property crime. *The Economic Journal, 114*(499), F441-F463.

Gibelman, M. & Gelman, S. (2002). On the departure of a chief executive officer. *Administration in Social Work*, *26*(2), 63-82.

Gothard, S., & Austin, M. (2013). Leadership succession planning: Implications for nonprofit human service organizations. *Administration in Social Work, 37*(3), 272-285.

Gramlich, J. (2019). What the data says about gun deaths in the U.S. Retrieved from https://www.pewresearch.org/fact-tank/2019/08/16/what-the-data-says-about-gun-deaths-in-the-u-s/.

Herman, M. L. (n.d.). Lost in space: Managing facility rental risks. Retrieved from https://nonprofitrisk.org/resources/articles/lost-space-managing-facility-rental-risks/.

Houston Police Department. (2019). Commercial burglary prevention. Retrieved from https://www.houstontx.gov/police/keep_houston_safe/commercial_crime_prevention.htm

Home Advisor. (n.d.). Learn how much it costs to repair water damage. Retrieved from https://www.homeadvisor.com/cost/disaster-recovery/repair-water-damage/.

Ibrisevic, I. (2018). Top funding sources for nonprofits and charities. Retrieved from https://donorbox.org/nonprofit-blog/nonprofit-funding-sources/.

Kim, P., Perreault, G., & Foster, W. (2011). Finding your funding model: A practical approach to nonprofit sustainability. Retrieved from https://ssir.org/articles/entry/finding_your_funding_model.

Lyttle, S., Penland, B., & Cooke, M. (2012, March 4). 'It was devastating' - 132 homes damaged in Meck. The Charlotte Observer. Retrieved from https://infoweb-newsbank-com.eu1.proxy.openathens.net/apps/news/document-view?%20p=WORLDNEWS&docref=news/13D5413E175A4968.

Mansfield, M. (2019). Cybersecurity statistics: Numbers small businesses need to know. Retrieved from https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html.

Metivier, B. (2018). Why managing third-party cybersecurity risk matters. Retrieved from

https://www.tylercybersecurity.com/blog/why-managing-third-party-cybersecurity-risk-matters

Miller, L. (1999). Workplace violence: Prevention, response, and recovery. *Psychotherapy: Theory, Research, Practice, Training, 36(2)*, 160. Retrieved from http://dx.doi.org/10.1037/h0087694

Mirza, B. (2012). Getting back to work after a workplace violence event. Retrieved from https://www.shrm.org/resourcesandtools/hr-topics/risk-management/pages/backtowork.aspx

National Council of Nonprofits. (2019). Board roles and responsibilities. Retrieved from https://www.councilofnonprofits.org/tools-resources/board-roles-and-responsibilities.

National Crime Prevention Council. (2017). Strategy: Business watch. Retrieved from https://www.ncpc.org/resources/home-neighborhood-safety/strategies/strategy-business-watch/.

National Fire Protection Association. (2019). Fire loss in the United States. Retrieved from https://www.nfpa.org/News-and-Research/Data-research-and-tools/US-Fire-Problem/Fire-loss-in-the-United-States.

National Institute for Occupational Safety and Health. (2018). Occupational violence. Retrieved from https://www.cdc.gov/niosh/topics/violence/default.html

National Neighborhood Watch. (2019). Business watch. Retrieved from https://www.nnw.org/business-watch.

National Ocean Service. (n.d.). What is a hurricane? Retrieved from https://oceanservice.noaa.gov/facts/hurricane.html.

National Oceanic and Atmospheric Administration. (n.d.). US tornado climatology. Retrieved from https://www.ncdc.noaa.gov/climate-information/extreme-events/us-tornado-climatology.

National Weather Service. (2009). Thunderstorms, tornadoes, lightning...Nature's most violent storms. Retrieved from https://www.weather.gov/media/owlie/ttl6-10.pdf.

Nonprofit HR. (2016). Nonprofit employment practices survey results. Retrieved from http://www.nonprofithr.com/wp-content/uploads/2016/04/2016NEPSurvey-final.pdf.

North Carolina Climate Office. (n.d.a). Hurricane statistics. Retrieved from https://climate.ncsu.edu/climate/hurricanes/statistics?state=NC.

North Carolina Climate Office. (n.d.b). Winter weather: Introduction. Retrieved from https://climate.ncsu.edu/climate/winter/intro.

North Carolina Department of Insurance. (2019). North Carolina civilian fire deaths. Retrieved from https://ncdoi.maps.arcgis.com/apps/opsdashboard/index.html#/28fb59dcb9df4bc791868bb52949aee8

North Carolina Department of Public Safety. (2018). State of North Carolina hazard mitigation plan. Retrieved from https://files.nc.gov/ncdps/documents/files/State%20of%20North%20Carolina%20Hazard%20Mitigation%20Plan%20Final%20As%20Adopted.pdf.

Occupational Safety & Health Administration. (2001). How to plan for workplace emergencies and evacuations. Retrieved from https://www.osha.gov/Publications/osha3088.html

Occupational Safety & Health Administration. (2015). Workplace violence in healthcare. Retrieved from https://www.osha.gov/Publications/OSHA3826.pdf

Portman, J., & Steingold, F. (2005). *Negotiate the best lease for your business*. Berkeley, CA: NOLO.

Powell, M. (2019). 11 eye opening cyber security statistics for 2019. Retrieved from

https://www.cpomagazine.com/cyber-security/11-eye-opening-cyber-security-statistics-for-2019/.

Renz, D. O., & Herman, R. D. (2016). *The Jossey-Bass handbook of nonprofit leadership and management*. Hoboken: Jossey-Bass, a Wiley brand.

Robinson, M. K. (2003). *Disaster recovery planning for nonprofits*. Dallas: Hamilton Books.

Scism, L. (2019). American homeowners and their insurers face a flooding crisis from within. Retrieved from https://www.wsj.com/articles/american-homeowners-and-their-insurers-face-a-flooding-crisis-from-within-11551960001.

Segal, C. (n.d.). 8 cybersecurity best practices for your small to medium size business. Retrieved from https://www.coxblue.com/8-cyber-security-best-practices-for-your-small-to-medium-size-business-smb/.

Strawbridge, G. (2018). 5 examples of security breaches. Retrieved from https://www.metacompliance.com/blog/5-examples-of-security-breaches-in-2018/.

U.S. Fire Administration. (2019). North Carolina fire loss fire department profile. Retrieved from https://www.usfa.fema.gov/data/statistics/states/northcarolina.html.

U.S. Office of Personnel Management. (n.d.). Succession risk assessment. Retrieved from https://www.opm.gov/services-for-agencies/workforce-succession-planning/succession-planning/#url=Succession-Risk-Assessment.

Vendrell, E., & Watson, S. (2010). Emergency response plan. Retrieved from https://www.sciencedirect.com/topics/computer-science/emergency-response-plan.

Wallace, M., & Webber, L. (2011). *Disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets*. (2nd ed.). New York: American Management Association

Wayland, B. A. (2015). *Emergency preparedness for business professionals: How to mitigate and respond to attacks against your organization*. Oxford, UK: Butterworth-Heinemann.

Wester, J. (2019). Charlotte matched 2018 homicide total in less than 6 months. What happens now? Retrieved from https://www.charlotteobserver.com/news/local/crime/article230476619.html.