Stansfield Capstone Final Draft

by Craig Stansfield

FILE	10616_CRAIG_STANSFIELD_STANSFIELD_CAPSTONE_FINAL_DRAFT_1599558_835447324.DOCX (1M)		
TIME SUBMITTED	01-SEP-2019 10:32AM (UTC-0400)	WORD COUNT	9359
SUBMISSION ID	1165858387	CHARACTER COUNT	54062

Datacenter Alternate Site Selection: Requirements, Criteria, and Application

Craig Stansfield

MGMT 850 Strategic Management Integrative Capstone

Granite State College

September 5, 2019

Table of Contents

Abstract

The purpose of this research project is to develop a deeper understanding into the criteria that is used to select an alternate location as a fail-over site for information technology infrastructure. This alternate site would be activated after loss of equipment or facilities at the primary location due to manmade disruption or natural disaster. The research conducted intends to develop the distance and geography requirements needed to provide a secure location to restore critical functions and provide continuity of operations for the New Hampshire Army National Guard Datacenter. This project will explore ideal and best-case scenarios for alternate site considerations through the use of Graphical Information System database and research of critical infrastructure within the State of New Hampshire. Constraints will be placed on alternate locations due to unique topographic and meteorological considerations and the requirement to position the secondary site at an appropriate National Guard facility.

Keywords: Continuity of Operations, Business Continuity, Disaster Recovery

Acknowledgments

I would like to offer thanks to the professors and fellow students at Granite State College for their guidance and support throughout the entire program of study. Specifically, Kathy L. DesRoches for providing steadfast encouragement and wisdom during the Integrative Capstone project.

I also extend my thanks to the many member of the New Hampshire Army and Air National Guard for thier knowledge and expertise which provided clarity and insight during the research phase of this project.

Finally, I express my heartfelt appreciation to my wife and two children. Without their support and understanding, this undertaking could not have been successful.

Introduction

Founded in 1636, the United States National Guard was formed by citizen soldiers who desired to protect their families and businesses from hostile natives or foreign invaders. Originally the National Guard was established in the face of growing threats to local communities in colonial America. The Guard has since taken a role as an important component of the United States Military, with both an Army and Air National Guard in all 50 States, and four U.S. Territories. Today the National Guard has a unique dual-role responsibility. The first role is as a ready force for the Governor of each state to call upon in case of natural disaster, civil disturbances, or perform rescue services. To perform the secondary role requires the federalization of the National Guard by the President to perform combat duties as an Operational Force beside the Regular U.S. Army. The National Guard needs to stand ready to protect the homeland, as well as be prepared to mobilized and deploy globally when required.

The primary purpose of this project is in support of the National Guard as a Federal and State of New Hampshire ready response force for the President of the United States and the Governor of New Hampshire. New Hampshire National Guard forces are maintained to ensure a ready for that can be mobilized during a time of war, natural disaster, or civil disturbance. The National Guard trains one weekend each month, and is called to active duty for two weeks a year to maintain readiness and familiarity with their weapons, systems, and equipment. To support the needs of the over 2000-member part-time force, the State of New Hampshire maintains a contingent of over 700 full-time members to ensure continuity between training periods.

In support of the full and part-time forces, the New Hampshire Army National Guard (NHARNG) maintains a state of the art, fully virtualized Server and Network infrastructure. This Information Technology (IT) equipment supports the requirement to have accessible and

accurate information on the soldiers, equipment and financial transactions. These records are needed to determine vital information such as special skills and qualifications that Soldiers possess to build rosters, create task forces, and select the appropriate soldier for each mission. Federal financial information is stored and processed to support pay and purchasing transactions. These operations ensure all Soldiers are properly paid, and Unit equipment is purchased, and government acquisitions are satisfied.

The primary NHARNG datacenter is located at the New Hampshire State Military Reservation (SMR) in Concord, NH. The physical location is protected by fencing, and stationary and roving security forces. The datacenter is secured inside the facility behind cryptographic locks, closed circuit television monitoring and thermal sensors. The datacenter is well protected as it contains all the databases, servers, networking and telephony equipment necessary to maintain all IT related Mission Essential Functions needed to sustain operations for the NHARNG and provide the required ready force. The critical information residing in this IT infrastructure not only has to be correct, but be available at all times. This requirement drives the necessity to have a fault tolerant and available solution to continue operations in the event of loss or damage of the primary facility.

Currently, the NHARNG operates an alternate site containing a near mirror of all requirements necessary to perform critical functions in the electrical room at the Manchester Armory, located in Manchester, NH. This facility contains adequate electrical power, with a stand-by generator to provide backup power during an outage. This site also contains the Internet Service Provider point of entry as a means of establishing connectivity back to the primary location via the internet. The location also contains a streamed copy of all data present at the primary site. Additionally, weekly full and daily incremental backups of all critical data is stored

at both the primary and alternate site. As a further method of protection, data from all Federal Databases of Record is exported nightly via a VPN tunnel to the Vermont Army National Guard datacenter in Colchester Vermont. This method of copying files provides a very basic backup of critical data as a tertiary method of defense from loss.

On the surface, it would seem that the NHARNG data infrastructure is well-protected, with robust security controls, fire suppression, multiple locks, and redundant equipment at two locations. The close geographic proximity between the primary and alternate sites has been identified as a concern. The Manchester Armory is 15 miles, straight-line distance from the datacenter located at the SMR in Concord, NH. Both sites are connected along the Interstate 93 corridor, and both share a close proximity to the Merrimack River. These facilities are both located within a few miles from major population centers and could both potentially be desirable targets for terrorist or extremist activities. The primary datacenter is located in-line with the Concord Municipal Airport runway with low flying aircraft routinely passing close to the structure.

Literature Review

Throughout history there has been an intrinsic need to record events and information about society, and to preserve that knowledge for future generation's consumption. Evidence of this need to retain and protect documents can be witnessed by the architects of American freedom. There were an estimated 200 copies of the Declaration of Independence created in 1777 after the original signing, of which only 26 are known to exist worldwide today (Harvard University, 2019).

The original framers of the Declaration knew that this document would need to be preserved, this was done through stone pressing and the process of wet transfer (National

Archives, 2018). The stone pressing process preserved the words on the document, the data needed to recreate the original. This procedure is similar to data protection method of backing up raw data files and keeping exact duplicates of the original information. The alternate method of wet transfer allowed for an exact copy of the document, to include the signatures. This replication comes at the cost of transferring a portion of original ink, leaving the original lighter after each subsequent replication. On 15 December 1952, 176 years after the original signing that the document was enshrined in glass and protected for future generations (National Archives, 2018).

Today the Declaration of Independence and the remaining pressed and transferred copies are either properly protected at the National Archives in Washington D.C. (National Archives, 2018) or distributed throughout locations in the United States and the United Kingdom. This could be seen as an early example of implementing a business continuity or disaster recovery strategy, backing up and multi-site storage of critical information. The protection of this founding document represents the need for information and data security, duplication and fault tolerance.

Managerial Responsibilities and Regulatory Requirements

In an ideal world, systems would not fail, and hardware and software would operate flawlessly. Systems would be impervious to natural disasters, human errors, and malicious intent. There is an inherent responsibility as a manager to protect the continuity of operations of the department that they are charged with. In the early days of computing through the 1970's, the high cost of equipment coupled with the lack of understanding lead to the creating what is known as a Single Point of Failure (SPOF) (Bahan, 2003). Early systems rapidly developed into critical pieces of infrastructure. Businesses began to move from paper files into the developing digital

architecture in the 1970s (Tsatsou, 2016). These automated systems became the most essential part of the infrastructure for most large organizations.

Digital expansion occurred throughout all sectors, private and public. The first systems were low powered, slow and expensive, and demand was quickly increasing. With the rise in reliance on business systems there came two requirements: develop the ability for communication between systems, and eliminate the single point of failure architecture (Bahan, 2003) .

The internet made its first appearance in the 1960s as part of the United States Advanced Research Projects Agency (ARPA) which eventually became the Defense Advanced Research Projects Agency (DARPA) (Tsatsou, 2016). Originally used for defense purposes, the ARPANET was duplicated in the civilian arena around 1965 when the first simple Wide Area Network (WAN) was created by Lawrence Roberts (Tsatsou, 2016). After Mr. Roberts developed the first packet-switching network, he became employed by ARPA (Tsatsou, 2016). This technology advancement in the 1960s lead to the development of nuclear blast tolerant Ethernet topology in 1973 which is the most commonly employed internet technology today (Tsatsou, 2016).

In 1983 (Tsatsou, 2016) the ARPANET project was split from a purely government technology into a secondary usage, the World-Wide Web. This internet technology continued along its path at an exponential rate until reaching a more mature status in the 1990s (Tsatsou, 2016).

Today, more than 80% of the United States population now has access to the internet (Camille, 2018). This level of internet can be attributed to the reduction in cost and the incremental increases in speed and reliability (Camille, 2018). Technology has become

accessible to almost all individuals, businesses, and government agencies. The ease of acquiring the technology has provided the conduit that is used to transfer organizational data and information globally (Martyushev & Bogdan, 2016).

The development of internet infrastructure that was tolerant to failure was done by designing the architecture of the systems to be more resilient through the use of more durable components. In the 1960's and 1970's, owning computer equipment was expensive, and the ability to own redundant systems was cost prohibitive (Bahan, 2003). Redundant Array of Inexpensive Disks (RAID) were developed in 1987 (Martyushev & Bogdan, 2016). This technology allowed information to span over several inexpensive hard disks providing hardware fault tolerance. These RAID arrays, effectively provided protection of data locally (Martyushev & Bogdan, 2016). This solved one matter, but did not address the issue of a catastrophic loss of the site as a whole.

In addition to the expectations of an employer that a manager would have a plan in place to continue operations in the wake of a devastating loss, there also may be regulatory requirements and legal statutes that need to be followed starting in the 1970s (Snedaker, 2014). Therefore, a loss of facilities, equipment, power or connectivity, may require a business continuity plan by law (Snedaker, 2014). Public, private, and governmental agencies have multiple levels of regulatory guidance that must be followed.

Most corporate legal obligations are industry specific. With invention of the internet, ecommerce and online markets and banking have emerged legislation aimed at protecting consumers and ensuring financial obligations are met to the government. (Snedaker, 2014) Among these are Security and Exchange Commission's regulations for publicly traded

corporations, security regulations to protect consumer credit information and finances, and protections to ensure confidentiality of personal and health information (Snedaker, 2014).

Federal organizations are also required to adhere to the Federal Information Security Management Act (FISMA) regulations and meet the restrictive requirements of the Defense Information Security Agency (DISA) guidelines. Adherence to these stringent requirements is required and routinely audited in the form of compliance inspections (Department of the Army, 2019). The New Hampshire Army National Guard (NHARNG) is further restricted or regulated by Army Regulation AR 25-2 Army Cybersecurity (Department of the Army, 2019) and the National Guard Regulation NGR 130-6 United States Property and Fiscal Officer Appointment, Duties and Responsibilities. The Data Processing Centers in each state, is the NHARNG entity which maintains the Army National Guard data and infrastructure. These regulations provide a framework and minimum-security guideline for system confidentiality, integrity and availability (Department of the Army, 2019).

Managing Risk and the Business Impact Assessment

The term risk is broad in scope and can relate to many categories or types of risk dependent on the context. From the standpoint of information technology infrastructure, risk is the amount of exposure that systems or facilities from internal or external threats or disruption. Unwanted results could be the outcome from not properly understanding, assessing or preparing for risks within an organization. This can lead to mission failure, loss of expected functions, financial loss or injury, or in extreme cases, and death of personnel (Gustin, 2010). Some examples for potential personnel injury could be, not having proper fire suppression systems, physical security measures, or electrical grounding. The consequence for lack of preparation can

result in damage to image or reputation, loss of productivity, or legal liability. (National Institute of Standards and Technology, 2011) Snedaker states that risk can be defined using the formula: "Risk = Threat + (Vulnerability + Likelihood) + Impact" (Snedaker, 2014, p. 157)

The National Institute of Standards and Technology (NIST) is the Risk Management Framework. Risk management is the multi-step process of analyzing the likely threats or hazards to personnel, facilities or equipment (Gustin, 2010). To probe the level of risk for a given situation, one must assume hazards to determine the impact and likelihood of occurrence of each risk (National Institute of Standards and Technology, 2011). For example, a threat that would have a catastrophic effect, but an insignificant possibility of occurrence may be have less consequence than a very common, less harmful hazard. Once the magnitude and likelihood of a risk have been identified, it must be eliminated, mitigated, or accepted. (Snedaker, 2014) Not all risk can be excluded or alleviated, there will always be a residual amount or risk (National Institute of Standards and Technology, 2011).

Risk Tolerance is the level of residual risk that an organization is willing to accept and operate under (Snedaker, 2014). The response to the accepted risk could be the result of the probability of a threat from extremely low, low impact financially, or the cost to implement the controls to mitigate the risk is too high. All entities have different appetites and allowances for risk and there is a tradeoff between operational and fiscal priorities. (National Institute of Standards and Technology, 2011)

The tool to identify the level of acceptable risk in the form of downtime, damage, data-loss, financial cost or personal injury is the Business Impact Analysis (BIA) (Bahan, 2003). The BIA is the founding process that enables the understanding of the level or risk tolerance an

organization has (Krahulec & Jurenka, 2015). This process helps quantify the risk mitigation strategy to determine the organizational impact realized after an event.

The value of data as a commodity has risen while the tolerance for loss of integrity and availability has declined (Bahan, 2003). This is particularly true in the online market arena, where system outages directly translate to lost revenue (Bahan, 2003). The BIA helps to identify the critical systems and processes needed to sustain operations and the impact of a partial or complete loss of these components. This analysis focuses on the information security triad, confidentiality, integrity and availability (Swanson, Bowen, Wohl Phillips, Gallup, & Lynes, 2010).

According to the National Institute of Standards and Technology, the BIA is performed in four steps;

1. Determine business processes and recovery criticality,
2. Identify outage impacts and estimated downtime,
3. Identify resource requirements, and
4. Identify recovery priorities for systems

(Swanson, Bowen, Wohl Phillips, Gallup, & Lynes, 2010). The output of this analysis is the determination of the Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO) and Recovery Point Objective (RPO) (Bahan, 2003). These time standards are calculated during the creation of the BIA and are unique for each organization (Snedaker, 2014).

The MTD characterizes maximum amount of time management authorizes that systems can be unavailable in a given event (Bahan, 2003).

RTO represents the maximum amount of time a specific or process can be offline before it has detrimental effects on other components (Swanson, Bowen, Wohl Phillips, Gallup, & Lynes, 2010).

Finally, RPO denotes the maximum age of the data that will be recovered from previous system backups. This factor will specify how often data is protected within an organization's environment (Bahan, 2003).

Continuity of Operations (COOP) Site Selection Criteria

The Continuity of Operations (COOP) Plan is the process followed by an organization to restore mission essential functions (MEF) after a catastrophic event. The COOP site is an alternate location where all functions required to sustain the organization can be performed until the primary site has been restored (Swanson, Bowen, Wohl Phillips, Gallup, & Lynes, 2010). The Maximum Tolerable Downtime is determined during the Business Impact Analysis and provides the level at which alternate site should be developed and equipped.

An alternate site is a location that can owned, leased or under a memorandum of agreement, from an external organization, where mission essential functions can be relocated to during a period of system unavailability (Bahan, 2003). Generally, an alternate site is only activated for large scale disruptions or for testing of functionality and not used for minor events. The alternate site should be sized, equipped, and operational to support the BIA functionality requirements. These sites are delineated into five groups; Cold Sites, Warm Sites, Hot Sites, Mobile Sites, and Mirror Sites (Swanson et al., 2010).

Relocation to an alternate site may be performed for multiple reasons. The reason to activate an alternate site could be as simple as a regulatory required test, to a catastrophic and total loss of the primary site (Swanson et al., 2010). The origin of the loss of functionality at the

primary location could be infrastructure system failure, malicious attack, or facility loss via manmade or natural event or loss of power or environmental controls. (Cappelletti, 2002) These categories of failures and attacks should be identified during a vulnerability assessment as part of the BIA prior to selecting an alternate location.

The three most common sites, cold, warm and hot are chosen in relation to the level of business continuity required upon determination of the MTD. Cold Sites encompass the most basic features, generally power and communication infrastructure. A cold site may or may not have the ability to support operations, but generally do not have any internal infrastructure (National Institute of Standards and Technology, 2011). Expected return to operation time for a cold site could be from multiple days up to a month or more.

A Warm Site will contain all the necessary power and communications infrastructure found in a cold site, as well as most, if not all, of the hardware requirements to perform disaster recovery operations (Swanson et al., 2010). A warm site has the organizational systems ready to accept all of the data, but will require human interaction to prepare and configure the systems to perform MEFs. Recovery time for a warm site, is much shorter, from hours to a week to be in full operation.

A Hot Site is the most advanced and ready state of the three common alternate sites. The site is pre-staged with all communication, power and hardware requirements in place and operational. This site will also be properly configured, with near real-time data and requires minimal human intervention to bring into operation. These sites can quickly transition in to operation and start performing mission critical functions within minutes to an hour (Swanson et al., 2010).

The final two less common alternate site options are the Mobile Site and Mirrored Site. A mobile site is a portable, easy to relocate, deployable IT infrastructure asset. This self-contained system typically has power and communications on-board, along with hardware ready to accept data from the most recent off-site backup (Swanson et al., 2010). The final site, the most complex and costly is the Mirror Site, it is an exact replica of the primary site. This site could be fully automated to transition to operation immediately upon loss, or outage of the primary location (Swanson et al., 2010). This site provides 100 percent fault tolerance and delivers instantaneous continuity of operations (Swanson et al., 2010).

When considering an alternate site type, there are many location criteria to be considered. The first is geographic the distance from primary site (Perry, 2019). This needs to be a balance of being far enough from the original location to avoid reliance the same critical infrastructure which are affected by the same catastrophic event as the primary location (Perry, 2019). This includes reliance on separate electric power grids, water and sewer systems, and data and voice communication networks. At a minimum, the site should be located no closer than five miles from any primary location which could be a likely candidate for a terrorist activity. These can include large metropolitan areas, federal facilities, near power plants or transportation hubs. A further consideration to the 5-mile distance would be prevailing winds to avoid effects from nuclear or chemical fallout (Perry, 2019). The alternate site should be located where displaced personnel can receive life support in the form of food and water, hotels, and medical facilities (Department of Homeland Security, 2004). Consider geography to ensure that a manmade or natural event at the primary site won't affect the alternate, this may include occupation of the same flood plain or earthquake fault-line.

Conversely, a site too far from the primary site could interrupt the accessibility of displaced personnel to travel to the secondary site. While meeting the minimum distance requirements, Maximum Tolerable Downtime must be considered by calculating travel time into the formula (Swanson et al., 2010). The alternate site should ideally have multiple ingress and egress routes to ensure access from different directions.

Security is a concern to protect the personnel and infrastructure located at the site. Depending on the industry, and sensitivity of the alternate site, protection could vary from a door lock, to fencing, video surveillance and armed security personnel. The purpose for relocation, such as a terror attack, also influences the level of security implemented (Department of Homeland Security, 2004).

Information Technology Infrastructure Vulnerabilities and Threats

Examples of system failures could be in the form of spontaneous loss of hardware, software, or networking equipment (Cappelletti, 2002). Generally speaking, there are built-in redundancies in components that commonly fail, such as power supplies or hard disks. Certain expensive components such as large-scale blade-server shelters or core network routers can become a single point of failure at given site. Environmental systems such as cooling and dehumidification systems failures can also cause activation of the alternate processing site (Gustin, 2010).

Malicious attacks in the form of a harmful software attack such as a virus or other malevolent code that can cause a local or distributed outage. A denial of service (DOS) attack can accomplished by inundating systems with internet traffic, externally by hackers, or internally from an insider threat (Cappelletti, 2002). Other manmade threats include terrorist attack, arson, theft, or vandalism (Gustin, 2010). Any attack by an individual or group on the facility that

renders it inoperable, will trigger moving mission critical functions to the alternate site. Many manmade threats can be mitigated through the use of security and implementing information assurance vulnerability scanning and remediation (Department of the Army, 2019).

The final category of threats to an organizations information technology infrastructure are unpreventable and often destructive natural hazards. These can be fires, floods, hurricanes, winter storms, tornadoes or earthquakes (New Hampshire Department of Safety, 2019). Each of these events require care assessment as they can cause wide-spread damage and lead to secondary and tertiary threats to personnel and infrastructure. These events can cause systematic losses of facilities and produce large financial strains on agencies and civilian organizations (Gustin, 2010).

Agencies should develop appropriate and proportional countermeasures for each threat determined in the vulnerability assessment. Countermeasures should be developed when considering the magnitude and the likelihood of a specific event. For example, in the North East, the magnitude of volcanic activity would be cataclysmic to personnel and infrastructure, but the probability of an event is inconsequential (Beckett, 2014). New England is prone to winter storms which can cause distributed power and communication outages. A proper response to this threat could be placing an alternate site on separate power grid and different Internet Service Provider (ISP) connection to the internet (Department of Homeland Security, 2004). The overarching goal is to ensure an equal response to all threats, while maintaining MEFs. This response should be mutually supported within the business impact analysis performed prior to alternate site selection (Swanson et al., 2010).

This project will analyze the natural and manmade threats to the New Hampshire Army National Guard datacenter and determine the ideal facility to relocate the alternate site. The

purpose of relocating the alternate site is to provide independent infrastructure and protection using geographic separation. The overarching goal is to ensure a threat or disruption at the primary location will not disturb the alternate site.

Framework for Analysis

The outcome of researching and evaluating alternate site locations can lead to an almost immeasurable number of criteria to be assessed. The potential threats to Information Technology infrastructure are numerous. Some risks can be remediated with minimal effort or can be neglected completely, depending on geographic location. The question this research paper endeavors to answer is, where is the ideal location for New Hampshire Army National Guard to move its alternate site to ensure the continuation of Mission Essential Functions upon loss of the primary site?

The list of potential risks to a facility or equipment is nearly immeasurable, and would be impossible to discuss all conceivable threats. The first step is eliminating those with an infinitesimal probability regardless of magnitude of damage they could inflict. Many of these risks will be mitigated in preparation for common phenomena. An example would be the distance needed to protect a facility from a hurricane could diminish the threat of an asteroid strike.

Certain threats to IT infrastructure will be applied at the primary and secondary sites regardless of their geographic locations. Many of these controls are mandated in the Army Cyber Security Regulation. These include virus scanning and remediation, internet firewalls, intrusion detection systems, and software updates (Department of the Army, 2019). Additionally, standard facility equipment such as standby generators and fire suppression, as well as the application of routine firmware and hardware updates.

For this research paper, the threats considered will be grouped into three categories, human, natural and environmental (Swanson et al., 2010).

- Human - malicious actor, terrorism, human error
- Natural - weather events, hurricanes, tornados.
- Environmental - power or network outage, climate control failure

These risks will then be evaluated for the impacts against the infrastructure and how to best mitigate the threat. Physical separation, geographic formations, external electrical and communication infrastructure, and physical security equipment will be assessed as possible means of protection.

Human threats can come in many different forms, some physical others digital. Common digital attacks are from malware or denial of service attack (Zipfel, 2019). Malware is harmful code, or software applications that are unknowingly installed into systems that can destroy, damage, or exploit computer systems, usually for nefarious purposes (Hardikar, 2019). A denial of service attack occurs when an information system or network receives an overwhelming amount of malicious traffic or data making the resource unavailable to legitimate users (Cybersecurity and Infrastructure Security Agency, 2009)

Human physical threats could be deliberate or accidental. Accidental threats to systems could be carelessly damaging equipment, improper configuration, or unintentional destruction of facilities. Deliberate actions could come in the form of malicious insider activity, terrorism, arson, theft of property.

Natural dangers to systems and facilities are those that cannot be controlled such as severe weather or earthquakes. For this paper, common or likely environmental effects for the New England region will be established and evaluated. Incidents which have an extremely low

or negligible potential will be disregarded. The last Volcanic activity in New England occurred over 100 million years ago (National Oceanic and Atmospheric Administration, 2010). However, it is possible for a volcano to form but the likelihood would be so remote that it would not justify resources planning for an occurrence.

Environmental threats often are temporary in nature such as a localized power outage due to an accident or non-climate event (Swanson et al., 2010). Mitigation of environmental threats takes analysis of communications and electrical supply sources. If possible, alternate facilities should be on isolated infrastructure from the primary location to avoid affecting both facilities.

The model that I have selected to perform my analysis of the threats and evaluation criteria is the U.S. Army Military Decision Making Process (MDMP) (Headquarters Department of the Army, 2012). This analytical decision-making tool assists in the development of distinct courses of action, and aid in their evaluation and eventual selection. This nine-step process is at the core of staff level decision making for the U.S. Army. During MDMP, multiple sub steps are used to drill into an assigned mission and perform a deep analysis of the requirements. This provides a visualization of the environment and more thorough understanding of mission which leads to the determination of the required end state.

The Military Decision-Making Process (MDMP) is primarily used for detailed planning at the tactical, operational and strategic levels of the U.S. Army (Headquarters Department of the Army, 2012). The origins of MDMP can be traced back for thousands of years but first appeared in Army doctrine just prior to WWI. (COL Paparone, 2001) The process contains seven steps: (Headquarters Department of the Army, 2012, pp. 2-12).

1. Receipt of Mission
2. Mission Analysis

3. Course of Action (COA) Development
4. Course of Action (COA) Analysis
5. Course of Action (COA) Comparison
6. Course of Action (COA) Approval
7. Orders Production

The first two steps of this process were performed during the initial weeks of class. The Receipt of Mission was twofold, the first being the guidance from NGR 130-6 requiring the implementation of a Continuity of Operations Site (Departments of the Army and the Air Force National Guard Bureau, 2007). Secondly, the formal receipt of mission given in week one of this course was to select a Capstone Project. The second step of the MDMP process, Mission Analysis, has been an ongoing process presented in the Literature Review and the Framework for Analysis sections of this paper.

Methods

The method used to evaluate selection criteria will vary depending on the individual risk or threat associated with it. There will be some commonalities associated with responses for different threats, such as physical distance from the primary to alternate site. The variance will depend on the type of threat, such as a hurricane would require a further distance between sites than a tornado. Therefore, if both events are equally likely, planning for the effects of a hurricane, would also provide protection for other events.

The evaluation of manmade digital threats will be intentionally disregarded for the purpose of this report. The assumption being made is that all digital architecture will meet or exceed the cyber security requirements for all U.S. Army Information Systems (Department of

the Army, 2019). Threats of this nature would initiate the movement of operations from the primary to alternate site, but have minimal effect on the location or physical security.

A known constraint for this research project is that the New Hampshire Army National Guard (NHARNG) alternate infrastructure site will reside within the state boundaries. This simplifies the analysis as the primary site location on the State Military Reservation is within a 4-hour driving radius of the entire state, assuming normal road conditions. The furthest most National Guard Armory is located in Lancaster, NH, which is located roughly 35 miles from the international border with Canada, and less than a two hour drive from the primary site (Google, 2019).

Risk to the primary site from a physical, either accidental or deliberate can be averted or mitigated by increasing the distance between sites, or avoiding similar potential targets or analogous population centers (Department of Homeland Security, 2004). For instance, if the primary site is located near a likely terrorist target such as a metropolitan area, the alternate site should be based in a rural area. The minimum distance considered should be 5 miles from critical infrastructure or potential target and 60 miles from the primary site (Perry, 2019). The distance between two locations should be far enough to discourage a coordinated attack of both locations simultaneously. These threats could vary in size from localized rioting, through arson, or as large a terrorist action or nuclear threat.

Natural disasters are those that cannot be influenced by mankind, they can only be protected against. These natural risks will be evaluated based upon the specific threats facing the Northeast United States. According to the New Hampshire Department of Safety the most likely sources for natural disasters in New Hampshire as (New Hampshire Department of Safety, 2019):

- Floods – Most likely natural threat in New Hampshire, and occur yearly in some part of the state. Generally caused by continuous rainfall over multiple days or during the spring due to snow melt. (New Hampshire Department of Safety, 2019)
- Hurricanes – The largest threat from hurricanes comes in the form of a storm surge which can lead to inland flooding from heavy rainfall. They can produce severe wind leading to property damage and power outages. (New Hampshire Department of Safety, 2019)
- Tornadoes and Severe Winds – On average one or two tornados are recorded yearly in NH. Most tornados are small in size and only cause minimal damage. The most damaging tornado on record in NH was categorized as an EF-2 with almost 160 mph winds that effected multiple counties in southern through central NH. (New Hampshire Department of Safety, 2019) Tornados can destroy facilities, electrical and communications infrastructures leading to long-term power outages and equipment damage.
- Severe Winter Storms – Winter storms become a menace to information technology infrastructure due to the potential for strong winds and heavy snow which can make roadways impassible and lead out power and communication outages (New Hampshire Department of Safety, 2019).
- Ice Storms – Similar to Winter Storms, ice storms also have the potential for reduced mobility, but may lead to widespread and severe power and communication outages. These storms have the ability to damage communication towers and lines by depositing ice onto lines, or by bringing down trees or limbs. Return to operation times are often long due to debris left behind from the storm. (New Hampshire Department of Safety, 2019)

- Thunderstorms – Primarily a threat during the summer months, powerful lightning strikes can directly impact communications and power equipment, but also bring hail, strong wind and flooding to bear (New Hampshire Department of Safety, 2019).
- Earthquakes – The USGS has deemed NH to be an area of moderate seismic hazard (US Geological Survey, 2014) NH records one or two small scale earthquakes annually ranging from a magnitude 2.0 to 3.5. (New Hampshire Department of Safety, 2019). The risk to NH from earthquakes is high due to dated infrastructure that does not meet current standards for earthquakes. Additionally, a powerful earthquake in NH has the ability to cause damage over a larger area due to the composition of the earth below the state. The geological make up of NH could allow seismic activity to travel up to 40 times further than in other parts of the county (New Hampshire Department of Safety, 2019).
- Wildland Fires – Historically, New Hampshire experiences two large forest fires per century, with the last major wildfire season occurring in the 1940s (New Hampshire Department of Safety, 2019). The potential for a damaging fire season is past due by 20 years (New Hampshire Department of Safety, 2019). A wildfire could have the potential to cause damage to both facilities and infrastructure.

Each threat that poses a potential to cause service disruptions or damage to facilities and equipment will be evaluated individually to determine the proper countermeasure. These threats may require both distance and a separation based upon geological and geographical differences throughout the state of New Hampshire. Potential countermeasures could be:

- Increased distance between primary and alternate site. This will be an additive distance, the threat that requires the furthest distance will supersede any lower threat.

- Relocation of the alternate site to an area that will provide safety by being established on an isolated:
    - Power grid
    - Communications demark
    - Flood plain
    - Seismic threat area
    - Forest management area.

Results

To determine the results of this project, multiple categories of threats that are relevant to an IT datacenter within the State of New Hampshire were taken into consideration. Among these are geography, geology, municipal infrastructure and potential for terrorism. Some events were deemed to be extraordinarily low probability, for example volcanic activity, and disregarded

Appendix A provides a map produced by the Geographic Information System (GIS) used by the New Hampshire Army National Guard (NHARNG). This graphic displays New Hampshire National Guard armories and the Pease Air Force Base location as they are distributed throughout the state. Relevant factors such as distances, direction, and critical infrastructure was plotted and overlaid on this map using the ESRI Geographic Information System Company software, ArcGIS (ESRI Geographic Information System Company, 2019).

The ArcGIS software and the New Hampshire Army National Guard Domestic Operations (DOMOPS) database were leveraged to display and analyze the effects of threats and on the primary site. The overlays created allowed inferences to be made upon other armory locations, for potential similar effects to the primary site. The DOMOPS GIS database contains

multiple layers indicating critical information about the State of New Hampshire, for example; flood zones, electric transmission lines and topography.

This graphical representation of the information provided the ability to create a matrix of threats presented to each armory location. Appendix B lists the 28 New Hampshire Army and Air National Guard locations. For simplicity the nine buildings located on the State Military Reservation (SMR) in Concord, NH were treated as one facility and referred to as the SMR. This reduced this to number of facilities considered to the primary site, Building A, located on the SMR, and 20 potential secondary locations.

The factors analyzed for each location were assigned a score from zero to three depending on the aggravating or mitigating effects of their geographic location. The factors evaluate were:

- Distance from Primary Location – Straight-line distance from Building A to secondary location. A score was assessed based on distance. Less than 25 miles received a zero, this distance would have very minimal mitigating factors to separate the primary and secondary locations and an agreed upon minimum distance given by the Deputy Chief of Staff Information Management (DCSIM) (LTC Groton, 2019). The further the distance from the primary, the higher the score awarded:
    - Less than 25 miles – zero points
    - 26 to 35 miles – one point
    - 36 to 45 miles – two points
    - 46 miles or more – three points
- Hurricane Effect – This was a determination whether a hurricane would have a higher, equal, or lesser effect at the alternate than the primary site. The primary site in Concord, NH is

roughly 40 miles from the Atlantic Ocean. As a hurricane travels inland the energy available is reduced, lessening the damaging force of the storm (National Oceanic and Atmospheric Administration, 2016).

- Power Service – This analysis of the power transmission lines throughout New Hampshire concluded whether the electrical service to the alternate site was on the same transmission line, or had multiple paths to other suppliers. A score of zero was given for the same service, one point was awarded for multiple paths.
- Wildfire Concern – This evaluation involved researching each armory location and ascertaining the level of forestation around a potential secondary location via satellite imagery. An interview of a representative from the Society for the Protection of New Hampshire Forests determined there were no location in New Hampshire with an higher than average threat of wildfire (Weisiger, 2019). Locations with little or no local tree cover were awarded three points or two points for moderate tree coverage.
- Seismic Activity – The threat level of Seismic Hazard was gauged by information provided by the United States Geological Survey (USGS) Earthquake Hazard Program. Armory locations were plotted on the USGS Seismic Hazard Map (United States Geological Survey, 2014). There were three threat regions exhibited on the USGS map, points were conferred depending on their level of threat in relation to the rest of New Hampshire. The seacoast and central regions presented the greatest risk for a damaging earthquake, mid-west to lakes region a moderate concern, and northern portion of the state the lowest threat.
- Distance from the Seabrook Nuclear Power Plant – During an event at a nuclear power plant, locations ten miles from the site could receive direct ionizing radiation and sites up to 50 miles would be affected by contamination (Ready Department of Homeland Security , 2019).

Sites that were located within 50 miles of the Seabrook Nuclear Power Plant were awarded zero points, sites beyond 50 miles were given on point.

- Potential for Terrorism – All military facilities inherently are potential targets for terrorism (U.S. Army Cyber Command, 2017). Pease Air Force stands out among the other NH National Guard military locations due to their larger number of personnel and high valued refueling aircraft. Other factors in increasing the risk of terrorism could be critical infrastructure or highly populated areas. The 20 potential secondary locations were evaluated based on these criteria and were assessed a higher score for a lower potential for terrorism.
- Internet Service Provider Connectivity (ISP) – Though an incredibly important factor when considering potential alternate sites for disaster recovery, all armory locations in New Hampshire provided the potential for multiple paths and providers. Given this ability to choose isolated providers, this criteria was deemed irrelevant and was not evaluated.

The main finding was that the furthest north active armory location in Littleton, NH through this analysis was determined to be the highest rated site with a total score of 16. Appendix C is a simplified matrix sorted from the highest to lowest scores assigned. The Berlin, NH armory and Lancaster, NH armory both scored highly, 16 and 15 respectively, but were disqualified due to their inactive status. Lebanon, NH also was deemed a potential for consideration at a score of 15. Of the remaining armory locations, seven were disqualified due to their close proximity, less than 25 miles, from the primary location.

Discussion and Analysis

The primary datacenter in Concord, NH meets all physical security and is protected from cyber-attack in accordance with the Army Regulation 25-2, Army Cyber Security (Department of the Army, 2019). The systems contained in the datacenter are under 24-hour closed-circuit

television surveillance, FM-200 clean agent fire suppression system, and protected from heat and humidity by means of redundant industrial environmental units. The equipment is housed inside a concrete building, in an access-controlled area, behind a cryptographic lock and further confined inside a secured server cabinet. The entire State Military Reservation (SMR) is protected behind a fence with a 24-hour manned security check points and roving patrols.

The systems and facility have been secured from most average threats both physical and cyber. The facility faces other threats, though less probably, could have catastrophic effects on the sensitive hardware and data. The SMR is the second largest military facility in the State of New Hampshire making it a potential for terrorist activity. Furthermore, the Concord Municipal Airport runway 17 is located 1600 feet from the datacenter. This runway which can support aircraft as large as a Boeing 727 is located in-line with the datacenter facility, causing low flying aircraft to routinely pass over the building (Concord Municipal Airport, 2019). In addition to the threat from aircraft, the facility is approximately one-half mile from a FEMA designated flood zone. Finally, the building surrounded on two sides by the endangered Karner Blue Butterfly sanctuary. This woodland area does not receive wildfire preventive treatment to safeguard this protected species (Weisiger, 2019).

After completion of the analysis of the 20 potential locations for an alternate datacenter for the NHARNG, 11 sites remained as viable candidates and 9 were regarded as disqualified. The Berlin and Lancaster armories were disqualified as they have been taken out of operation by the Senior Army Staff. These two locations no longer house units, or full-time staff and are now under control of the State of New Hampshire for municipal usage.

The other locations on the SMR, the AASF flight facility and the Pembroke Edward Cross Training Center all fall within 2 miles of the primary datacenter and were immediately

disqualified. Franklin, Hillsboro, Hookset and Strafford are all located within 22 miles of the principal location. These locations were disqualified based on the consideration that the current alternate site located in Manchester and is 14.6 miles from the primary. The cost and time required to relocate the infrastructure from Manchester to one of these nearby facilities would not be feasible or permissible. Of the remaining armory locations, eight were determined to be valid, but scored 30% lower than top two site except for Plymouth. The Plymouth Armory scored nearly as high as the top two locations, but located on the same electrical transmission line as the primary site.

Three potential Courses of Action (COA) were generated upon completion of the site surveys:

- COA 1: Littleton, NH – The Littleton armory had the highest score (16) of any valid armory location. This facility is located north of the White Mountains providing a differing weather pattern found in Concord region, a lower potential for disruption via hurricanes, and a very low potential for terrorism. The facility is located on the outskirts of the town of Littleton, providing access to life support items such as hotels, stores and hospitals. Its location is 48 miles from the international border with Canada, though it is buffered by the State of Vermont. Interstate 93 connects the two locations with a drive time of 1.5 hours during standard conditions. Littleton receives on average more than 25” to 50” of snow annually in comparison to Concord, Manchester or Lebanon, NH (National Oceanic and Atmospheric Administration, 2019).
- COA 2: Lebanon, NH – The Lebanon armory received a score of 15. This location has many favorable qualities including close proximity to two hospitals, multiple power transmission lines, and a one-hour drive time from Concord on Interstate 89. The site is located 48 miles

northwest of the primary datacenter and south of the White Mountains. Due to the geographic similarity to Concord and location, this site will observe similar weather patterns and snowfall annual totals (National Oceanic and Atmospheric Administration, 2019). Several adverse characteristics became apparent upon closer analysis of the facility's location. The armory is positioned 150 feet from a FEMA designated flood zone, during periods of unusually heavy rainfall, this location could experience water damage before the primary site. The town of Lebanon, NH is situated in a moderate area of seismic activity. Those this area has a lower hazard than the primary datacenter, it is higher than the Littleton facility.

- COA 3: Manchester, NH – The final course of action would be to retain the alternate datacenter in its current location in the Manchester Armory. This solution is the most cost effective as it will require no additional expense to move equipment and data circuits. In addition, the facility will require further hardening for physical security and the installation of environmental equipment controls to maintain temperature and humidity levels. Aside from the cost savings, the Manchester Armory location was evaluated with a score or eight, half the score of other locations it was compared with. The Manchester armory experiences nearly all the same threats as the primary site. Moreover, the armory additionally is located in the largest city in New Hampshire which increases the threat of terrorist activity. The datacenter equipment is protected by simple lock and key doors. The facility is without external physical security fencing and does not have assigned security guards.

This study of potential alternate datacenter locations contained a number of constraints to the analysis that hindered selection of the most ideal disaster recovery location. The New Hampshire National Guard (NHNG) is a state entity residing under the control of the Governor of New

Hampshire. This restricted site selection to current NHNG facilities all of which were located within 100 miles or less of the primary datacenter in Concord, NH. Ideally, an alternate datacenter should be located 200 – 300 miles from the primary to ensure absolute segregation from geographic, geological and climate influences (Swanson et al., 2010). Additionally, the alternate datacenter location should be decided as part of a larger strategic plan for Continuity of Operations (COOP). Further constraints may be enacted on the alternate datacenter location upon approval of the NHARNG COOP plan.

Recommendations

In conclusion, relocation of the alternate datacenter from Manchester, NH to the Army National Guard armory located in Littleton, NH is the preferred course of action. At 77.4 miles from the primary datacenter, the Littleton location provides the best protection against human, natural and environmental threats. In every category evaluated, this location exceeded or matched the protections provided by the current alternate location. Furthermore, this location provides a segregation from all critical infrastructure in the Concord, NH region.

The New Hampshire Army National Guard protects its data at three locations. The primary in Concord, NH, the secondary location, currently in Manchester, NH, and tertiarily at the Vermont Army National Guard Headquarters in Colchester, VT. Currently the primary and alternate datacenters contain similar information technology infrastructure, and an exact replica of data at both locations.

Currently, the tertiary site in Colchester, VT, contains partial data and no further hardware. A data storage device will be moved to the Vermont location within the next year, and

be capable of storing an exact replica of all NHARNG data at their secured facility. The facility will provide data protection, but will not contain the hardware to allow disaster recovery.

The potential move of the alternate datacenter from the Manchester location to the Littleton armory reduces the distance between the secondary datacenter to the tertiary storage location. The current distance of 134 miles would be reduced to 69 miles providing the potential to develop alternate means of internet connectivity such as Worldwide Interoperability for Microwave Access (WiMAX) technology or dedicated fiber optic lines. Both technologies would allow for alternate paths for the data to travel between primary, alternate and tertiary locations.

This study was designed to provide an increased understanding of ways to best protect the NHARNGs critical data and increase its availability during times of state and national emergency. This data provides the National Guard the ability to provide a ready force of Soldiers and Airmen to respond to natural disasters and civil disturbances. Without this information, units would be unable to mobilize, pay and equip military members effectively during a call to defend the homeland.

References

Bahan, C. (2003). *The Disaster Recovery Plan*. North Bethesda: SANS Institute.

Beckett, D. (2014). *National Response and Disaster Recovery Frameworks*. New York: Nova Science Publishers.

Camille, R. (2018). *Computer and Internet Use in the United States 2016*. Washington, DC: United States Census Bureau.

Cappelletti, C. (2002). *Designing and Implementing a Disaster Recovery Plan*. North Bethesda, MD: SANS Institute.

COL Paparone, C. R. (2001). US Army Decision Making, Past, Present and Future. *Military Review*, 45-53.

Concord Municipal Airport. (2019, August 28). Retrieved from Concord New Hampshire: https://www.concordnh.gov/344/Concord-Municipal-Airport

Cybersecurity and Infrastructure Security Agency. (2009, November 04). *Understanding Denial-of-Service Attacks*. Retrieved from National Cyber Awareness System: https://www.us-cert.gov/ncas/tips/ST04-015

Department of Homeland Security. (2004). *State and Local Government Continuity of Operations Planning:*. Washington D.C.: Department of Homeland Security.

Department of the Army. (2019). *Army Cyber Security*. Washington DC: Department of the Army.

Departments of the Army and the Air Force National Guard Bureau. (2007). *United States Property and Fiscal Officer Appointment, Duties and Responsibilities*. Arlington: National Guard Bureau.

ESRI Geographic Information System Company. (2019, August 28). *NGNH DOMOPS View Web App*. Retrieved from New Hampshire National Guard GIS: https://ngdomops.maps.arcgis.com/apps/MapSeries/index.html

Google. (2019, August 4). *Google Maps*. Retrieved from Google Maps: https://www.google.com/maps/dir/Lancaster,+New+Hampshire/4+Pembroke+Road,+Concord,+NH/@44.6826671,-72.2716743,9z/data=!4m14!4m13!1m5!1m1!1s0x4cb40e0f649f2edb:0xb5936cc429430be6!2m2!1d-71.5692477!2d44.4889204!1m5!1m1!1s0x89e26a455a229fbf:0x3e5a35a4775ee6c3

Gustin, J. F. (2010). *Disaster & Recovery Planning : A Guide for Facility Managers*. Lilburn, GA: Fairmont Press.

Hardikar, A. (2019). *Malware 101 - Viruses*. North Bethesda, MD: SANS Institute.

Harvard University. (2019, 07 24). *How many copies were originally made of the Declaration of Independence? Were they all signed?* Retrieved 07 24, 2019, from https://declaration.fas.harvard.edu/

Headquarters Department of the Army. (2012). *ADRP 5.0 The Operations Process*. Washington D.C.: United States Army.

Headquarters Department of the Army. (2012). *ADRP The Operations Process*. Washington, D.C.: United States Army.

Krahulec, J., & Jurenka, M. (2015). Business Impact Analysis in the process of business continuity management. *Security and Defence Quarterly Vol 6 Iss 1*, 29-36.

LTC Groton, B. W. (2019, August 15). Deputy Chief of Staff, Information Managment. (C. B. MAJ Stansfield, Interviewer)

Martyushev, N., & Bogdan, A. (2016). *High Technology: Research and Applications*. Pfaffikon, Switzerland: Trans Tech Publications.

National Archives. (2018, May 14). *The Declaration of Independence: A History*. Retrieved July 24, 2019, from https://www.archives.gov/founding-docs/declaration-history

National Institute of Standards and Technology. (2011). *Managing Information Security Risk*. Gaithersburg, MD: US Department of Commerce.

National Oceanic and Atmospheric Administration. (2010, August 25). *Geological Origin of the New England Seamount Chain*. Retrieved from NOAA: https://oceanexplorer.noaa.gov/explorations/03mountains/background/geology/geology.html

National Oceanic and Atmospheric Administration. (2016, June 28). *What are hurricanes? What happens during a hurricane?* Retrieved from National Data Buoy Center: https://www.ndbc.noaa.gov/educate/hurr.shtml

National Oceanic and Atmospheric Administration. (2019, August 27). *Average Annual Snowfall (1981 - 2010 Normals)*. Retrieved from National Weather Service: https://www.weather.gov/btv/climate

New Hampshire Department of Safety. (2019, August 4). *Natural Hazards*. Retrieved from Homeland Security and Emergency Management: https://www.nh.gov/safety/divisions/hsem/NaturalHazards/

Perry, S. A. (2019, March 14). *Alternate Sites for Continuity of Operations Plan (COOP) Relocation*. Retrieved July 26, 2019, from GSA General Services Administration: https://www.gsa.gov/directive/alternate-sites-for-continuity-of-operations-plan-(coop)-relocation

Ready Department of Homeland Security . (2019, August 27). *Nuclear Power Plants*. Retrieved from Ready.gov: https://www.ready.gov/ur/nuclear-power-plants

Snedaker, S. (2014). *Business Continuity and Disaster Recovery Planning for IT Professionals*. Waltham: Snygress.

Swanson, M., Bowen, P., Wohl Phillips, A., Gallup, D., & Lynes, D. (2010). *Contingency Planning Guide for Federal Information Systems NIST Special Publication 800-34 Rev. 1*. Washington D.C.: National Institute of Standards and Technology.

Tsatsou, P. (2016). *Internet Studies: Past, Present and Future Directions*. New York: Routledge.

U.S. Army Cyber Command. (2017, July 13). *SECURITY FACT SHEET: Antiterrorism Awareness*. Retrieved from U.S. Army Cyber Command:

https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/1440622/security-fact-sheet-antiterrorism-awareness/

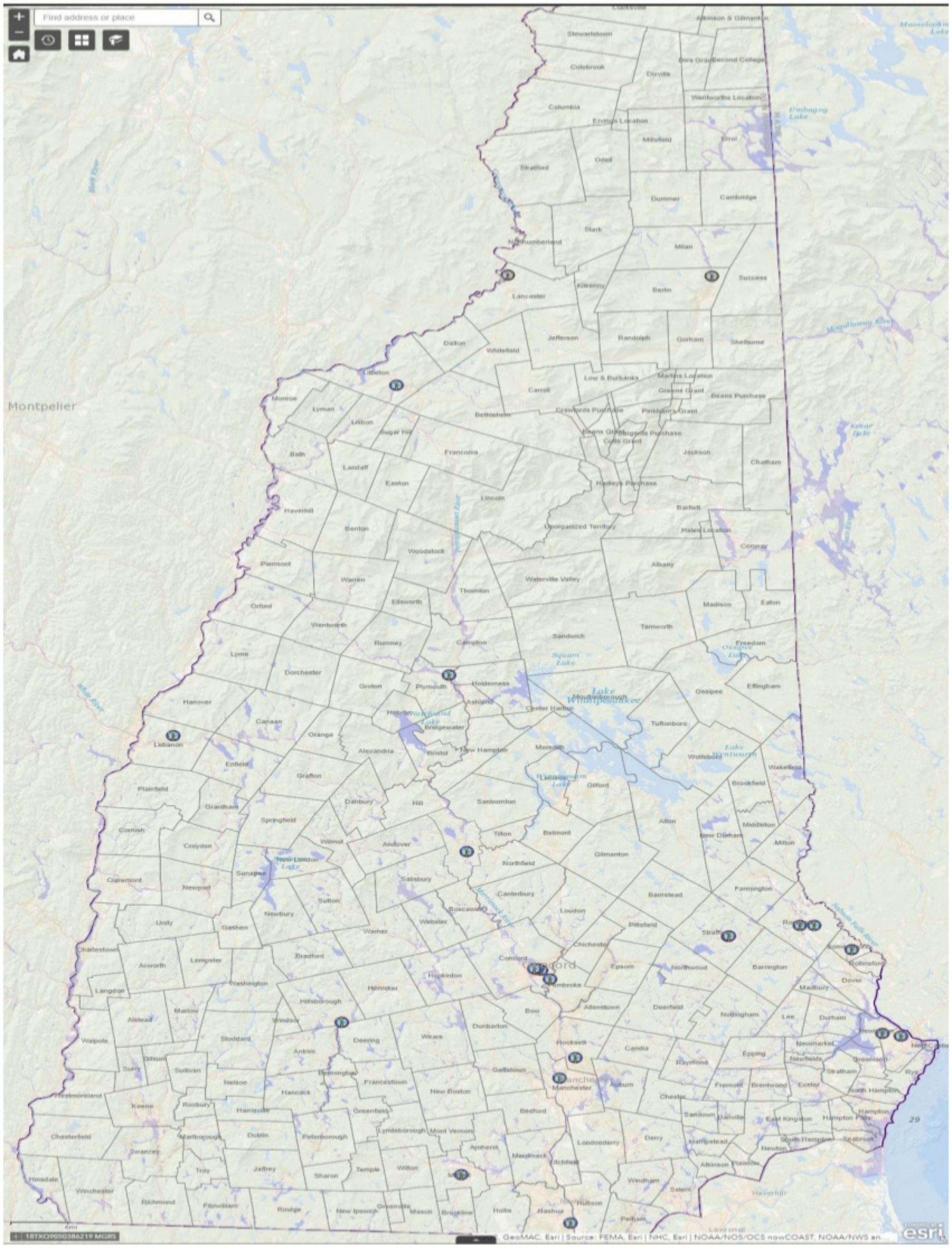
United States Geological Survey. (2014, August 27). *Information by Region-New Hampshire*. Retrieved from United States Geological Survey: https://earthquake.usgs.gov/earthquakes/byregion/newhampshire-haz.php

US Geological Survey. (2014). *Information by Region - New Hampshire*. Retrieved from 2014 Seismic Hazard Map: https://earthquake.usgs.gov/earthquakes/byregion/newhampshire-haz.php

Weisiger, W. L. (2019, August 16). Managing Forester. (C. Stansfield, Interviewer)

Zipfel, F. (2019). *Understanding the Virus Threat and Developing Effective Anti-Virus Policy*. Norht Bethesda, MD: SANS Institute.

Appendix A


Find address or place
Montpelier
Lake Winnipesaukee
GeoMAC, Esri | Source: FEMA, Esri | NHC, Esri | NOAA/NOS/OCS nowCOAST, NOAA/NWS an...
esri

Appendix B

Site	Status	Distance (Bldg A)	Score	Hurricane	Score	Power Service	Score
SMR - Bldg. A	Primary	0					
Manchester	Alternate	14.6 Miles	0	Equal	2	Same xmsn line	0
SMR, Concord	Disqualified	< 1 Mile	0	Equal	2	Same xmsn line	0
AASF, Concord	Disqualified	< 1 Mile	0	Equal	2	Same xmsn line	0
Berlin	Out of Service	92.6 Miles	3	Lesser	3	Alternate path	1
Franklin	Disqualified	17.0 Miles	0	Lesser	3	Same xmsn line	0
Hillsboro	Disqualified	21.1 Miles	0	Lesser	3	Alternate path	1
Hooksett	Disqualified	12.3 Miles	0	Equal	2	Same xmsn line	0
Lancaster	Out of Service	90.0 Miles	3	Lesser	3	Same xmsn line	0
Lebanon	Valid	47.8 Miles	3	Lesser	3	Alternate path	1
Littleton	Valid	77.4 Miles	3	Lesser	3	Alternate path	1
Milford	Valid	28.2 Miles	1	Lesser	3	Alternate path	1
Nashua	Valid	33.9 Miles	1	Higher	1	Alternate path	1
Pease ANGB	Valid	36.0 Miles	2	Higher	1	Alternate path	1
Pembroke ECTC	Disqualified	1.9 Miles	0	Equal	2	Same xmsn line	0
Plymouth	Valid	39.1 Miles	2	Lesser	3	Same xmsn line	0
Portsmouth	Valid	38.7 Miles	2	Higher	1	Alternate path	1
Rochester - Brock	Valid	26.9 Miles	1	Higher	1	Alternate path	1
Rochester - Bisson	Valid	28.9 Miles	1	Higher	1	Alternate path	1
Somersworth	Valid	31.6 Miles	1	Higher	1	Alternate path	1
Strafford	Disqualified	20.0 Miles	0	Equal	2	Alternate path	1

Site	Status	Wildfire	Score	Seismic	Score	Seabrook	Score	Total
SMR - Bldg. A	Primary	Mod		Highest		< 50 Miles		
Manchester	Alternate	Low	3	Highest	1	< 50 Miles	0	8
SMR, Concord	Disqualified	Mod	2	Highest	1	< 50 Miles	0	7
AASF, Concord	Disqualified	Mod	2	Highest	1	< 50 Miles	0	7
Berlin	Out of Service	Mod	2	Lowest	3	50+ Miles	1	16
Franklin	Disqualified	Low	3	Highest	1	50+ Miles	1	11
Hillsboro	Disqualified	Low	3	Highest	1	50+ Miles	1	12
Hooksett	Disqualified	Low	3	Highest	1	< 50 Miles	0	9
Lancaster	Out of Service	Mod	2	Lowest	3	50+ Miles	1	15
Lebanon	Valid	Mod	2	Moderate	2	50+ Miles	1	15
Littleton	Valid	Mod	2	Lowest	3	50+ Miles	1	16
Milford	Valid	Mod	2	Highest	1	< 50 Miles	0	11
Nashua	Valid	Low	3	Highest	1	< 50 Miles	0	9
Pease ANGB	Valid	Low	3	Highest	1	< 50 Miles	0	9
Pembroke ECTC	Disqualified	Low	3	Highest	1	< 50 Miles	0	8
Plymouth	Valid	Low	3	Moderate	2	50+ Miles	1	14
Portsmouth	Valid	Low	3	Highest	1	< 50 Miles	0	10
Rochester - Brock	Valid	Low	3	Highest	1	< 50 Miles	0	10
Rochester - Bisson	Valid	Low	3	Highest	1	< 50 Miles	0	10
Somersworth	Valid	Low	3	Highest	1	< 50 Miles	0	10
Strafford	Disqualified	Mod	2	Highest	1	< 50 Miles	0	9

Appendix C

Site	Status	Distance	Hurricane	Power	Wildfire	Seismic	Seabrook	Terrorism	Total
SMR - Bldg. A	Primary				Mod	Highest	< 50 Miles	Mod	
Littleton	Valid	77.4 Miles	Lesser	Alternate path	Mod	Lowest	50+ Miles	Low	16
Lebanon	Valid	47.8 Miles	Lesser	Alternate path	Mod	Moderate	50+ Miles	Low	15
Plymouth	Valid	39.1 Miles	Lesser	Same xmsn line	Low	Moderate	50+ Miles	Low	14
Milford	Valid	28.2 Miles	Lesser	Alternate path	Mod	Highest	< 50 Miles	Low	11
Portsmouth	Valid	38.7 Miles	Higher	Alternate path	Low	Highest	< 50 Miles	Mod	10
Rochester - Brock	Valid	26.9 Miles	Higher	Alternate path	Low	Highest	< 50 Miles	Low	10
Rochester - Bisson	Valid	28.9 Miles	Higher	Alternate path	Low	Highest	< 50 Miles	Low	10
Somersworth	Valid	31.6 Miles	Higher	Alternate path	Low	Highest	< 50 Miles	Low	10
Nashua	Valid	33.9 Miles	Higher	Alternate path	Low	Highest	< 50 Miles	Mod	9
Pease ANGB	Valid	36.0 Miles	Higher	Alternate path	Low	Highest	< 50 Miles	High	9
Manchester	Alternate	14.6 Miles	Equal	Same xmsn line	Low	Highest	< 50 Miles	Mod	8
Berlin	Out of Service	92.6 Miles	Lesser	Alternate path	Mod	Lowest	50+ Miles	Low	16
Lancaster	Out of Service	90.0 Miles	Lesser	Same xmsn line	Mod	Lowest	50+ Miles	Low	15
Hillsboro	Disqualified	21.1 Miles	Lesser	Alternate path	Low	Highest	50+ Miles	Low	12
Franklin	Disqualified	17.0 Miles	Lesser	Same xmsn line	Low	Highest	50+ Miles	Low	11
Hooksett	Disqualified	12.3 Miles	Equal	Same xmsn line	Low	Highest	< 50 Miles	Low	9
Strafford	Disqualified	20.0 Miles	Equal	Alternate path	Mod	Highest	< 50 Miles	Low	9
Pembroke ECTC	Disqualified	1.9 Miles	Equal	Same xmsn line	Low	Highest	< 50 Miles	Mod	8
SMR, Concord	Disqualified	>1 Mile	Equal	Same xmsn line	Mod	Highest	< 50 Miles	Mod	7
AASF, Concord	Disqualified	>1 Mile	Equal	Same xmsn line	Mod	Highest	< 50 Miles	Mod	7