SECURITY ASSESSMENT PLAN (DETROIT ENERGY)

Alok Kumar Dubey

University of the Cumberland's

ISOL699 - B01 Info Security Project

Dr. Machica McClain

12/4/2020

TABLE OF CONTENTS

INTRODUCTION

Detroit Energy is a utility company based in Detroit which serves more than a million customers. It provides essential services with the sole purpose of energy diversification. The Company is involved in the management and development of energy-related businesses and their services nationwide. Its central operational units are electric and natural gas utilities that serve more than three million citizens in Southern Michigan. The energy portfolio of DTE company also includes the non-utility energy businesses with a focus on power, natural gas, collection, and storage together with trading and marketing of energy (DTE Energy | About DTE, 2020).

Detroit energy electric produces, transmits, and distributes electricity to millions of customers within Michigan. Coal, nuclear fuel, hydroelectric pumps, and natural gas are the renewable sources used by Detroit energy to generate its electrical output with a system capable of at least 11,000 megawatts. Its nuclear plant energy capability has represented more than 35% of Michigan's total energy capacity (Nelson, 2017). The utility also operates gas energy engaged in the distribution, purchase, transmission, storage, and sale of natural gas in America and Canada. DTE has more than 200 storage well facilities, which approximates close to 30% of Michigan's underground energy working capacities (Serletis and Andreadis, 2004). As a result, there is a need to develop a security plan that would effectively enhance the Company's operations with defects or interference from intruders. This paper conducts a security risk assessment of the Detroit Company and ultimately designs a security plan implemented by the Company to enhance its operations.

BACKGROUND OF PRODUCTS AND SERVICES

Detroit Energy was established in 1903 by the famous Detroit Edison. The Company offers electric utilities, natural gas utility and non-electric utilities, which serve over 5 million

people across southern Michigan. Due to its economic sustainability, over 450 communities living in Detroit depend on the services and products of Detroit Energy. Over the years, DTE has established flexible, convenient, affordable, and environmentally friendly products, which have made the livelihood more comfortable, secure, and updated with ever dynamic changes in technology. The Company's energy utility has over 11000-megawatt system capacity, drawn from Hydroelectricity, Coal, natural gas, and nuclear energy.

A hydroelectric plant comprises three different operational parts: the electric plant where the production of electricity is done, a reservoir point to store water, and a dam that can be opened and closed to control the flow of water. The amount of electricity generated depends on the fall's height and the water flow through the system. Long-distance transmission of electricity to the consumer is done through the electric wire and can be controlled by installing transformers at distinct positions. On the other hand, Detroit uses coal, which is a combination of different combustible hydrocarbon gases. They are abundantly found deep underground or associated with other hydrocarbon materials such as petroleum and fossil fuels. Primarily, natural gas is mostly produced as a byproduct of oil production.

Primarily natural gas is purely made of methane. Its termed as 'wet' when methane is combined with other hydrocarbons such as propane and butane and 'dry' when it's pure methane. It's transmitted from the point of extraction to its point of use through a network of pipelines. Its mostly measure by volume consumed under normal pressure and temperature. Currently, the USA is the largest producer and consumer of natural gas.

Nuclear energy is generated from nuclear reactants. Scientist Fermi Enrico engineered the idea of nuclear power in the early 20th century. Enrico discovered how atoms could be split by neutrons when they come into contact. The nuclear chain reaction was first found in 1942 in

Chicago, USA. The most significant move was made in 1950 when the first electric power was generated by a series of scientists in Breed Reactor at Idaho. Uranium is the commonly used fuel for nuclear power because it easily split. Nuclear fission occurs when atoms and neutrons collide with atoms, making them break with heat production. This process leads to a chain reaction, thus making the response self-sustainable.

Benefits

The Company has employed more than 10,000 employees distributed across the 450 Michigan communities. The workforce is spread across a variety of services that are provided to its customers. Some of the services offered by DTE Energy include volunteerism, philanthropy, and economic progress. Thus, the Company has been rated one of the leading forces for Michigan's citizens' growth and development. The Company's sole mission is to be the top producer of cleaner, safer, and smarter energy in North America.

PURPOSE OF THE PLAN

This security assessment document provides the discussed utility (Detroit Energy) with enough methodology that can be used to conduct and plan for the physical and technical security systems. The report is yet to provide a thorough and enhanced consistency in the quality assessment process's actualization. This guide aims to be useful for the utility company at all departmental levels by implementing and actualizing essential security control applications. The information has been organized systematically to allow for easy asses and referencing when analyzing and actualizing the report.

The physical security plan provides guidance, sets responsibility, and sets the standards minimal for the security of personnel, assets, and properties. The physical security offers advice that will ensure the properties remains strong even in extreme conditions. For the good of the

article, this security assessment refers to prior measures of protection and defense against unauthorized or forceful attempts to access the institution's physical properties or the organization. On the other hand, a technical security plan incorporates the techniques required for authentication, authorization, and protection of sensitive data and information against malicious access and theft. This security applies to all institutions that rely on computer applications and other technologies in their operations. It entails detecting potential threats and loopholes in the system and provides the best solution in cases of attacks and intrusions.

SCOPE OF PROJECT

Detroit Energy requires a review of the utility to determine security vulnerabilities and provide suggestions for improvements. The security of the staff and the facilities is the primary focus for the document review. Secondary security consideration is placed on public safety.

a. Location selection. A review of the Detroit Energy security system is provided for the following locations: Office Security management, Detroit power plants and storage facilities, the customer buildings, and the transmission channels.

b. Necessary elements of review.

i. It is leading the evaluation and inspection of the aspects of the security features of the locations that have been identified above.

ii. Analysis of the strengths and weaknesses of the identified locations. Including assessment of the existing infrastructure and policies.

iii. Provide a summary of strengths and weaknesses for the identified locations.

iv. Provide a documented written summary of the suggested solutions to identify weaknesses. Resolutions to be separated according to ranks for the most significant vulnerabilities with the greatest risk of being exploited.

v. Cost range to be provided in cases where multiple solutions for the given risk.

vi. Provision of the submitted final report to the Detroit Energy management for further actions to be taken.

PROJECT CHARTER

(SECURITY ASSESSMENT PLAN)

D T E Energy Inc.

444 Wealthy ST

Detroit, Michigan 48226

Date

SECURITY ASSESSMENT PLAN (DETROIT ENERGY)

The charter permits the security assessment plan to effectively conduct a physical, technical, and administrative security risk assessment of Detroit energy and establish a remedial action plan for the Company. The security assessment plan will be availed to the Company's top management officials for approval. This assessment plan will entail the purpose of the security assessment, the scope of the project, the schedule, and the estimated budget for evaluation. The project will also include the designed infrastructure, which will provide an in-depth analysis of both the long-term energy security for environmental and economic prosperity. The infrastructure will also offer short-term energy security that highlights the energy production system's ability to

adjust to the expected and sudden threats that could hinder the supply of energy. All resources for assessment will be developed and designed by the department of human resources.

The security assessment plan's ultimate goal is to ideally improve Detroit's security measures by implementing and actualizing essential security control applications. This would enable the organization to determine security vulnerabilities and provide suggestions for improvements. This would significantly secure the Company's assets against cyberbullies and any other system intruders. The security of the staff and the facilities is the primary focus for the document review. Secondary security consideration is placed on public safety. The physical security plan provides guidance, sets responsibility, and sets the standards minimal for the security of personnel, assets, and properties. The physical security offers advice that will ensure the properties remains strong even in extreme conditions. For the good of the article, this security assessment refers to prior measures of protection and defense against unauthorized or forceful attempts to access the institution's physical properties or the organization. On the other hand, a technical security plan incorporates the techniques required for authentication, authorization, and protection of sensitive data and information against malicious access and theft. . The corrective actions for the energy security plan depend entirely on the remedial action plan. The infrastructure vulnerability can be identified based on the following approaches: Relocation, access control, facility design, and redundant sites.

The project manager of the organization will officiate the process, and he will be in charge of organizing, monitoring, controlling, and more so planning on how the assessment will be conducted and assigning responsibilities to the team works to ensure that the activities are completed within the project scope, time and budget.

The security assessment plan will be effectively conducted and submitted for approval as per the assessment schedule (timeframe) provided below. The resources will be assigned subsequently by the Company's human resource manager. The work is supposed to commence with due effect, i.e., about two to three days after resource allocation.

Schedule: Assessment Timeframe

Activity	**Duration**
Identification of energy sources and critical facilities	Week 1
Vulnerability Assessment Conduction	Week 2 and 3
Updating the Energy Security Plan	Week 4
Developing a Preparedness and Operation Plan	Week 4 and 5
Remedial Action Plan	Week 5, 6, and 7
Project Implementation Preparation	Week 7
Project Implementation	Week 8

The estimated budget for the security assessment plan's competition till implementation will be $217,500.00, and the Company's investment funds will fund it.

Declaration (Official only)

Approved by Detroit Chief Executive Officer

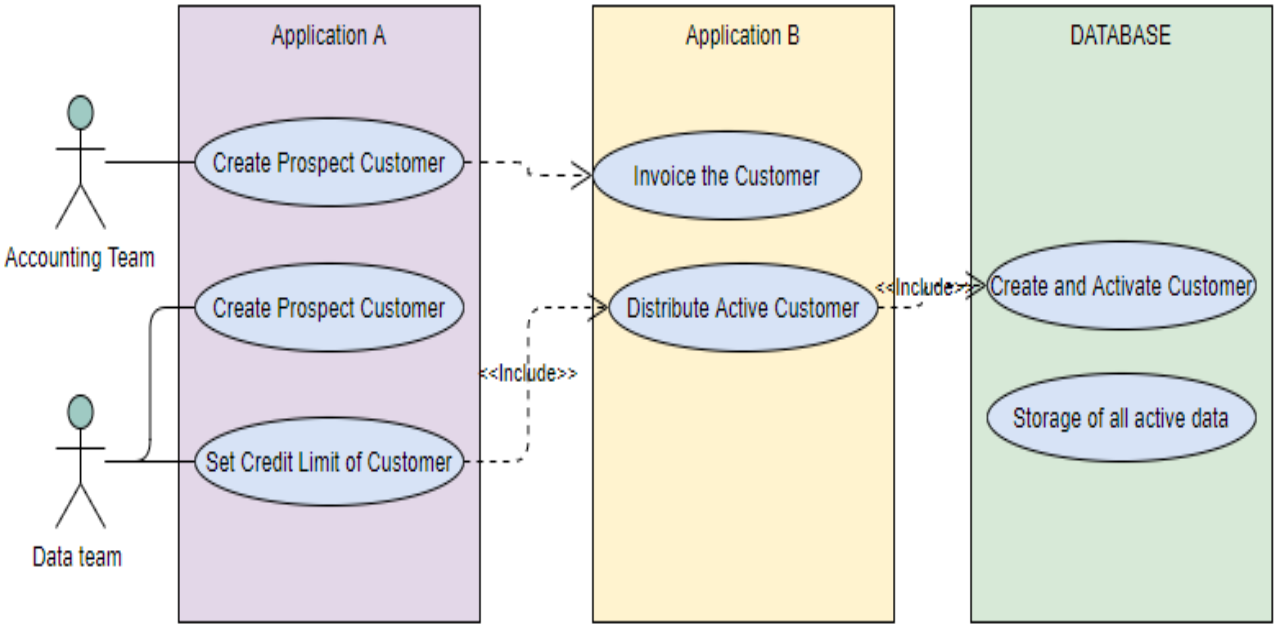
Name: _____

Sign: _____

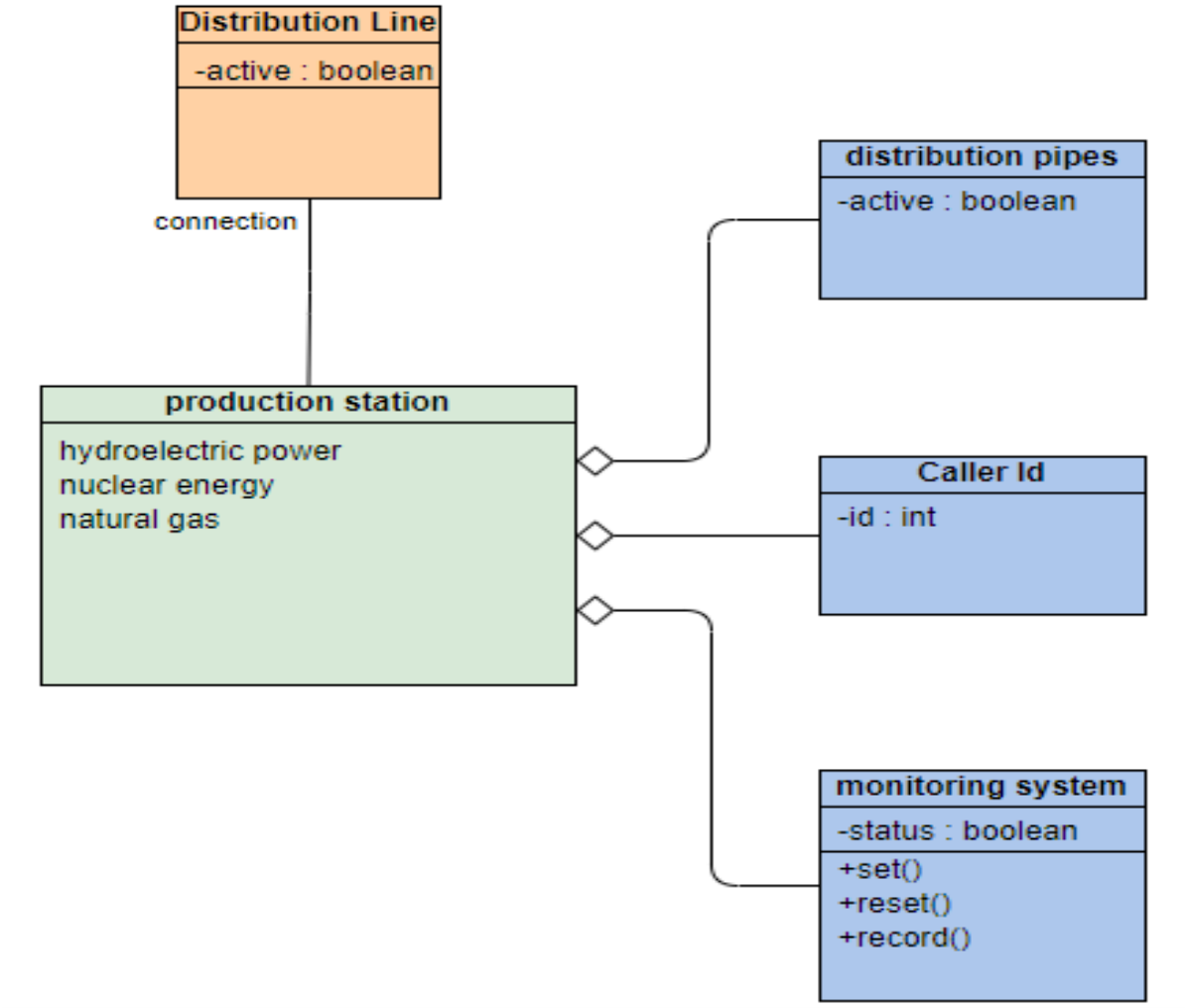
Date: _____

ORGANIZATION'S INFRUSTRUCTURE

(a) Database, applications, and communication



(b) Physical infrastructure



Energy security involves the production, storage, and distribution of energy without interruption of its availability. The above structure provides an in-depth analysis of both the long-term energy security for environmental and economic prosperity and short-term energy security that highlights the energy production system's ability to adjust to the expected and sudden threats that could hinder the supply of energy (Gupta et al., 2014). The analysis of possible hazards, their economic impact on the organization, and the administrative functions that could help promptly handle any of the risks and threats posed to the utility (Detroit Energy).

VULNERABILITY ASSESSMENT

PHYSICAL RISK ASSESSMENT

The section discussion evaluates the vulnerabilities of energy production and supply as electricity and natural gas. Maximizing the system's security involves an intense analysis of how different energy production elements interact to create a tight set of interdependencies. The three main requirements for an optimal and stable electrical system includes:

1. Availability of transportation network for fuel delivery
2. The clear communication channel between the control sector and data systems
3. Natural gas as fuel for both heating and electricity

The physical plan is involving three technical assessments:

Identification of energy sources

Energy sources and their storage facilities to be identified and assessed in detail before the vulnerability assessment. Different practices need to be followed to accomplish the best task above.

First, the site electrical system's description, the overall source, and the distribution system are the most critical aspects. The most significant emphasis on the on-site distribution system provides the full description of the power monitoring and control system, the noncritical switch off the system, and the alternate feeds. The off-site electrical system fully describes the off-site stations and the directly supplied power of the switching stations. The historical records that describe the off-site system's robustness should be analyzed as the critical/important data for documentation.

Description of the storage and the delivery facilities for the natural gases. The availability of fossil fuel, natural gases provides the dependency and the stability of the utility. The full

description of the piping and transportation of fossil fuel. The provision of the physical security of the storage facility and the distribution channels of the natural gas. The logistics and the system's general reliability are encoded to help for the site's vulnerability assessment.

Identification of critical facilities

The energy security plan foundation is based on the list of critical facilities. The consequence of each facility to interrupt the supply of energy needs to be considered by the board. Facilities that bring significant losses to the utility are thus termed as critical. Critical facilities to be identified, estimated on the amount of energy required to support the facility and the facilities' security to be reconsidered by the security manager. The elevation of energy emergency requirements to some of the buildings depends on the facility's emergency operations.

The facility's vulnerability alone should not be the relying information and the relevance of the identified facility and its importance. Grey areas in the decision-making process could be assumed as long as high standards for the critical facility definition are maintained. Misconceptions on the selection process to be identified, addressed and emphasized to be enhanced on the whole process during this stage. The assessment process to be done with concerns placed on energy security and the remedies on the energy plans.

Analysis of potential threats

Potential threats that may cause interruptions should be listed and given priority. The categories of the threats considered are Natural phenomena, failure of the equipment, or threats by employees or individuals with ill motives of causing an interruption. After identifying the critical energy source and facility, the extent of disruption of energy supplied to be assessed, and an estimate of the occurrence probability be made. It involves studying several possible threats

and the impact on the energy source of each threat. The potential impact and the chances of occurrence will allow for consideration of relative risks and risk remediation.

Natural phenomena such as earthquakes, floods, hurricanes, and ice storms could pose threats to energy sites depending on the utility's location. Extreme heat during the summer months applies to most areas but a few. The site-specific threats such as fire and mechanical or electrical failures can also threaten the utility (Broder & Tucker, 2018). Accidents can adversely impact the generation, transportation, and storage of the energy source. Accidents are bound to occur during maintenance, transportation, construction, or operations on energy systems. Human error can be the root cause of accidents. Cyber-attacks mostly initiate intentional threats on computer systems, contract defiance, vandalism, arson, or terrorism. Some of these attacks are considered nonviolent, such as strikes, while some, like terrorism, can seriously impact the system's security (Todorović & Todorović, 2020).

Performance of analysis based on the probability of occurrence should reduce the level of threats to the utility. Records on the most frequently occurred threats to be identified and analyzed and the mitigation measures to be implemented to minimize the extent of threat effect in re-occurrence.

Listing the unacceptable risks

This is the estimation of the impact and likely hood of threat occurrence that can cause damage to the organization and mitigation action put in place. This risk has a high probability and severe consequences for the organization (Broder & Tucker, 2018). The table below shows a list of the unacceptable risks identified by the results of vulnerability analysis.

Table 1 unacceptable risks

Priority	Facility	Threat	Impact	Recommendation

Hydro-electrical system				
1	Production	flood	medium	
2	Transportation	human	medium	
Natural Gas				
1	storage	Earthquake	high	
2	Transportation	Human	low	
Coal				
1	Production	Earthquake	high	
Nuclear energy				
1	Production	Human error	high	
2	Production	Mechanical failure	high	

TECHNICAL RISK ASSESSMENT

These are threats that come with the system without the involvement of external forces. The threats could be much severe, leading to data loss or interference with the system'regularal operation. Some of the risks posed include:

Computer security risks

Cybersecurity remains one of the biggest threats to energy utility as its random, and its occurrence remains unpredictable. Computer security possesses a significant impact on the data and information of the utility. The info could analyze energy production, customer data information, billing records, energy consumption records, or utility assets records.

Some of the threats posed by cybersecurity include unauthorized computer access such as backdoor Trojans, which allow for access by bypassing computer security protocols. This type of visa is remotely and vulnerable to systems connected over the internet. Bluejacking is the

computer risk that keeps sending unwanted messages to other email contact using Bluetooth. This threat distracts the system user by sending files, never meant to be sent. On the other hand, cookies are system threats that record the user's website for personal information. Cookies do not affect the computer system data, but they interfere with the user's confidentiality. Adware is a security risk that displays ads on the computer screen. They come in the form of pop-ups and banners used by advertising-supported software. The threat posed by the adware may include installed unwanted programs that are hard to uninstall or hijacked web browser that only displays adverts and sometimes records web information and communicating it to other users.

Other system security risk

The use of low-quality materials can result in advert security risk in energy production. For example, materials that could not withstand high temperatures in coal energy production could lead to the system's failures or even fire. Distribution of natural gas requires high pressure withstanding materials to prevent leakages, losses, and accidents.

ADMINISTRATION SECURITY MEASURES

Provision of an internal energy framework that governs the production and distribution of energy policies. The framework helps the administration with pre-identified procedures to be followed in case of security emergencies. The framework should explicitly provide energy infrastructure, interconnection, and supply. Budgeting of the energy provision needs to be considered (Gupta et al., 2014). The administration to consider the amount required for the sustainability of the production of clean and reliable energy, plus the determination of the sources of funds to the budget. This can be the internal fund allocation or funds from the multi-union organizations. Conduction of research activities in the energy field to be encouraged within the utility, aiming to develop and adopt new technologies to increase security in energy production

and distribution. Education and training of the workforce facilitate enough know-how issues in case of risks and guarantee to the utility (Abualkishik et al., 2020). The administration should consider the development of employees for the sole purpose of the Company's flexibility, stability, and standardization.

BUSINESS IMPACT ANALYSIS

Risks posed on the security of energy production can significantly pose a commercial impact on the organization's strategic, tactical, and operational activities. Disruptions on the output can hamper utility processes leading to a direct effect on production, delivery, and quality of energy consumed. Insecurity on energy production, such as cybersecurity, could compromise the entire SCADA system that manages customer relationships (Gupta et al., 2014). Interference with nuclear energy production by extreme weather conditions or earthquakes can potentially lead to an environmental disaster affecting both animals and plants. Industries depend on electricity as a source of power and raw material in their operations. Energy insecurity can significantly affect the production capacity of associate drives getting supplies from Detroit Energy by a large percentage (Abualkishik et al., 2020).

REMEDIAL ACTION PLAN

Disaster recovery is an energy security plan may be administrative, training, procedural, or upgrades of the infrastructures serving the site. The corrective actions for the energy security plan depend entirely on the remedial action plan. The infrastructure vulnerability can be identified based on the following approaches: Relocation, access control, facility design, and redundant sites ("Disaster recovery yellow pages: the definitive directory of business continuity & disaster recovery resources," 2017).

Identify Unacceptable Risks and Remedial Actions

The unacceptable risks identified should be accompanied by a brief list of solutions gotten from a brainstorming process. The suggested remediation needs to be quick for fast listing in case of urgency. Justifiable action is designed to give answers to scenarios with high occurrence chances and with high impact. Future assessment entirely depends on the utility stored data like better record keeping of energy outages, required restoration time, and improved records of accidents and fire.

The following practices need to be considered when dealing with disaster recoveries: First, the use of an up to date, quality technological solutions. The superior technology helps address energy solutions in a sweeping action and saves on the production cost, thus reducing the probability of unacceptable risks at various points. Secondly, have independently building surveys for accurate analysis of the affected site such as hospitals. Listening to the installation experts for priorities and selecting high-priority action from a list of proposed solutions for the urgently needed action.

Preparation of the remedial action plan.

Table 2 below shows the remedial action plan. The plan helps to prepare the immediate corrective actions and for easy access. The table copy is kept and updated yearly for the purpose of progress tracking and budgeting. It also helps to provide the project status, key goals, and accomplished milestones. The table is updated according to the working actions taken the previous year on a particular threat.

Deficiency	**Corrective action**	**Budgeting**	**Status**

Table 2

Projects from previous years

While analyzing the new proposal, energy security measures from previous years, both funded and ones not funded, should be reviewed for the actions on the risks posed and the possibility of incorporating it into the new plan. The list from previous years to be examined to validate the posted unacceptable risks, the predictable status of the utility (Energy system), and potentially taken actions could be applied based on the new technology. Previous projects provide in-depth information for the current risk and the best solution to handle the situation. Completion of the last year's tasks might help in taking risks posed in the current assessment. The funded projects should not be overlooked.

Provide alternative funding.

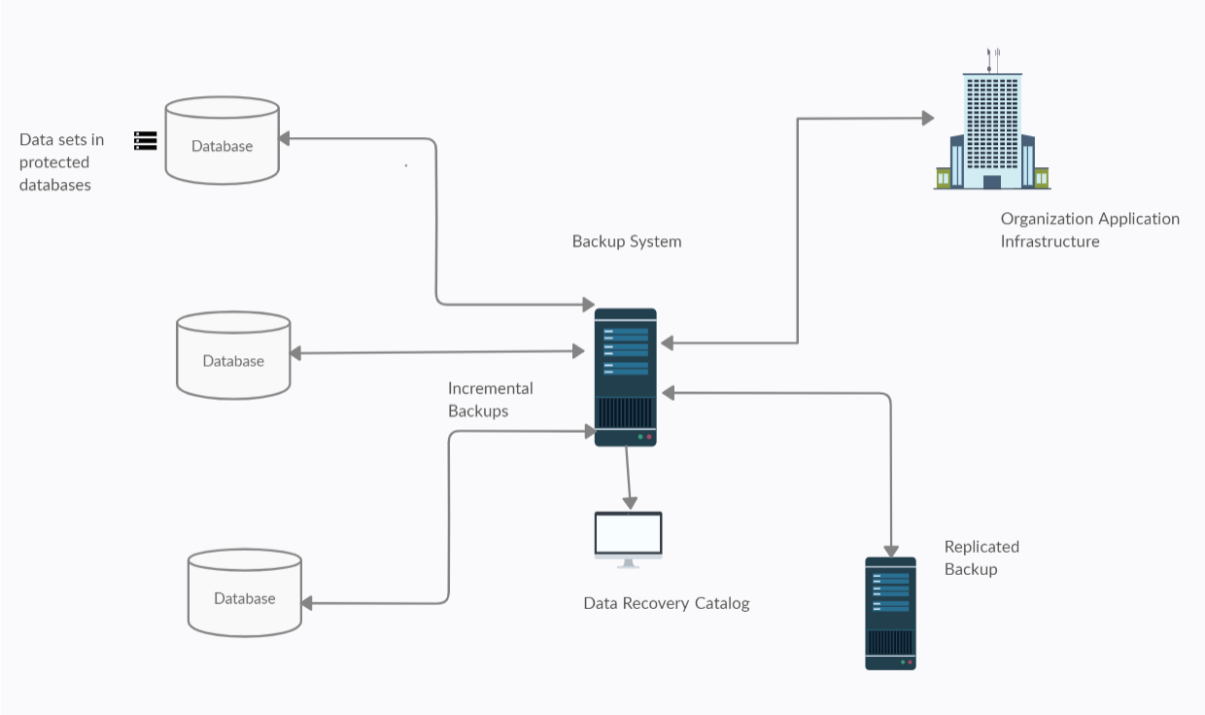
Obtaining funding for the energy security project may be difficult; thus, an alternative funding source to address disaster recovery. All funding alternatives should be listed for proper and appropriate steps in the funding request. The project size affects the funding of the report. Small energy security projects could be funded from an expected budget source, while large projects may require additional alternative sources such as savings, appropriate funds, and enhancements from privatization contracts. Having a specific financing option for large and costly projects helps ensure the availability of funds. Privatization of property by the government-owned commodities helps raise funds that could be used to fund some of the long-term, take-or-pay projects for energy services. Project streamlining and management could also help the government reduce funding projects using contracts to the private sectors with specialized skills (Hire et al., 2020).

BACKUPS

Management and enhancement of energy production and supply have been associated with response to problems and reduced power outages. Several ways can be incorporated for steady and reliable energy production. First, the reduction in energy consumption and an increase in production. Outsourcing of energy services from other utilities helps in the steadiness of supply and deliverance (Abualkishik et al., 2020). The exploitation of different regions for expansion of production for adequate energy supply. Employment of tracks and reports that verify resilience track on cost savings and report on the system's success and failures. Secondly, training and education on the implementation of specific strategies. Development of the strategic action plans helps in faster recoveries in case of disaster and insecurity by the provision of measures for goal achievement. Energy use profile helps track the distribution of energy use and identify the sources of each energy system.

Backup plan for the organization infrastructure

Data is a valuable asset to an organization; hence it is essential to protect against loss, corruption, or disasters. This calls for a need for a backup system alongside organization application infrastructure. A backup plan offers simplified operations to recovery in case of any disaster. This backup system implements incremental backup operations. This involves copying only the data that has changed since the last backup. Since it only copies data that has changed, this type of backup is faster and does not consume a lot of storage. The information is then stored in a protected database. The same may then be replicated in another backup system, thereby offering a back for the primary backup system fail.



DISASTER RECOVERY.

Disaster recovery is an energy security plan may be administrative, training, and procedural or upgrades of the infrastructures serving the site. The energy security plan's corrective actions depend entirely on the remedial action plan (Abualkishik et al., 2020). The infrastructure vulnerability can be identified based on the following approaches: Relocation, access control, facility design, and redundant sites ("Disaster recovery yellow pages: the definitive directory of business continuity & disaster recovery resources," 2017). Besides, the site-specific threats such as fire emergence due to electrical fault or mechanical failures can also cause danger to the Company's utility. Therefore, their recovery plan will entail conducting a performance analysis based on the probability of threat occurrence to minimize future occurrence of potential threats to the utility. The data in the back plan will also be useful in identifying,

analyzing, and establishing possible mitigation measures to be implemented to reduce the extent of the threat effect in re-occurrence.

RECOMMENDATIONS

The document has provided for the steps to be followed in the identification of deficiencies and security weaknesses. Therefore, the security manager implements the best feasible solution following the guide's disaster recovery. Application of the remedies should be consistent with a threat to the facility, utility mission, limits to the budget, available resources, current regulations, and urgency on the necessary action. The administration to consider the amount required for the sustainability of clean and reliable energy, plus the determination of the sources of funds to the budget. This can be the internal fund allocation or funds from the multi-union organizations. Conduction of research activities in the energy field to be encouraged within the utility, aiming to develop and adopt new technologies to increase security in energy production and distribution.

CONCLUSION

When used correctly in the utility, the above plan can significantly help identify loopholes within the system security. Costs could be reduced considerably through the implementation of the discussed recovery plans. The organization security manager is tasked with the frequent assessment of the utility security features to assess the likelihood of threats occurrence. Analysis of previously done reports helps open adverse more opinions and solutions in handling threats and recoveries from disaster occurrence. This plan provides Detroit Energy utility with a broad discussion on the security features. It can also be applied to any organization's task with the generation, distribution, and management of electric energy.

References

Broder, J., & Tucker, E. (2018). *Risk Analysis and the Security Survey* (4th ed., pp. 135-270). AMSTERDAM: Elsevier.

NELSON, A. (2017). Rise and Shine Detroit. Retrieved 1 December 2020, from https://www.nationalgeographic.com/travel/city-guides/detroit-traveler/

Andrews, C. (2009). Improving data security measures in business. *Computer Fraud & Security*, *2009*(8), 8-10. https://doi.org/10.1016/s1361-3723(09)70099-5

Disaster recovery yellow pages: the definitive directory of business continuity & disaster recovery resources. (2005), *43*(01), 43-0057-43-0057. https://doi.org/10.5860/choice.43-0057

DTE Energy | Home. Newlook.dteenergy.com. (, 2020). Retrieved 1 December 2020, from https://newlook.dteenergy.com/wps/wcm/connect/dte-web/home.

Hire, B., Boiler, 1., Boiler, 2., Boiler, 3., Boiler, 4., & Boiler, 1. et al. (2020). *Disaster Recovery Plans for Heating and Hotwater - Rapid Energy*. Rapid Energy Ltd. Retrieved 1 December 2020, from https://rapidenergy.co.uk/disaster-recovery-plans/.

Todorović, I., & Todorović, I. (2020). *Significant flaws in EPS environmental study for TENT A coal plant overhaul*. Balkan Green Energy News. Retrieved 1 December 2020, from https://balkangreenenergynews.com/major-flaws-in-eps-environmental-study-for-tent-thermal-power-plant-overhaul/.

Abualkishik, A., Alwan, A., & Gulzar, Y. (2020). *Disaster Recovery in Cloud Computing Systems: An Overview*. ResearchGate. Retrieved 4 December 2020, from https://www.researchgate.net/publication/344435966_Disaster_Recovery_in_Cloud_Computing_Systems_An_Overview.

Gupta, V., Goswami, S., Kumar, A., & Singh, M. (2014). *Networking and Security Measures*. ResearchGate. Retrieved 4 December 2020, from https://www.researchgate.net/publication/265141277_Networking_and_Security_Measures.