

Name/id: abdelkareem yousef mamdoh soubar/19110022

Assignment Title: X-Power

Course Tutor: Eng. Moath Sulaiman

Submission Date: 26/1/2022

**Introduction**

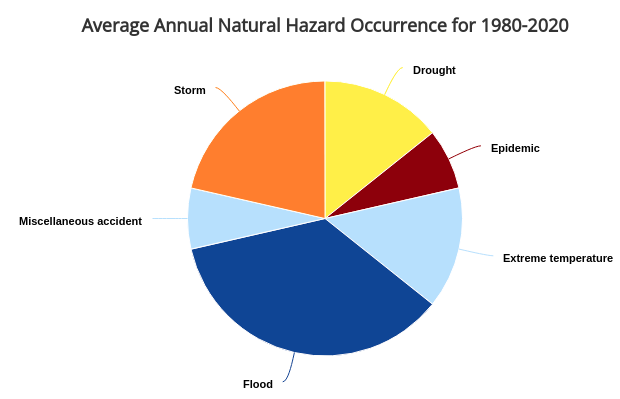
I have been assigned by the three-year-old startup company X-Power to check their new design and report back my feedback and provide them with the security report.

When it comes to security, I have to say that it’s not that easy to achieve and that's for have so many things that can interfere with security measurements where we have taken human error and thing that come from the nature.

**IT Security Risks**

To start talking about its security risks first we need to understand how big risks that are would lead us to categorize them, risks include everything that can interfere with my server, software, hardware or anything that can relate to them risks are split into.

1. Natural Causes

Natural risk are the risks that might happen because of the environment for example in some areas in China can flood and there flooding is a natural risk but here in Jordan the risks are different because here we have a different environment.  
 • droughts

• extreme temperature

• storms

• landslides

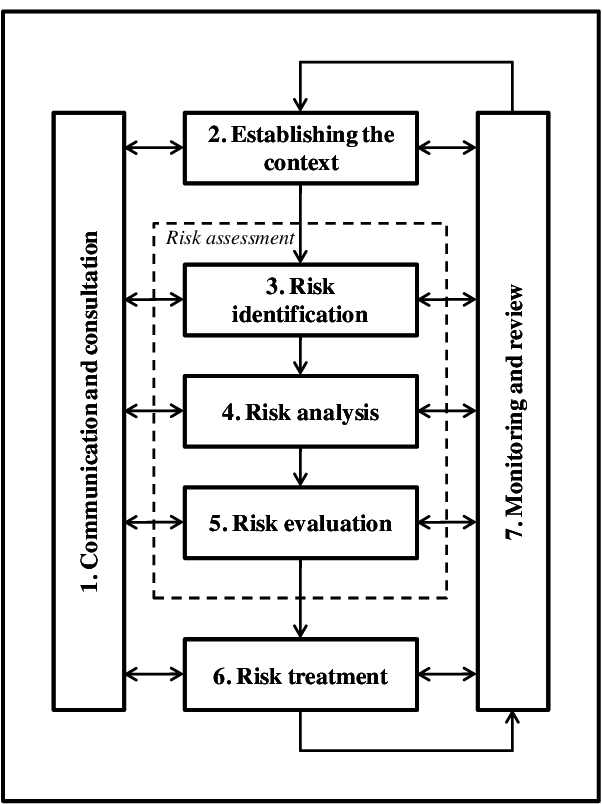
• flash floods

1. Human Causes  
   Humans can do mistakes and for security we must take that into consideration but not all of them do them as mistake so we have to take intentional and unintentional behavior for humans.  
     
   Intentional behavior  
   It’s when somebody tries to harm the X-Power company by destroying their equipment or trying to attack their servers to harm their data or computers this type humans is very random because they can be paid or sent by someone.

* Social Engineering  
  It’s basically getting your data(information or any sensitive info like the client )stolen and threating you to unleash them to public if don’t do as he says which usually is money and on the devices that been infected it would be like a malware that is harmful being planted in   
  your file and it can lock up your files.
* Man-in-the-Middle  
  Man-in-the-Middle attack is simply standing in the middle of the user connection and server connection but it has more to that because it can check everything you send and if it not encrypted it will show your data if it was it would become the matter of time form it to get cracked in addition to that it can fake itself as if it became the server which means it can talk to you as if it were the original server and for example it can tell you windows that it has updates and when you do them you will install a program from him which can inject your pc with anything it likes.
* Viruses  
  It is mostly a small file that had the ability to copy itself into other programs or files and it can only be received to the PC ether by user or downloaded some of them change them self a bit so it can adapt and spread and make it self-harder to remove, a lot of those viruses are annoying but some of them are very destructive.
* D Dos  
    
  It is an attempt to disturb the traffic on a specific IP/server by flooding it with requests which leads the server to fill the memory with data that will lead it to crash and restart or lag make the security stop working and making the server unavailable or get temp free access to the server without any security check for lagging in the memory by quickly feeding it data and the server receiving it without having it looked over by the security protocol in that service.
* TCP/IP Hijacking  
    
  it’s one of the forms of man in the middle attack were the attacker gets the IP addresses for the 2 sessions then forces one of them to be inadvisable by using a Dos attack and the other one gets attacked by using a spoof attack on the former and get the network ID For the session
* Trojan Horses  
  It is a virus that come hidden inside installable files can be activated when the program runs and usually it come on the form of a thread remover or something to repair your computer but in reality it dose the complete opposite from what it says, in the old days it wouldn’t copy itself to other places and stay active which means it goes off when the application/program goes off but now days it can copy itself and become a background process.
* Worms  
    
  It’s the most common virus these days and its specialty that it can copy itself and send itself plus usually it would be one of the most destructive viruses.
* Logic Bombs  
    
  It’s a string of code that is inserted into a program to harm a network when specific conditions are meet when that happens the it explodes and execute the specific code that was written, usually this type of injection is hard to detect until the executes then it detectable and found and using this attack in the past it used to be deleting files and corrupting files but these days it can be used to take in a virus to the system.  
    
    
    
  Unintentional
* Unintentional risks come usually from employees who do things and forget about them like forgetting to lock the server room door behind them or while testing the backup battery for server and leave unplugged from the wall or forget to lock their computers or shut them down, and there are the software part were they do mistakes like forgetting to save or placing weak passwords and for employees who work on database they can forget to backup or delete things by mistake, in addition to all of the employees get mails sometimes those mail can be infected and they would be in spam but some of them still do open them or when they send files/data through 3ed party services and the data gets taken or spied on through some social-engineering tools that can listen to the Wi-Fi or have the man in the middle connection to himself.
* Assessing Risks   
  CBA :A cost-benefit analysis is a process used by businesses to evaluate the potential rewards and costs associated with a given decision. The analyst sums up the expected returns and then subtracts the total costs.  
    
  I will have to start by saying that x-power company is a startup company and it haven’t been long on the market only 3 years, so we will need to use cost benefit analysis(CBA) to check wither it’s worth it or not because it doesn't make sense to place 5000 jds security/fire system on 1500 jds power generator or on a 2000 jds ups, so we are going to use CBA to check and what to do regarding security and safety systems.
* Treating Risks   
   Treating risks in our case it based on two factors physical, networks risks  
  physical risks are like natural causes are not that bad in Jordan by that I mean that we don't have much earthquakes in Jordan and if it happens it’s not strong as for high temperature we have to install Air conditioning units for the building and servers as for sand/rain storms, in Jordan the building structure is strong and can hold up very well in front of storms as for floods, it’s very rare to happen in Aqaba pandemic and other stuff are on the government to cover.  
    
  As for human mistakes we can install CCTV systems (camera) to monitor who enters and exits the building plus we need keep an eye on the server room and the important components inside the company.  
  We can install security system associated with the CCTV system to insure that only authorized people can enter the important rooms such as the server room and its doable through using RF-ID or finger print scanners on each room and with the CCTV and security system we will have a control room for live monitoring screens and in case anything wrong or anyone unauthorized got in through some one the security team would interfere and kick them out to restore order.  
    
  As for human error we can put on each door a mechanism to shut the door automatically and we can ban 3ed party network to make sure our employees stay on a secured network as for password we can put a restriction on how long and special characters they must use and every 3 month they must change the password.  
    
  For the network and the infected files we can add a firewall to the network to filter and make sure that data coming in is clean plus it prevents D-dos attacks and check how clean the connection to network is and it can prevent viruses from coming in and it can detect social-engineering attacks from happening which over all it would result in a secured network with low variability options.
* What could happen if we configured the network/security incorrectly  
    
  Network in this company is a base bone for how? Will the entire system is based on data collection from different location from the IOT devices that being said if we had missed something in the configuration the data might get corrupted or not saved maybe not even secured or others can manipulate it and we don’t want to be place in the risk were the data didn’t arrive or anything happened to it as for the main building where data is being saved, it must be secured and backed up were it gets cold and hot backups because as far as I understand all of the data is being saved in one location and that’s good but not perfect, so the main building would get most out of this security system and will be most focused on   
    
  1. Physical security from natural causes is mostly solved by the building structure and there isn’t much room do anything other than install air conditioning units
  2. as for normal building security we will have control room that have full connection with human security force(security guards) that can interact accordingly wo the situation.
  3. Control room will have access to CCTV/security system to make sure only people who need to be there are there.
  4. As for employees each one of them would get a PC that is secured and have everything pre-installed by the IT department including VPC(virtual private connection) in case of working from home the IT department can provide secured laptops that get full secured connection to the server through using SSH keys (hashed keys ) and VPN for the company and it comes with encrypted connection to be sure that no 3ed party programs are used or in case that some was trying to listen to the network, they won’t be able to get any useful data from you.
  5. Firewall is one of the most important security components in their system   
     firewall it prevents unauthorized connection plus filter the network connection and stops social-engineering, DDOS attacks from happening and can use sandbox method to make sure all of the files are not infected that go in to the company, if the firewall was misconfigured it can drop and refuse connection which means it can get read of the data that is being sent from the other locations or let other people (hackers) get a connection to the main server.
  6. VPN are the programs that allow you get a secured connection to server, and it would allow you to connect to the server if the configuration wasn’t placed correctly, we would have anon secured connection which would mean hacker would be able to listen to what you are send and they might be able to get password and keys and setup their own connection and start manipulating the main server.
  7. VPC are the virtual networks that are place in the company so in case the hacker goes through firewall and security, the hacker would take him mor time to figure out the system which means it will give the security team more time to take action not configuring the VPC correctly would not affect the day-to-day work, but it would make the road for the hacker easier in case the succeeded and hacked security.

**ISO risk management**

It is required to protect our assets such as users, hardware and software, so we need understand and asses the risks that would face us and can affect them.  
  
Risk assessment is the method that used to see what can result in damage or harm to the X-Power company and then do some analysis to understand those risks so we can create a way/method to protect our equipment and assets from being harmed or damaged.  
   
Risk management has some steps:

1 Identify

2 Analyze

3 Evaluate

4 Treat

5 Monitor  
  
I have been assigned by my manager to this task as a junior IT security Analyst, and it’s my responsibility to take care of the risks that can harm / damage our security/ CCTV/network systems and it my job to find them and find a way to minimize/ eliminate them.

**Risk Assessment Procedures**

Since risks are bound to happen, it is essential to protect our resources from these risks. Whether they are caused by human or natural causes. So, a part of our project is to plan to avoid or minimize the effects of these risks.

For us to know we can manage upcoming risks, it is important to know how our system operates and how our personnel would react. Therefore, a key point in our system to know the details of the details of our system.

Even if it is advertised that this hardware or software is "fail-proof", there a slight chance that they could fail. It is important to get the best hardware and software in the market to reduce the redundancy of the system.

New hardware and software are brought every now and then. It is a key point to update the statistics that are related to the risks.

ISO 31000 is a global standard which was founded in 2009, that provides key elements in risk management.

The risk management criteria in the ISO 31000 standard are the following points:

* Risk identification: It is the process of what can we prevent from damaging our system.
* Risk analysis: Studying the statistics of these risks
* Risk evaluation: Compares the risks analysis with the risk criteria
* Risk treatment: Whether a risk is positive or negative, we would like to know how it would be treated.
* Establishing the context: This process consists of defining the scope of risk management process as well as defining the company's objectives.
* Monitoring and review: This point involves checking the differences from the risk management plan and to check whether the risk management framework is still suitable.
* Communication and consultation: The point is all about the social impact and to identify the stakeholder's interests and concerns.

There are multiple theories that risk management follows, here is a couple:

* Creates and protects the value.
* Is based on the best information.
* Takes human and cultural factors into account
* Is transparent and inclusive.

After finishing the framework, it is important for this process to be taught.

It has some key components:

* Establishing the context.
* Risk assessment
* Risk treatment.

**ISO 31000 Application in IT Security**

In order to implement the 31000 ISO certification in the X-Power company we need to follow certain regulations and criterias to protect the privacy of the company.

To integrate such a standard, we must follow:

"The risk management framework".

Firstly, it is needed to point out all the risks without excluding any risk. Then sort them in a format from the most severe to the least severe on how they would affect the system. After that, it is important to update the risks and provide weekly reports of the risks. Finally, it is a good idea to try to improve any flaws in the system.

Improving Renewable Energy IT security by implementing certain techniques and methods, which in I'm going to count a few:

* DMZ: DMZ stands for (Demilitarized Zone) in which its main function is to add an extra layer to a local area network. A physical or a logical subnetwork is created to protect the system's external acts.
* Static IP: A static IP address is a way of identifying the device. Once an IP is allocated to the network device, the IP wouldn't change. There are many benefits of using static IP allocation and I am going to count a few:

- It provides a better level of protection: Once a static IP is assigned, the network device will get an extra layer of protection against malwares.

- Access to geolocation data is more accurate: Gaining geolocation data is more accurate than getting it from a dynamic IP. In which the data can be far-reaching, that includes delivery management, asset location information and load balancing.

-Reduced lapses in connection: The latency of the connection decreases, since in the dynamic IP allocation the IP changes and since it must be recognized another time, it would take more time. Therefore ,static IP is used.

* NAT: NAT (Network Address Translation), it is a method of mapping multiple local private addresses to a public one before transferring the information. The reason why we use NAT is to provide an increased flexibility when connecting to the public internet. It also allows the user to own a private IPV4 addressing system and prevent internal address changes.
* VLAN: By splitting workstations into fully independent isolated local area network segments, network directors can manually limit access to a specific cluster of users. Directors do not need to setup the network or change VLAN teams once users transfer their workstations.
* VPN: connects an entity's private network (such as a company network) to public infrastructure, typically the internet. A VPN allows users to efficiently exchange data over shared or public networks, as if they were directly connected to the non-public network.

**Different Security Procedures**

Why do we need to secure a network? It is preventive way to keep the network and data

safe from viruses or any unauthorized users. And one method to help prevent this issue is

using NMS (Network Monitoring Systems)

NMS is a server that runs a network management application. Network elements communicate

with the NMS to transfer management and control information. In which there is a logging system

in each network device and software ( PC, servers, and firewalls)

There are a lot of benefits of using the NMS, and I am going to count a few:

-Allocating Resources at Peak Effectiveness: If any undetected network outage is bound to

happen, it would decrease the general performance of the network.

-Identifying Security Threats: Since we are in an era of cyber-attacks, cybersecurity is an

essential topic to focus on. So, to resolve this threat, it is important to detect any forms

of threats.

- NMS Save Time: Errors could occur at any given time, so it is good to know where is the

issue from the start, other than "fumbling" with different protocols and trying to guess

which is the cause of this errors.

**Data Protection Processes and Regulations**

All the data that travels through the intranet or the internet must be protected no matter what it contains!

Data protection is the process of guarding important data from corruption, compromise, or loss.

We can provide the data protection using certain methods, like ( Encryption Algorithms, Data Integrity Checking,

SSL protocols and using Firewalls.)

-Encryption Algorithms: Encryption is the process of changing data into a form to be only

readable using a decryption key. Encryption must point out all the communications within the

database as well as securing all protocols into the database. Examples of encryption methods:

-RSA: A secret key is randomly generated which is unique to each session. All the

network traffic is fully safeguarded.

-DES (Data Encryption Standard): This method uses symmetric key cryptography to safeguard

network communications.

-Triple DES: This method is based on DES, but the difference is that the message data has three passes of the DES algorithm. One drawback of using such an encryption method is that

it decreases the general performance of the network.

-Data Integrity Checking: Integrity algorithms are also added to the network to make as safe

as possible to use. It verifies that the data has not been changed. A database uses these

algorithms to detect corruption. There are two common methods of integrity checking.

-MD5 Checksum: It is a method that provides data integrity through hashing and

sequencing to assure that data is not modified or stolen.

-SHA (Secure Hash Algorithm): It is a similar method to MD5, but in contrast it

produces a larger message digest for greater security.

-SSL Protocol: SSL protocol stands for "Secure Socket Layer" protocol. This exact protocol

provides authentication, data encryption, and data integrity in a PKI form. PKI stands for

Public Key Infrastructure. In addition to that, SSL can only authenticate server-to-client and

client-to-server communication.

-Firewalls: To exclude any weak points the network infrastructure, it is a method to transfer

data from a protocol to another protocol without the trouble of decryption and re-encryption

One way to ensure that the data is protected is to place the firewall between the public

network and the intranet.

**Benefits of IT Security Audit**

To reduce the chance of cybersecurity breach, we tend to use a security audit. A security

audit is a set of reviews of an IT system's configurations, technologies and infrastructure.

How Do Security Audits Work?

-First of all, we define the assessment criteria. In other words, we determine the overall goals

to be addressed in the audit, as well as agreeing on how the audit will be performed and

tracked

-Afterwards, we prepare the security audit. In which we select the required tools and

methodologies to meet goals.

-Another point that we need is to conduct the actual security audit. This means that we need

to take care and provide appropriate documentation, as well as monitor audit progress and

data points for accuracy.

-Finally, we complete and share the results. This indicates to share results with all

previously determined parties and to create a list of action items based on the audit

findings.

There are a lot of benefits in implementing the security audit, I am going to count a few!

- Using a security audit checks that the security training efforts are working.

- Discover any irrelevant hardware and software.

- Locate any bugs and flaws that introduced by using new technology or processes

- Prove that the organization abides with global regulations.

What would be a security impact of any misalignment of IT security in the X-power company?

Access to the X-power's network must be always controlled, and data integrity must be

sustained at each reachable point. Why do we need a good security infrastructure in such a

company? The reason is that many renewable energy systems use advanced controls, digital sensors

and network architectures that must not be vulnerable to any unauthorized user. Some of threats

of getting breached is:

- Loss of essential data.

- Financial crisis, in which the security threat could cause a loss of energy generation.

- Reputational damage. In any field, having a good reputation is a key for a successful

company. And if such an attack is presented to the public, the company's reputation would decrease.

**Designing and implementing a security policy for X-Power.**

Having the best security policy is a key point is essential to the X-power foundation.

Because as mentioned above, a simple security misalignment could cause a lot of negative

consequences on this foundation. In this part, I am going to count some security policies

and how can we implement them.

- Physical Security: Physical security is about how security is handled at data centers,

server rooms, and endpoints within the company's premises. And to implement this

policy, we must follow some criteria:

-Installing access control and surveillance systems for any space that contains

crucial data.

- Verify that both internal teams and security system providers follow the optimum

practices for cybersecurity.

-Create a formal collaboration to give teams a better way to share information

- Data retention: Data retention means that on what is the type data that is collected and stored

by the company. Where, how, and for how long will it be stored? To assure that we have this

policy, some rules must be followed!

- Be compliant: The data retention policy enables business to manage their compliance

within industry guidelines and regulations

-Discard outdated and duplicated data: Looking through data frequently assures

that this policy creates a chance to remove duplicated and outdated data.

-Making room for more storage: This makes sure that unneeded data is no longer

stored.

-Data encryption: Data encryption is a method to encrypt (scrambles) data and only can be accessed or

by the user that has the correct decryption key. To implement data encryption, some major

things must be considered.

- Defining the X-power's security needs: Since X-power is responsible on the renewable

energy of some major cities in Jordan, it is important to assess any threats. Also, it is

critical to know the strength and processing requirements of different encryption methods.

- Choosing the right encryption tools: Choosing the right encryption tools enables

the network to store and transfer data as efficient as possible.

- Maintaining a culture of security after implementation: It is good to make sure

that the team responsible of the data encryption is well trained and up to date with the

recent technology and methods of data encryption.

- Access Control: Access control is basal component of data security that assures who is

allowed to access and use company resources and information. It is important who gains

control to the network devices, since it helps confidential data from falling into the

wrong hands. To follow this policy, we should consider the options that are available.

- Discretionary access control (DAC): in this method the administrator of the system

sets who is authorized to access the data.

- Mandatory access control (MAC): in this method, resources based on the sensitivity

of the information that the network has, and the authorization of the user that can access

this information based on different security levels.

- Role-based access control (RBAC): RBAC restricts network access based on an

individual’s role within an organization.

- Attribute-based access control (ABAC): ABAC is a dynamic method, therefore access

is based on a set of attributes and environmental conditions.

- Security Training: Human errors are bound to happen, so it is essential to train the

employees that are responsible on managing the data. A way to help them to maintain the top

level of security is to keep the updated and do certain check-ups in given time domains.

- Risk Management: Risk management is the process of identifying, evaluating and addressing

potential threats that are bound to occur. Risk management is very crucial in such an organization

since it is a key requirement of many information security standards and frameworks. There

are some steps that can be followed to make sure that the risk management policy runs

smoothly.

- Identify the risks that might compromise the cyber security of X-power foundation

- Analyze the severity of each risk by knowing how likely it is to occur and what

would be the impact if it happened.

- Evaluate how each risk fits within the level of acceptable risk.

- Prioritize the risks.

- Decide how each risk could be handled:

- Treat: This method usually is about implementing extra or updated security

methods

-Terminate: Avoiding the risk entirely by changing the activity causing the risk

- Tolerate: Make an active decision to preserve the risk

- Transfer: Sharing the risk with another party.

-Monitor the risk to make sure that they are still acceptable.

- Business Continuity: Business continuity is the process of creating preventive and recovery

systems to deal with potential cyber threats to an organization. It is important to have

a business continuity plan to get operations up and running in the least possible time if

a cyber-attack was presented. We can follow some steps to make the finest business continuity

plan.

- Conduct Business Impact Analysis and Risk Assessment

- Develop Recovery Strategies

- Solution Implementation

- Testing and Acceptance

- Routine Maintenance

To avoid making the network vulnerable in any secure network, and in order to make that happen

Some rules must be set.

- Protecting Any Sensitive Data Using Strong Passwords:

- Make sure that the password is strong by using certain combinations of characters.

- Regularly change passwords.

- Make sure that employees don't share passwords with other employees.

- Paying Attention to Software Updates:

- In any security software, updates can occur which makes the software

more capable of handling data, so it is a good idea to keep looking out for these updates.

- Enable automatic updates to remove the chance of forgetting updating the software

- Being Careful on What Is Downloaded:

- Since it is a private machine, it is not acceptable for the employee to

download any files from the internet. Because if this happens, there would be a risk of vulnerability

- Providing a Backup Policy:

- The foundation should design a system that satisfies the strategy for

backup and recovery

- Creating a schedule of how often backups are performed

- Documenting all secure data backup and restore procedures

- Generating a matrix indicating how long backups should be retained for recovery

- Logs of scheduled restore test results

- Avoiding Any External Media to The Personal Computer :

- Pen drives pose a major security risk to networks and data. In which malware

could be transmitted through them.

- It is required to only use authorized removable media with their devices for work-related tasks.

- If the use of removable media is essential, the media should be enctrypted.

- Controlling Portable Devices Policy:

- Since we are an era that everything is wireless, and data can be transmitted

in various ways. It is important to control which devices enter the network premisses.

- It is important to handout certain authentication on which devices are

allowed to enter.

- Enabling fingerprint logins for the devices. In which using fingerprints

are way more complicated than using a password.

**Evaluating the suitability of the tools used in this policy**

Some tools can be implemented in order to optimize and test the security of the network. In this section

I am going to talk about three main tools, which are (NMAP, Nessus, and Wireshark)

-NMAP: NMAP is a service that is used to test out the network's security, in which it searches

for hosts and services on a network. The way that NMAP functions is that it analyzes raw IP packets

in distinctive ways that work out hosts are on the network. NMAP looks out and interprets the response that comes back and uses the information to create a "map" of the network. This map which is

created contains all the detailed information on what port is doing what. There are many reasons

that we opt on using NMAP, and I am going to count a couple.

- It is flexible to use, because NMAP supports several advanced techniques for mapping

out networks filled with IP filters, firewalls, routers, and other barriers.

- Since it is used in many operating systems (Linux, Windows Microsoft, FreeBSD, Mac OS, and many others) it is portable to be used.

- NMAP is quite easy to use, because a graphical user interface is available. A

command line interface is available also.

-Nessus: Nessus is a remote security scanning tool. It looks out for any threats that any unauthorized

user could gain to the information. Nessus works by testing each on a computer, which determines

what service is running. Testing this service makes sure that there are no liabilities found, that

can be used in any negative manner. There are some reasons to use Nessus:

- It is a user-friendly tool, since modules are configured in the tool for use

- It is updated frequently, so it assures that the consumer is looking out for correct data

- It has large configuration options; any configuration can be configured in Nessus as it

supports testing on all domains. This makes it versatile to use.

-Wireshark: Wireshark is a program the lets the network administrator to lookout for any things

that are happening within the network. The method on how it works is that it allows the user

to filter the logs before or after during the analysis.

- It is available on many platforms (Windows and Unix)

- Can see detailed information about packets within a network.

- It enables filtering, so it filters out specific data that is needed

**The Roles of Stakeholders in the X-power Foundation**

A stakeholder is the group of people or organizations that could impact or be impacted by the project.

It is a good idea to review the cybersecurity goals and current situation. This means that

reviewing the organization's goals and context is essential. Also, initiating productive

cybersecurity conversations is another point to be considered. This means that it is a must

to assess the environment and look around corners at upcoming risks. This can be solved by:

- Leading With a Risk:

- Illustrating the commitment to protect and secure the success of the foundation

- How important measures are needed. Since if any breach could occur, this can

by far be more expensive.

- Communicating With the Same Language:

- Stakeholders are not security specialists, so in the discussion process,

it is important to simplify the general conversation and make sure that the stakeholder is

interested in being a part in this foundation.

**A Disaster Recovery Plan**

To minimize any consequences that maybe caused by a cyber crisis, a disaster recovery plan must

be set in advance.

Firstly, we should define what is a disaster recovery plan (DRP). A DRP is a document that is created that accommodates instructions on how to respond to any negative sudden events. Afterwards, there are some steps that we can follow to make sure that the DRP functions as optimum as possible with minimal outcomes caused.

- Putting the Right Person in Charge: It is good to acquire that has good communication

skills and organized.

- Documenting the Risks: It is important to know what the risks and possible outcomes are

that can be produced and put out certain questions that can help produce a good DRP.

-Creating a Communication Plan: Developing a communication plan is making an outline of how the communication procedures function during a disaster.

- Evaluating Disaster Scenarios: Determining how severe are the threats and prioritize them

depending on the consequences that could occur.

**References**

“5 Key Benefits of Network Monitoring - Ramsac.” Ramsac, 24 Jan. 2018, [www.ramsac.com/blog/5-keybenefits-of-network-monitoring/](http://www.ramsac.com/blog/5-keybenefits-of-network-monitoring/).

Arthur, Jen. “Data Encryption: A Step-By-Step Guide.” Visual Edge IT, 24 Jan. 2019,

visualedgeit.com/data-encryption-a-step-by-step-guide/. Accessed 25 Jan. 2022.

“Backup Policy: What You Should Know about Backing up Your Data?” Certitude Security, 27 May 2020,

[www.certitudesecurity.com/blog/analysis-and-assessments/backup-policy-what-you-should-knowabout-backing-up-your-data/](http://www.certitudesecurity.com/blog/analysis-and-assessments/backup-policy-what-you-should-knowabout-backing-up-your-data/).

Bank, Security National. “Internet Safety Tips for Everyone Who Spends Time Online.” Www.snbsd.com,

Security National Bank, [www.snbsd.com/about/online-safety-guide](http://www.snbsd.com/about/online-safety-guide).

Cicchitto, Nelson. “Council Post: Winning the Cybersecurity Race Is a Team Sport: How to Engage Your

Stakeholders.” Forbes, www.forbes.com/sites/forbestechcouncil/2020/09/28/winning-thecybersecurity-race-is-a-team-sport-how-to-engage-your-stakeholders/?sh=469d69096667. Accessed

25 Jan. 2022.

“Cisco Prime and Wireshark Advantages and Disadvantages.” UKEssays.com,

[www.ukessays.com/essays/information-technology/cisco-prime-wireshark-advantages-7229.php](http://www.ukessays.com/essays/information-technology/cisco-prime-wireshark-advantages-7229.php).

“Cyber Risk Management | IT Governance UK.” Itgovernance.co.uk, 2018,

www.itgovernance.co.uk/cyber-security-risk-management#:~:text=What%20is%20cyber%20risk

%20management.

“Cyber Security for Renewable Assets.” Greensolver, 9 Dec. 2021, greensolver.net/the-growing-threat-ofcyber-security-in-the-renewable-energy-sector/. Accessed 25 Jan. 2022.

“Cybersecurity and Physical Security Convergence.” Cisco Meraki Blog, 3 June 2021,

meraki.cisco.com/blog/2021/06/merging-physical-security-and-cybersecurity/.

“Cybersecurity and Physical Security Convergence.” Cisco Meraki Blog, 3 June 2021,

meraki.cisco.com/blog/2021/06/merging-physical-security-and-cybersecurity/.

December 16, Dave Wallen on, and 2020. “Data Retention Policy: What It Is and How to Create One.”

Security Boulevard, 16 Dec. 2020, securityboulevard.com/2020/12/data-retention-policy-what-it-isand-how-to-create-one/#:~:text=What%20Is%20a%20Data%20Retention. Accessed 25 Jan. 2022.

“Disaster Recovery Planning for Cyber Security.” Crashplan,

[www.crashplan.com/en-us/business/resources/cybersecurity-disaster-recovery-planning/](http://www.crashplan.com/en-us/business/resources/cybersecurity-disaster-recovery-planning/).

Hegde, Shashank. “Six Practical Use Cases for Nmap.” Enable Sysadmin, [www.redhat.com/sysadmin/usecases-nmap](http://www.redhat.com/sysadmin/usecases-nmap).

“How Cybersecurity Policies and Procedures Protect against Cyberattacks | McAfee.” Www.mcafee.com,

[www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybersecuritypolicies.html#:~:text=A%20cybersecurity%20policy%20sets%20the](http://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybersecuritypolicies.html" \l ":~:text=A cybersecurity policy sets the).

“How to Create an Effective Disaster Recovery Plan.” The ITeam, 6 June 2019, theiteam.ca/bdr/how-tocreate-effective-disaster-recovery-plan/.

“How to Use Wireshark: Comprehensive Tutorial + Tips.” Www.varonis.com, www.varonis.com/blog/howto-use-wireshark#:~:text=Wireshark%20is%20a%20packet%20sniffer. Accessed 25 Jan. 2022.

Imperva. “What Is Social Engineering | Attack Techniques & Prevention Methods | Imperva.” Learning

Center, 2019, [www.imperva.com/learn/application-security/social-engineering-attack/](http://www.imperva.com/learn/application-security/social-engineering-attack/).

Kaspersky. “Top 10 Internet Safety Rules & What Not to Do Online.” Kaspersky, Kaspersky, 2019,

usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-todo-online.

KirkpatrickPrice. “The Main Types of Security Policies in Cybersecurity | KirkpatrickPrice.”

KirkpatrickPrice Home, 29 Mar. 2021, kirkpatrickprice.com/blog/main-types-security-policiescybersecurity/.

Lyon, Gordon. “Nmap.” Nmap.org, 2017, nmap.org/.

“Mandatory Access Control (MAC).” Www.ibm.com, www.ibm.com/docs/en/zos/2.3.0?topic=environmentmandatory-access-control-mac. Accessed 25 Jan. 2022.

“Mobile Devices.” Cybersecurity, 5 Oct. 2017, cybersecurity.osu.edu/cybersecurity-you/protect-personaldevices/mobile-devices.

“Nessus.” Cmu.edu, 2022,

www.cs.cmu.edu/~dwendlan/personal/nessus.html#:~:text=Nessus%20works

%20by%20testing%20each. Accessed 25 Jan. 2022.

Panhalkar, Tushar. “What Is Information Security & Types of Security Policies.” Infosavvy Security and IT

Management Training, 6 Nov. 2019, info-savvy.com/what-is-information-security-policies-what-rthe-types-of-security-policies/#:~:text=There%20are%202%20types%20of.

“Protecting Data in a Network Environment.” Docs.oracle.com,

docs.oracle.com/cd/A97630\_01/network.920/a96582/protnet.htm. Accessed 25 Jan. 2022.

Updated: 3/29/2020, Jeff Petters. “What Is an IT Security Audit? The Basics | Varonis.” Inside out Security,

22 Jan. 2020, [www.varonis.com/blog/security-audit](http://www.varonis.com/blog/security-audit).

USB Flash Drive Security Recommendations and Best Practices.

“What Is Access Control? - Citrix.” Citrix.com, [www.citrix.com/solutions/secure-access/what-is-accesscontrol.html#:~:text=Access%20control%20is%20a%20fundamental](http://www.citrix.com/solutions/secure-access/what-is-accesscontrol.html" \l ":~:text=Access control is a fundamental).

“What Is Business Continuity Planning.” EC-Council, [www.eccouncil.org/business-continuity-planning/](http://www.eccouncil.org/business-continuity-planning/).

“What Is Data Encryption?” Forcepoint, 4 Dec. 2018, www.forcepoint.com/cyber-edu/dataencryption#:~:text=Data%20encryption%20is%20a%20security.

“What to Include in a Cybersecurity Disaster Recovery Plan | Imperva.” Blog, 11 Jan. 2022,

www.imperva.com/blog/what-to-include-in-a-cybersecurity-disaster-recovery-plan/. Accessed 25

Jan. 2022.

Wireshark Foundation. “Wireshark · Go Deep.” Wireshark.org, 2016, www.wireshark.org/.

“World Bank Climate Change Knowledge Portal.” Climateknowledgeportal.worldbank.org,

climateknowledgeportal.worldbank.org/country/jordan/vulnerability#:~:text=Climate%2Drelated

%20hazards%20in%20Jordan.