Final assignment Fall- 2021-2022

SECURITY

Name: Mahmoud Rumaneh

Id: 20120103

Date: Jan 27, 2022

Engineer Moath Sulaiman

CONTENTS

A

1.Identifying those its security risks

1. Not all existing devices are well protected. Because there is no software that protects them and these devices contain data about the company, employees, or customers, which puts them at potential risk. Organizations can be attacked, such as by common endpoint attacks, and can damage the organization and its data. (Cyber security risk)

2. Employee PCs and data centers are connected to the same subnet, which poses a risk because if a hacker attack one of the employees' devices and obtains his employee IP address, the hacker can gain access to the data center. (Cyber security risk)

3. Datacenter the door is always open. I am certain that there is a risk because anyone can enter the data center without any barriers, stealing or altering information without our knowledge. (Human risk).

4. Some misconfigurations on network security devices such as VPN and firewalls. I have security misconfigurations that occur when security settings aren't established; misconfigurations are frequently regarded as an easy target for attack, and they are simple to detect and exploit, resulting in data leakage. (Cyber security risk).

5. Earthquakes: The earthquakes can destroy the building and make the system not usable.

2. Proposing a method to assess them.

	Not all existing devices are well protected	Employee PCs and data centers are connected to the same subnet	Datacenter the door is always open	Some misconfigurations on network security devices such as VPN and firewalls	Earthquakes
Impact	Any attacker can access to the data for the company	I will lose the data	Anyone can access the data center room	That allow the hackers can detect the data for the company	Destroy the building
Likelihood	High	Medium	High	High	Low

3. Proposing a method to treat them.

1. Not all existing devices are well protected: To decrease this risk, I create a password for each employee to avoid internal risk, configure the firewall to remove malware before the data arrives at the company, and then purchase antivirus. You need to recognize the virus and remove it.

2. Employee PCs and data centers are connected to the same subnet: To reduce this risk, we must use the VLAN feature to divide the subnet into multiple subnets. In addition, the Virtual Local Area Network (VLAN) allows a group of devices from different networks to be merged into a single logical network, which is composed of one or more local area networks. A virtual LAN is created, which is managed in the same way as a physical LAN.

3. Datacenter the door is always open: We should close the door and implement some physical security controls such as a password, fingerprint, or eye scan, and for the high temperature inside the room, we can install suitable air conditioning to reduce the temperature from high to suitable.

4. Some misconfigurations on network security devices such as VPN and firewalls: Educate employees on the importance of security configurations and how they can affect the overall security of the organization. As part of the patch management process, review and update all security configurations in relation to all security patches, updates, and notes.

5. Earthquakes: To reduce the risk, safer structures will be built, and earthquake safety education will be provided.

B

Risk Assessment: Risk assessment is that the identification of hazards that would negatively impact an organization' ability to conduct business. These assessments facilitate establish these inherent business risks and supply measures, processes, and controls to cut back the impact of those risks on business operations. [1]

The goal of risk assessment is to assist organizations steel oneself against and combat risk, meet legal requirements, create awareness concerning hazards and risk, and make an accurate inventory of accessible assets. [2]

There are five steps in the risk assessment process:

1. Identify the hazards: The first step we should know what hazards our employees and our company face including: Natural disaster like flooding, fire, earthquakes etc., biological hazards like pandemic diseases etc., workplace accidents like slips and transportation accidents, and mechanical breakdowns etc., technological hazards like lost Internet connection and power outage etc., and mental hazards like excessive workload and bullying etc. [2]

Take a look around your workplace and see what processes or activities could potentially harm your organization. Include all aspects of work, including remote workers and non-routine activities such as repair and maintenance. You should also look at accident/incident reports to determine what hazards have impacted your company in the past.

I will take a glance around my work and see what processes or activities may probably hurt your organization. embrace all aspects of work, as well as remote employees and non-routine activities comparable to repair and maintenance. [2]

2. I should Determine who might be harmed and how: I have to look around my company, reflect on consideration on how my teammates personnel may be harmed by business activities or external factors. For each risk that I identified in step one, I have to reflect on who may be harmed should that hazard take place. [2]

3. Evaluate the risks and take precautions: Now I actually have a listing of potential hazards, thus I want to think about how seemingly it's that the hazard can occur and the way severe the results are going to be if that hazard occurs. This analysis will facilitate me verify wherever I ought to scale back the amount of risk and that hazards I should rank first. [2]

4. Recording my findings: My plan should include the hazards I've found, the people they affect, and how I plan to mitigate them. The risk assessment plan should show that: Conducted a look at of my workspace, determined who could be affected, controlled and handled apparent risks, initiated precautions to keep dangers low, and kept my teammates involved in the process. [2]

5. Review assessment and update if needful: My workplace is usually changing, that the risks of my company change as well. As new equipment, methods, and folks are introduced, each brings the risk of a new hazard. I'll frequently review and update my risk assessment process to remain on prime of those new hazards. [2]

C

ISO 31000: ISO 31000 is a global standard that gives pointers on managing any style of risk in any business activity. The standard provides guidelines on principles, risk management framework, and application of the danger management process. [3]

ISO 31000 covers the risk management principles which are the foundation for managing risk, and guides organizations in developing a risk management framework by: Integrating risk management into organizational structures, designing a framework for managing risk that fits the organization's context, implementing the risk management framework, evaluating the effectiveness and continually improve the suitability and adequacy of the risk management framework, and demonstrating leadership and commitment. [3]

ISO 31000 is significant to our company because managing these risks in accordance with the principles, framework, and processes outlined in ISO 31000 provides a level of assurance that allows our company to succeed and thrive without risk. The implementation of ISO 31000 guidelines into governance, planning, management, reporting, and policies can improve our company's operational efficiency by facilitating the integration of risk-based decision-making into governance, planning, management, and reporting. [3]

ISO 31000 enables our company to identify potential risks that could impede the achievement of business goals. It will also assist us in determining the significance of risks and determining which risks should be mitigated first in order to achieve the objectives before they affect the business, as well as effectively controlling all other risks. Furthermore, it boosts public trust among customers and other stakeholders by demonstrating our

company's capabilities in mitigating internal and external threats. A risk management process based on ISO 31000 will improve our company's reputation and give it a competitive advantage. [3]

D

1.

A security procedure is a set of steps that must be taken in order to complete a task or a specific security task. Procedures can be defined as a collection of actions that must be carried out in a consistent and repeatable manner in order to achieve a specific goal. Once implemented, security procedures are a set of steps to perform security affairs for x-power, making training, auditing, and improving processes easier. The security procedure serves as a starting point for reducing consistency in the security procedure, resulting in improved security control within x-power, and we have various security procedures such as backup, cryptography, anti-virus, and password protection. [6]

1. Backup: is a copy of the data that is stored in a different location spare of the original data location. We stored it in another location because the building may be destroyed, and we need the backup for data to incase if I had a disaster because if I did not backup for data and the original data is a disaster, the data may be damaged, and if the data is ruined, I don't have another data, and if I don't have the data, I will lose all the investors Full backup, differential backup, and incremental backup are all options. [7]

A) Full backup: Full backup is a full copy of data compared to original data, if we make a full backup for data, every week for example that means our company should buy space storage each period of time. This leads to a high cost; the full backup is just one possibility of failure and I don’t recommend it because we have other options. [7]

B) Incremental backup: Incremental backup is a backup for data but not all data; for example, if I make a backup every day, the incremental backup is just a copy of what changed that day. If I make a backup every week, the incremental backup only copies the data that has changed since the last backup, and this is not a solution for me to include this backup procedure in the x-power. [7]

C) Differential backup: Differential backup is also a copy of data, but the difference here is that the first backup is a full backup, the second day I make a backup just for data that changed compared to the last full backup, and the third day I make a backup just for data that changed compared to the last full backup, which means I make a backup for data that changed in the second and third days, and this is a good solution to x-power to make a backup. [7]

2. Cryptography: Cryptography is a secure procedure that encrypts and decrypts data to protect it while it is being transmitted, and when the x-power makes cryptography for data, all people can't read it so that only those to whom it is addressed can read it, because of this I use cryptography for x-power to protect the data. [8]

3. Antivirus: An antivirus is a software that conducts research on viruses and other malicious applications and then detects, prevents, or removes them if they are encountered; however, the antivirus must be kept up to date because some viruses are created today, such as zero-day attacks; therefore, the antivirus must be kept up to date in order to detect these viruses, and the antivirus must be installed on each device in the x-power. [9]

4. Password: A password is a unique identifier. It's a pass that only you know, and we should make the password so complicated that it includes capital letters, small letters, symbols, and numbers in each device in the x-power. [10]

2.

Data protection is a process that protects data or information from detection, destruction, or loss and provides the ability to retrieve the data for use or when I want it, which means that if something happens, the data must be available to use. There are many processes to protect data, such as encryption or backup.

1. Backup: is a copy of the data that is stored in a different location spare of the original data location. We stored it in another location because the building may be destroyed, and we need the backup for data to incase if I had a disaster because if I did not backup for data and the original data is a disaster, the data may be damaged, and if the data is ruined, I don't have another data, and if I don't have the data, I will lose all the investors Full backup, differential backup, and incremental backup are all options. [7]

A) Full backup: Full backup is the same as a backup, but the difference here is the amount of data, which mean each once when you want to make a backup you should backup for all data even if it hasn't been modified, which is you want to high budget to make full back up in the x-power. [7]

B) Incremental backup: Incremental backup is a data backup; the incremental backup simply backs up data that has changed throughout the day; however, before performing the incremental backup, the x-power should perform a full backup. [7]

C) Differential backup: Differential backup is a backup for data, but the difference here is that the first backup is a full backup, and I should make a backup for all data that changed since the last full backup, which means that on the first day I should make a full backup, on the second day I make backup for data that changed or modified on that day, and on the third day I make backup for just the second and third days but not the first. [7]

2. Encryption: Encryption is a secure way to protect data, and it is just one of the ways to protect data. Encrypted data is not accessible or decrypted except for a few people who have a key to solve encryption. I should use encryption to protect data for x-power company. [11]

The General Data Protection Regulation (GDPR) is a law to security and privacy in the world, and it is considered one of the most difficult laws in the world, although it was developed for the European Union (EU), it applies to organizations anywhere and specifically if you make a process for PII or process personal data to European Union (EU) citizens or residents, the GDPR will apply to you until you are not in the European Union (EU). [12]

The General Data Protection Regulation was passed in April 2016 and went into full effect in May 2018. The General Data Protection Regulation requires some processes for revealing data, and the site should take steps to make consumer rights easy, as well as timely notification in the case of a data breach. Furthermore, according to the law, any organization that handles personal data, whether public or private, must adhere to a high level of data security. [12]

Personal Identifiable Information (PII) is data or information to realize or to recognize who is the person, for example, ID number, email address, and national number, and there are fines for those who infringe in GDPR.

The General Data Protection Regulation has established a set of regulations that deal with the broad and expanding identification of personally identifiable information; however, not everyone is permitted to read the regulations, except those who have permission to do. [12]

3.

An IT security audit is a ranking of the level of security for organizations, the auditing will help to determine vulnerabilities in the organizations including administrative vulnerabilities, technical vulnerabilities, and physical vulnerabilities, and we have some of the benefits of IT security audit like:

1. Uncover potential vulnerabilities proactively, so that I can detect the vulnerabilities before it's too late. For example, if I have a hiatus, the auditing can know about it before any hackers find it, and the auditing must block this hiatus and save us from disaster.

2. To ensure regulatory compliance, the auditor or team should read the legally required laws and standards for data privacy and security, and the audit will ensure that these standards keep in compliance.

3. Learn more about new technologies before purchasing them. The x-power should test the technology before purchasing it because it may contain viruses. If the x-power purchases this technology without testing and connects it to the network, the viruses will attack the network and the x-power will lose some or all data or information in it.

4. Reduce expenses, Also, audits cost money, but they save money for x-power in the long term because auditing in the x-power can detect a hiatus before it's too late and he will resolve it.

E

All employees must accept X-Power corporation's policies and procedures. The X-power policy serves general purposes. This is a decision-making process aimed at achieving goals that represent a set of values. IT security policies were created to address security and how users react with devices on the corporate network or the Internet. Any discrepancies between the two guidelines have the following adverse effects like System violation. X-power has also developed IT security policies and how users use devices on the X-power network or the Internet. Therefore, the two policies must match, both are important to ensure that your organization remains safe and prosperous. All employees of X-power corporation must follow organizational policies and procedures to protect themselves and the company from the risky impedance. Employees need to work together to develop current relevant policy and procedure initiatives.

F

Security policy is a set of roles the organizations have to follow, we have to create a security policy for x-power, to find out who is harming x-power and they are members of the company or competitors. The goal of security policy is to x-power protect Confidentiality, Integrity, and Availability. (C.I.A), we have many policies that I will use for x-power, such as physical access policies, server, password, and backup:

1. Physical access control policy: Physical access control policies determine who can access reading or viewing data. There are illegal ways to access the system or information, but in this case, the X-power data can

be discovered or hacked, these policies are X-power, the purpose of the physical access control policy is who can access it, determining who is inaccessible, registers all deliveries and removals, and the device cannot be taken in or out of the building without prior notice. You need to review and update this list. At least once a year. [14]

2. Encryption Policy: The encryption policy determines the type of device and media that needs to be encrypted and when to use the encryption policy. The encryption policy has to involve whole media and devices that can save X-power data. It may also include the transmission of data. That is, if you are sending data, you must send it over an encrypted channel to keep it safe, but if you are sending data via physical means such as DVDs, CDs, this data. Also needs to be encrypted. [15]

3. Password Policy: The purpose of password policies is to create very strong and complicated passwords that are difficult to guess and recognize by default. Password policies apply to everyone, not just a few employees. Passwords are an important factor in accessing important data. That is, not all users have access to your data, so password policies protect your data. All users are accountable for missing their passwords. Password policies are highly confidential, consistent, and available (CIA) and must be created within X-power. To create a strong or complicated password, you need the following properties: [16]

A) Use upper- and lower-case characters (a-z, A-Z). [16]

B) Use numbers, punctuation and letters (@#$%! *&%^.,)(‘[];). [16]

C) Password should be more than eight digits. [16]

D) Password reuse is not allowed. The password must not be the same as the last 5 changes made to the same employee in X-power. [16]

E) It`s not allowed to set in writing your password in notes on an open PC or in a paper on your desk. [16]

4. Backup policy: A backup is a print of the data you want to protect. Backups are used to retrieve data when the original data is attacked, I use three methods for backup. The first is a complete backup of the data compared to the original data, and the second is a pure copy of the data that has changed to date. Third, a differential backup is just a print of the data that has changed since the last full backup. The four things you need to include in your backup policy are:

A) When backing up, I should process the backup during non-working hours, like holidays such as Fridays and non-working hours, so as not to affect your company's work.

B) I will keep data external because the risks of data in our company are external, like the cloud on the Internet, and in real life, like cold sites, warm sites, and hot sites.

C) Make all backup data are encrypted to preserve its secret if it drops into the wrong hands.

D) Allow some reliable members of staff to arrive backup.

5. Clean Desk Policy: Clean Desk Policy is the standard for data protection. You should always clean up your desk documents as these documents may contain passwords and important information about your company.

That is, someone might come to your side desk to check this information or get the device password and the company information and information about the device isn't protected, the goal of the clean desk policy is to protect X-power company. [14]

G

1. Physical access control policy: We used the physical access control policy to raise the security of the company more and more, especially since the harm that may befall the company can only come from within. By using this policy, I will determine who can enter the system and choose only trusted individuals; as a result, the confidentiality of the company's information is maintained.

2. Encryption Policy: To protect company's data, I use an encryption policy. If the hackers attack them, the hackers will be unable to discover what this data is, and this is how I kept the information private.

3. Password Policy: When we have a solid policy in place, we can protect X-power accounts and devices, and by protecting the devices, we can also protect the entire data because it protects information from any person. Setting a firm policy for passwords with complex content will go a long way toward ensuring that our organization maintains a basic level of security. A solid password policy will usually include user authentication criteria.

4. Backup Policy: I used a backup to protect my data from corruption. I make a copy of the original data in case the company gets corrupted or something happens to the original data. Therefore, I made a backup so that the work wouldn't stop, and kept the company information and status.

5. Clean Desk Policy: The level of security in the company will rise as employees implement this policy. When the office is clean, even if other employees or customers pass by, they are unable to do anything for the company; thus, the confidentiality of the company's information is preserved.

H

1. Chief Information Security Officer (CISO): The Chief Information Security Officer (CISO) is the manager responsible for information and data security for our company. He has a lot of roles and responsibilities such as: [18]

A) Security Operations: Real-time analysis of imminent threats and triage in the event of a problem. [18]

B) Cyber Risk and Cyber Intelligence: Keep up with evolving security threats and help the board understand potential security issues that may arise from acquisitions and other large corporate moves. [18]

C) Prevent data loss and fraud: Make sure your employees aren't misusing or stealing your data. [18]

D) Security Architecture: Security hardware and software planning, purchasing, deployment, and ensuring IT and network infrastructure are designed with security best practices in mind. [18]

E) Governance: Make sure that all of the above initiatives are running smoothly, are receiving the necessary funding, and that senior management understands their importance. [18]

2. Cryptanalyst: Cryptanalysts develop athletically codes and methods to save data from computer hackers. This includes decrypting the ciphertext into plaintext and sending the message over an insecure channel. He has a lot of roles such as: [19]

A) Cryptanalysts know how to break secret code and write code that hackers can't break. He protects our privacy by monitoring the online security of our data systems. [19]

B) A cryptanalyst who operates a computer and develops code that saves our data from computer hackers. [19]

C) Cryptanalysts are math experts who can create, configure, and evaluate algorithms designed to solve number theory problems. If a hacker breaks the code of our data, the cryptanalyst is responsible for developing new ways to encrypt the data and scrambling the message to hide sensitive data. [19]

3. Cyber Intelligence Specialist: Cyber Intelligence Specialists are responsible for participating in threat actor-based intelligence analysis, creating relevant, timely and actionable intelligence products, and providing incident response and cyber threat hunting support. He must be in our company and he has a lot of roles such as: [20]

A) Cyber intelligence specialists identify cyber threats, trends, and new developments on a variety of cyber security topics by analyzing open-source information and data covering geopolitical and cross-border events. [20]

B) Cyber intelligence specialists apply analytical techniques to intelligence. document, Investigate and report on cybersecurity issues and emerging trends. [20]

C) Cyber Intelligence Specialists provide actionable technical, strategic and tactical cyber intelligence and intelligence through presentations, briefings and reports. [20]

D) Recognize threats by conducting relevant investigations and data analysis using internal and external resources and tools. [20]

E) Build relationships between cyber industry leadership and law enforcement agencies. [20]

4. Security Officer: Security personnel is responsible for ensuring the safety and security of company employees, visitors, and related assets. Security personnel are tasked with tour specific areas, reacting to security threats, and establishing a security presence. He must be in our company and he has a lot of roles such as: [21]

A) Assume public responsibility for the protection and security of determined areas. [21]

B) Recognize probable security risks and respond accordingly. [21]

C) Complete required documentation and incident reports for all security accident. [21]

D) Monitor alarms and security cameras. [21]

5. Security Analyst: Security analysts play an important role in protecting our company's sensitive and proprietary information. He works across departments to identify and fix failures in the company's security systems, solutions, and programs, and recommends specific actions that can improve the company's overall security regime. He must be in our company and he has a lot of roles such as: [22]

A) Continuously updating the company's accident response and disaster recovery plans. [22]

B) Verifying the security of third-party vendors and cooperating with them to meet security necessities. [22]

C) Performing internal and external security audits. [22]

D) Monitoring security access. [22]

I

Disaster Recovery Plan: The disaster recovery plan (DRP) is a process for organizations to help them execute the recovery process in the event of a disaster in order to protect their IT infrastructure. The (DRP) purpose to fully explain what you would do in the event of a disaster. You should develop a disaster recovery plan (DRP) if you experienced a disaster; examples of disasters include man-made disaster and natural disasters, and we have the main component to dealing with DRP: [4]

Team for DRP: We should act as a team for DRP because the DRP is in the document, but the team is working on recovery for those organizations. I mean, the team reads these documents and follows the steps in the documents to recover the organization from disaster. [4]

Recovery Point Objective (RPO): The recovery point objective (RPO) is the maximum amount of data that can be recovered before a disaster occurs. Of course, if you create a backup, I need to use the (RPO) in x-power because I need to retrieve the data after a disaster occurs. [5]
Recovery Time Objective (RTO): The recovery time objective (RTO) is a target time that it takes to restore the system to its pre-disaster state. Of course, I should make a backup before the disaster, but I also need the RTO in the x-power because I need to calculate the time to retrieve data. [5]

REFERENCES

[1] SearchCompliance. 2022. *What is a Risk Assessment? - Definition from WhatIs.com*. [online] Available at: <https://searchcompliance.techtarget.com/definition/risk-assessment> [Accessed 3 January 2022].

[2] Lucidchart.com. 2022. *A Complete Guide to the Risk Assessment Process | Lucidchart Blog*. [online] Available at: <https://www.lucidchart.com/blog/risk-assessment-process> [Accessed 7 January 2022].

[3] Pecb.com. 2022. *ISO 31000 Risk Management - Training Courses & Certification - EN | PECB*. [online] Available at: <https://pecb.com/en/education-and-certification-for-individuals/iso-31000> [Accessed 9 January 2022].

[4] Druva. 2022. *What is a Disaster Recovery Plan? Definition and Related FAQs | Druva*. [online] Available at: <https://www.druva.com/glossary/what-is-a-disaster-recovery-plan-definition-and-related-faqs/> [Accessed 9 January 2022].

[5] Ibm.com. 2022. *RTO (Recovery Time Objective) explained*. [online] Available at: <https://www.ibm.com/uk-en/services/business-continuity/rto#:~:text=What%27s%20an%20RTO%20(Recovery%20Time,go%20from%20loss%20to%20recovery> [Accessed 14 January 2022].

[6] https://purplesec.us/resources/cyber-security-policy-templates/#Physical

[7] https://spanning.com/blog/types-of-backup-understanding-full-differential-incremental-backup/#:~:text=There%20are%20mainly%20three%20types,full%2C%20differential%2C%20and%20incremental

[8] The Economic Times. 2022. *What is Cryptography? Definition of Cryptography, Cryptography Meaning - The Economic Times*. [online] Available at: <https://economictimes.indiatimes.com/definition/cryptography> [Accessed 19 January 2022].

[9] Support, T., 2022. *How Does Antivirus Work?*. [online] Soscanhelp.com. Available at: <https://www.soscanhelp.com/blog/how-does-antivirus-work#:~:text=Antivirus%20software%20searches%20for%2C%20detects,your%20computer%20and%20cause%20problems> [Accessed 19 January 2022].

[10] The Upcoming. 2022. *The benefits of getting an IT security audit*. [online] Available at: <https://www.theupcoming.co.uk/2020/11/23/the-benefits-of-getting-an-it-security-audit/> [Accessed 19 January 2022].

[11] Forcepoint. 2022. *What is Data Encryption?*. [online] Available at: <https://www.forcepoint.com/cyber-edu/data-encryption#:~:text=Data%20encryption%20is%20a%20security,or%20entity%20accessing%20without%20permission> [Accessed 20 January 2022].

[12] Ground Labs. 2022. *What is PII for GDPR | Ground Labs*. [online] Available at: <https://www.groundlabs.com/blog/what-is-pii-for-gdpr/#:~:text=GDPR%20PII%20Definition,email%20address%20and%20phone%20numbers> [Accessed 20 January 2022].

[13] The Upcoming. 2022. *The benefits of getting an IT security audit*. [online] Available at: <https://www.theupcoming.co.uk/2020/11/23/the-benefits-of-getting-an-it-security-audit/> [Accessed 20 January 2022].

[14] PurpleSec. 2022. *50 Free Cyber Security Policy Templates To Secure Your Network*. [online] Available at: <https://purplesec.us/resources/cyber-security-policy-templates/#Physical> [Accessed 21 January 2022].

[15] Luc.edu. 2022. [online] Available at: <https://www.luc.edu/its/aboutits/itspoliciesguidelines/encryption.shtml> [Accessed 20 January 2022].

[16] 2022. [online] Available at: <https://www.wlc.ac.uk/policies/it-password> [Accessed 21 January 2022].

[17] Vatner, S., 2022. *6 things you should include in your backup policy*. [online] Lanrex.com.au. Available at: <https://www.lanrex.com.au/blog/data-backup-best-practice-and-why-we-need> [Accessed 21 January 2022].

[18] Fruhlinger, J., 2022. *What is a CISO? Responsibilities and requirements for this vital role*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html> [Accessed 21 January 2022].

[19] Careerexplorer.com. 2022. *What does a cryptanalyst do? - CareerExplorer*. [online] Available at: <https://www.careerexplorer.com/careers/cryptanalyst/> [Accessed 21 January 2022].

[20] SupportFinity. 2022. *Hire Best Cyber Intelligence Specialist in Jan 2022 - SupportFinity*. [online] Available at: <https://supportfinity.com/hire-cyber-intelligence-specialist> [Accessed 22 January 2022].

[21] 2022. [online] Available at: <https://www.glassdoor.com/Job-Descriptions/Security-Officer.htm> [Accessed 22 January 2022].

[22] Digital Guardian. 2022. *What is a Security Analyst? Responsibilities, Qualifications, and More*. [online] Available at: <https://digitalguardian.com/blog/what-security-analyst-responsibilities-qualifications-and-more> [Accessed 22 January 2022].