1. Show evidence of understanding how management and leadership affects teams and organizations broadly and specifically with regards to cyber security

   Even though leadership is a well-studied construct, leadership in the context of cybersecurity must embrace the adaptive difficulties provided by emerging cyber-threats. Throughout history, leadership has been defined in numerous ways, emphasizing authority, the ability to influence, or a collection of behaviors or attributes. However, contemporary conceptions. A method by which one person can influence a group of people to attain a common aim. " As a process, leadership involves a separation between what a leader does and the features or characteristics that a leader may possess. As a result, one is not born a leader or become a leader because of their attractiveness, charisma, or intelligence, but rather because of their activities or accomplishments. Leadership, as a process, is more engaged with interactions between leaders and followers than with a linear edict from on high. It also entails the formation of a shared vision, which implies a desire for mutual benefit for both leaders and followers. Finally, leaders must be able to influence their followers and others in the pursuit of a common purpose.

2. Describe the concepts of threat, vulnerability, and risk

   The risk profile of a business differs based on situational and environmental factors. It considers not only the possibility or likelihood of a negative event, but also the impact that event could have on your system. And, while threats can never be completely eradicated, they can be controlled to a level that is appropriate to your organization's risk tolerance. Regardless of how you approach it, the final goal is to keep your potential losses minimal, manageable, and predictable.

   The word "threat" is often confused with the word's "risk" and "vulnerability." However, in cybersecurity it is critical to distinguish between a threat, vulnerability, and risk. A threat takes advantage of a flaw and can harm or destroy an asset. A weakness in your hardware, software, or procedures is referred to as a “vulnerability.” And risk refers to the possibility of assets being lost, damaged, stolen or destroyed.

   Threats can steal or damage data, disrupt operations, or cause general harm. To avoid this, we must be aware of the various cyber threats that exist. There are 3 main types of threat that the company may face. These include intentional threats, unintentional threats, and natural threats.

A weakness in the hardware, software, or procedures is referred to as a vulnerability. It is a vulnerability that allows an attacker to obtain access to our assets. Threats, in other words, take advantage of vulnerabilities.

The intersection of assets, threats, and vulnerabilities is known as cyber risk. When a threat exploits a vulnerability, it can result in the loss, damage, or destruction of an asset.

Threats + Vulnerability = Risk

3. Create a CV targeted at a chosen cyber security career Assessment

Task Pre-requisite: Develop your CV based on your current skills and abilities. This CV will be revised at the end of the assignment based on what you have learned from this module and this experience.

Assume that you have an e-commerce company in the retail business (like amazon.eg). During this coursework you will identify the essential security requirements of your organization. By assessing the risk to the organization, considering your online business (Cyber) and your company's IT infrastructure and premises (Physical).

1. Start by identifying the critical assets of your company

   Accounts, Passwords, User/Website data, Backups, Contacts and Sites

Everyone has at least one digital asset. They can be files, documents, audio, movies, or anything that can be kept digitally on a computer, hard drive, database, or cloud. They can be classified as assets if they add value to our organization. Their value is determined by how much time and money it took to build them, as well as how valuable they are in the future.

Fixed assets:

Fixed assets are important for businesses having a physical location, a warehouse, and staff. We can put real estate, office space, and equipment in this category if your firm owns them. They are classified as liabilities in your chart of accounts if they are rented or leased.

Digital assets:

Digital assets management can be done manually, but with the correct digital asset management (DAM) solutions, documents such as invoices and purchase orders can be kept and accessed easily. DAM software also lowers the chances of these assets being misplaced, damaged, or misfiled. As far as our inventory is concerned.

digital assets may include backup websites, user information, emails, passwords, addresses and phone numbers.

Physical assets:

Other than digital assets our company also has physical assets. Physical assets include items that may be bought and sold, as well as tangible property such as desks and computers that are used to run our business. When it comes to tangible assets in ecommerce, inventory is the most significant idea. Our inventory is just a list of items that we can sell or have for sale on the internet.

Inventory listing errors can cause chaos with order processing, resulting in customers receiving the incorrect products or obtaining them late. Even if our products are durable, knowing which products should be dispatched first will help us avoid returns and refunds, which can have a significant impact on

our revenue. As security experts we must be weary that our business has multiple sides other than it being secured.

Monetary assets:

Our company also has monetary assets. Monetary assets are simply cash at hand that may be used to pay suppliers or cover day-to-day expenses.

2. Identify the threats to and potential vulnerabilities of those assets

Intentional threats:

Malware, ransomware, phishing, malicious code, and accessing user login credentials incorrectly are all examples of intentional threats. Attackers can utilize these behaviors to compromise a security or software system.

Unintentional threats:

Human mistakes are frequently blamed for unintentional threats. Someone in the cybersecurity profession can forget to lock the door to the IT servers or leave important data unmonitored. It is possible that an employee will neglect to update their security system or anti-virus software. Current and even former employees may have unauthorized access to critical information or may just be oblivious of the dangers. Ways to avoid this include training the employees and making sure they follow the security policy.

Natural threats:

While natural disasters are not usually linked to cybersecurity, they are unexpected and can-do considerable damage to our assets, these may include earthquakes, storms etc.

1. Evaluate the likelihood of occurrence and estimate the potential impact.

   likelihood:

   1.
   "Data breaches are not always caused with malicious intention. In fact, 22% of incidents are the result of a mistake made by an employee according to IT Governance."

   The most prevalent mistakes concerned sending sensitive material to the incorrect person. Emailing the incorrect person, downloading the wrong document, or providing a hard file to somebody who should not have access to information are all examples of this. Misconfiguration, which often entails leaving a database holding sensitive information without any password constraints, was the second most prevalent source of human error.

   2.

Disasters strike, and they take various forms. The list goes on and on fire, floods, building collapse, electrical grid failure, power outages, internet outage, and so on. Having the correct safeguards in place will assist you in getting back online so that your ecommerce firm can continue to operate.

3.
Nowadays, it is all about the customer experience. If your site needs to wait, if visitors cannot find what they are searching for, if it is difficult to browse or comprehend, or if your material is of inferior quality, most visitors will leave without hesitation and will not return.

4.
A successful SQL injection attack might result in unauthorized access to sensitive data such as passwords, credit card numbers, or personal user information. In recent years, SQL injection attacks have been blamed for several high-profile data breaches, resulting in reputational damage and regulatory sanctions. An attacker can occasionally get access to a company's systems using a persistent backdoor, resulting in a long-term infiltration that goes unnoticed for a long time.

5.
An attacker can use XSS to send a malicious script to an unknown user. The end user's browser has no way of recognizing that the script should not be trusted and will nonetheless run it. Because it believes the script came from a reliable source, the malicious script can access any cookies, session tokens, or other sensitive information stored by the browser and utilized with that site. These programmers can even change the text of an HTML page. Here is where you can learn more about the many types of XSS attacks.

6.
A path traversal attacks attempt to get access to files and directories that are not located in the web root folder. By altering variables that reference file sequences and variations or exploiting absolute file paths, it may be able to access arbitrary files and directories stored on the file system, including application source code or settings and critical system files. It is important to note that file access is restricted by system operational access control.

7.
On their wired networks, most firms now utilize web filters to limit the kind of material that employees may access but protecting wireless networks can be more complex. Controlling and monitoring access and restricting content on Wi-Fi networks is more complex.

Anyone near the access point, especially at public Wi-Fi hotspots where all guest users share the same set of credentials, can launch an assault. As a result, it is vital to take steps to strengthen wireless access point security and safeguard Wi-Fi network users.

Impact:
Businesses that suffer data breaches face serious and growing implications. This is mostly due to the increasing regulatory burden associated with notifying individuals whose personal information has been exposed. The regulations for notification and sanctions for firms who suffer a data breach vary depending on the authority.

3. Provide risk mitigation techniques and security controls to reduce the impact of a potential attack.

1. While you can retain your perimeter security and other safeguards in place, you will also need a data-centric method that allows you to precisely restrict who has access to certain files and data sets. This level of control is provided through encryption, but it must be the correct sort of encryption. You can always manage who can read a given file or email if it is properly encrypted. Even if your IT system has a data breach and unauthorized persons obtain access to personal records, they will be unable to read it, preventing a data leak about that data.

2. Cloud data recovery software is an important part of any comprehensive. You can be certain none of your essential data will be lost if your ecommerce business and all its data are stored on the cloud.

3. Faster server that does not have frequent crashes, have a security system that prevents ddos attacks to prevent such issues

4.
Most instances of SQL injection may be avoided by using parameterized queries instead of string concatenation within the query. To avoid SQL injection when using a parameterized query, the query string must always be a hard-coded constant with no variable data from any source. Do not be tempted to determine whether a piece of data is reliable on a case-by-case basis; instead, continue to utilize string concatenation within the query for situations that are considered safe. It is all too easy to make assumptions about data sources or have other programmers' adjustments contradict assumptions about what data is polluted.

5.
Depending on the application's complexity and how it manages user-controllable data, limiting cross-site scripting can be straightforward in certain cases but far more complicated in others. In general, preventing XSS flaws will need a combination of the following measures: Filter the info when it arrives. Now where user input is received, filter as precisely as feasible based on expected or legitimate input. The output data should be encoded. To prevent being mistaken as active content, encode user-controllable data in HTTP replies. Depending on the output context, this may demand a mix of HTML, URL, JavaScript, and CSS encoding. Use the relevant response headers. The Content-Type and X-Content-Type-Options headers can be used to guarantee that browsers read HTTP replies in the manner you want them to, avoiding XSS in HTTP responses that are not meant to contain HTML or JavaScript.

6.
A web filtering solution is a straightforward way to improve the security of wireless access points. Web filtering technologies are commonly used to protect wired networks, but there are alternative ways to improve wireless access point security. Between network users and the Internet, a web filter functions as a barrier. Controls can prohibit users from accessing hazardous, unlawful, or inappropriate internet information. Even if each user has their own set of access rules, users will be vulnerable to malware and phishing attempts without a web filter, and the hotspot provider may be held liable for illegal conduct on the Wi-Fi network.

4. The last section of your report will be addressed to the business owners of your organization convincing them to invest in implementing the identified mitigation techniques

The hackers all have the same goals in mind, such as achieving a Domain Admin position. Having the ability to safeguard certain objects (such as the Domain Admins group) and instantly rollback any modifications made is an efficient approach to stop an assault in its tracks before it does more harm to the company. Changes made inside the firm should be audited. If you do not know what has changed, you will not be able to recuperate adequately. It is critical to have visibility down to object attributes and group policy changes in this case, as these are the modifications that give the hackers. To help with stealthy, resilience, lateral movement, and control, skilled threat actors have worked to develop automated processes that trawl infiltrated systems for credentials, test access, attempt to exploit weaknesses within the firm, and achieve higher privileges. Our company aims to satisfy both customers and employees alike, we aim to provide easy accessibility while maintaining security for our customers from both outsider and insider threats, these threats may include threats from hackers like malware, phishing, and other cyber threats.

Rules:

- Per Group: A word/pdf file (around 2000) words that includes the whole scenario description.
- Per Student: CV with cover letter.
- Plagiarism is unacceptable

Source:

https://www.kennasecurity.com/blog/risk-vs-threat-vs-vulnerability/

https://www.interactsoftware.com/blog/the-impact-of-managers/

https://www.ayvid.co/how-does-management-affect-an-organizations-performance/

https://www.travasecurity.com/resources/the-difference-between-threat-vulnerability-and-risk-and-why-you-need-to-know#:~:text=A%20threat%20exploits%20a%20vulnerability,%2C%20damaged%2C%20or%20destroyed%20assets.