# CYB 200 Project Two Milestone Decision Aid Template

Complete the template by filling in the blank cells provided.

1. Detection

| **1. Describe the following best practices or methods for detecting a threat actor.** | |
| --- | --- |
| **Awareness** | In cybersecurity, awareness is being mindful of the situation we face every day, from receiving emails to our workspace. Aware of any suspicious co-worker that could harm the company, do not provide your username and/or password to anybody. Be aware of new individuals in the organization, changing passwords constantly (at least every 6 months), and using complicated passwords to difficult malicious user’s jobs. Do never click the link in the emails, and in case there is a question about it, contact the sender directly. |
| **Auditing** | Auditing is a depth review of an organization’s security measures and policies put in place in the company, association, firm, or any identity. Important factors like the inspection of the firewalls, the monitoring RBAC, and the other security tools used in the company. Update the constant of the system, to keep the latest software and in some cases hardware. And always, have a plan of response to any threat to the organization. |
| **Diligence** | Diligence is the process to anticipate, identify, and address risk across the company or organization. The best practice for diligence is conducting a risk profile, which means, identifying the target, we can identify the perpetrator. Understand the relationship between companies and vendors to re-evaluate the potential risk. Analyzing asset ownership of the company and managing the transaction that occurs in the company. Understanding the roles and their privilege will help the diligence too. |
| **Monitoring** | Monitoring is the examination of the system and remediation of risk within the network. Constantly monitoring provides an effective approach and time framework to react to any threat. The use of the SIEM (Security Information and Event Management) platform will analyze and aggregate data across multiple systems. If there is an unusual activity, it’s important to have a close look to prevent any threat or vulnerability. |
| **Testing** | Testing is the evaluation of a subject to determine how well something is working, in Information Security testing. In Information Security, testing is crucial to determine if the application or software is adaptable to the environment and prevent any zero days in which a malicious user could infiltrate the system. Malicious users will try to find vulnerabilities and inject viruses, trojans, worms, etc. To make the system down, implementing antivirus is crucial to avoid threats against the system. Testing allows us to create risk assessments and detect potential threats. Penetration tests allow us to identify where the system fails and where will need more improvement. |
| **Sandboxing** | Sandboxing is the implementation of running, observing, and analyzing the code in an isolated environment on a network. Sandboxing helps us to prevent any threat to a vulnerable face in the creation of the software or application. It helps to test untrusted code. Sandboxing evaluates potentially malicious software threats with new vendors. The quarantine zero-day threats to prevent potential vulnerabilities unknown. Also, if the application goes to the cloud secure the existing gateway. |
| **Enticing** | Enticing is the act of encouraging criminals to keep committing crimes until they get caught. Acting like the company doesn’t know is getting breached will make the attacker feel more comfortable and the security team is available to find him when the malicious user does not expect it. Allowing the malicious user to extract fake data provides us with a better view of where and how the data is being leaked. |

| Citations: |
| --- |
| Koziol, J. (2023, July 24). *Cybersecurity awareness: What it is and how to start*. Forbes. https://www.forbes.com/advisor/business/what-is-cybersecurity-awareness/  *How to perform a cybersecurity audit: A 3-step guide: Upguard*. RSS. (n.d.). https://www.upguard.com/blog/how-to-perform-a-cybersecurity-audit  Patel, K. (2022, October 25). *How to conduct cybersecurity due diligence + checklist*. RSS. https://dealroom.net/blog/cybersecurity-due-diligence  Hamilton, T. (2023, July 22). *What is security testing? example*. Guru99. https://www.guru99.com/what-is-security-testing.html  Jnguyen. (2021, October 25). *What is sandboxing?*. Check Point Software. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-sandboxing/ |

1. Characterization

| **2. Briefly define the following threat actors.** | |
| --- | --- |
| **Individuals who are “shoulder surfers”** | Shoulder surfer is a type of criminal practice that consists of the stealing of information by spying over the shoulder. Insiders usually practice shoulder surfing since they try to get access to the system, and they use this method to get credentials to access the system. Competitors are known for the intent to get access to the competitor system, and they will use different methods including shoulder surfing. Thrill seekers could potentially use shoulder surfer to gather information and get to the system just for the sensation of excitement or fun. APTs (Advanced Persistent Threats) could potentially use shoulder surfing since they are persistent, even if their techniques are more sophisticated, they could use shoulder surfing as a last resource. Hacktivists use shoulder surfing since they try to get access to important information, and they will use many different methods including shoulder surfing. |
| **Individuals who do not follow policy** | Hacktivists are known to attack company networks if they disagree with the policies. Cyberterrorist do not follow policies and their main goal is to inflict damage to the company, organization, or country. APTs (Advanced Persistent Threats) are highly knowledgeable individuals which attack counties which have policies or rules that they are not agree with. National-state actors attack companies to disrupt their network or gather information since they are not agreeing with the policies, example Chinese government. Script kiddies could threaten the company if they do not agree with their policies even if they are not sophisticated in their methods. |
| **Individuals using others’ credentials** | Insiders will use other people’s credentials to get access to the physical location of their system. Hacktivists will use people’s credentials so it’s easier to get access to their system and threaten it. Competitors are known to use competitor credentials to gather information in their systems. Criminal syndicates will use credentials to gather information and steal it. APTs (Advanced Persistent Threats) will find a way to get access to the system and using credentials is one of the threat vectors to do it. |
| **Individuals who tailgate** | APTs (Advanced Persistent Threats) tailgate systems to get access to important information. Insiders will tailgate to gain access to secure information. Criminal syndicates will tailgate to exploit end users for financial gain. Competitors will tailgate for performance espionage. Hacktivists will tailgate against their company to sabotage the system. |
| **Individuals who steal assets from company property** | Competitors will steal assets and property as espionage or copy the product. Criminal syndicates will steal assets and ask for financial compensation. Insiders will steal the assets of a company and try to sell them. The National-sate actor will steal company property either to copy, use them against them, or espionage. APTs (Advanced Persistent Threats) to get access to many systems and replicate their system. |

| Citations: |
| --- |
| *What is a threat actor?*. IBM. (n.d.). https://www.ibm.com/topics/threat-actor  *Cybersecurity threats and threat actors*. Unit | Salesforce Trailhead. (n.d.). https://trailhead.salesforce.com/content/learn/modules/cybersecurity-threats-and-threat-actors/identify-threat-actor-tactics |

| **3. Describe the following motivations or desired outcomes of threat actors.** | |
| --- | --- |
| **Fraud** | Dishonest acts most of the time are linked to financial gain. Fraud will be used for committing a data breach and acquiring information from third parties. Fraudulent individuals gain power by manipulating people or companies. Fraudulent individual has the idea that they will never get caught and the satisfaction of the act, sometimes could be the main reason why they damage others. |
| **Sabotage** | Sabotage is an attack that consists in damaging or destroying a specific target, organization, or system. Sabotaging could be used for financial gain, asking for some type of ransom to return the system to normal. Sabotage could be for a sense of joy, like a kid sabotaging a videogame just for fun. Competitors use sabotage to damage competitor products so they can benefit from the migration of customers. Sabotage could be used as prevention for people to concentrate on possible problems within the system. |
| **Vandalism** | Vandalism is used as a method to spread the opposite point of view in the system of the contraries. As damage, vandalism could provide an advantage to the competitors if they get to hurt enough the competitor, so they end up going with the competitors. The sense of joy that produces vandalism is addictive for many people. Vandalism could be used to draw attention and make them feel more important. |
| **Theft** | Thef is used for financial gain, either by acquiring specific information from users or stealing important parts of the system to produce damage. Espionage is one reason why individuals or organizations steal information from others. Also, using the material stolen could benefit their product by making them close to the competitors. Theft is used to incriminate others to pass the responsibility of any action to a third individual. |

| Citations: |
| --- |
| Lin, B., Huang, J., Liao, Y., Liu, S., & Zhou, H. (2022, October 6). *Why do employees commit fraud? theory, measurement, and validation*. Frontiers in psychology. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9590450/  *Workforce Management Software News, blog, and resources*. Workforce.com. (n.d.). https://workforce.com/news/sabotage-in-the-workplace-is-an-inside-job  Author(s)                                R E Wilson. (n.d.). *Vandalism - overview of the problem and recommended prevention techniques*. Vandalism - Overview of the Problem and Recommended Prevention Techniques | Office of Justice Programs. https://www.ojp.gov/ncjrs/virtual-library/abstracts/vandalism-overview-problem-and-recommended-prevention-techniques |

| **4. Identify the company assets that may be at risk from a threat actor for the following types of institutions.**  *Remember: Each company will react differently in terms of the type of assets it is trying to protect.* | |
| --- | --- |
| **Financial** | Financial institutions have a lot of important information which includes full name, address, account(s) number, and SSN among others. A threat actor could easily use that information to create fake accounts under people’s names or move the user's money for their benefit. |
| **Medical** | Medical institutions carry a lot of information including full name, address, medical record, and in many cases account(s) number. The threat actors could damage people's lives by changing the record of the patient which could end up in a problem for the hospital and doctor. |
| **Educational** | Educational institutions store students’ information like full name, address, GPA, attendance, and grades. Educational institutions will protect this information in case any threat actor intent to damage student grades or manipulate student information. |
| **Government** | Government is one of the most important sectors that need to be protected, since they carry many important information from classified, top secret, and public. Any threat against the government could be crucial for national security, since they storage so much information that could affect in many ways, from elections to military. |
| **Retail** | Retail institutions store important information like credit cards, debit cards, account(s) numbers (checks), and data about customer consumption. Maintaining the information secure will mitigate a threat to the financial of their customers. |
| **Pharmaceutical** | Pharmaceutical institutions carry a lot of information like full name, address, medical record, and in many cases account(s) number. Protecting this information could prevent an accident of leaking information and selling it to competitors or attacking the pharmaceutical which distributes the major amount of medicine. |
| **Entertainment** | Entertainment institutions have a broad area to protect from movie theaters to videogames companies, all the companies have valuable information to store. Entertainment companies have a lot of areas where threat actors will attack and breach to gain information about either the intellectual property to user information. |

| Citations: |
| --- |
| Angela Horneman                                                                                    and Lauren Cooper. (2019, October 16). *Situational Awareness for cybersecurity: Assets and risk*. SEI Blog. https://insights.sei.cmu.edu/blog/situational-awareness-for-cybersecurity-assets-and-risk/  Securing High Value Assets - Cisa. (n.d.). https://www.cisa.gov/sites/default/files/publications/Securing%20High%20Value%20Assets\_Version%201.1\_July%202018\_508c.pdf  *7 pressing cybersecurity questions boards need to ask*. Harvard Business Review. (2023, March 28). https://hbr.org/2022/03/7-pressing-cybersecurity-questions-boards-need-to-ask |

1. Response

Choose a threat actor from Question 2 to research for the response section of the decision aid:

| **Threat Actor** |
| --- |
| **Insider** |

| **5. Describe three potential strategies or tactics that you would use to respond to and counter the threat actor you chose.**  *Hint: What are the best practices for reacting to this type of threat actor?* | | |
| --- | --- | --- |
| **Strategy 1** | **Strategy 2** | **Strategy 3** |
| Insiders use many tactics to find vulnerable points in the company, and one of the simplest ones is shoulder surfer. Insiders use shoulder Surfer to reach information or credentials of any user that has privileges within the company. Privacy protectors and lock screeners are effective tactics that will prevent any shoulder surfer. Also, always be aware of your surroundings help to notice who is paying attention on your screen. | Insiders will use personification tactics as part of their social engineering to get individuals in the company to provide them with their credentials. Tactics like spam emails or malware could be attached to the email sender by the insiders. Educating the staff constantly about the problem of clicking links or sending important information to suspicious users. Also, keeping the antivirus updated and running all the time. | Insiders in the company could download a trojan that may contain a virus or open a backdoor so outside users can have access or control of the system. It’s important to have antivirus running all the time and revise all the potential problems that may occur, this includes the most insignificant notice. Updating the system constantly will also help to patch any type of information leaked. |

| Citations: |
| --- |
| *Cybersecurity fact sheet: Shoulder surfing*. . (n.d.). https://www.arcyber.army.mil/Resources/Fact-Sheets/Article/1440819/cybersecurity-fact-sheet-shoulder-surfing/  *What is an insider threat? definition, types, and prevention*. Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/insider-threats |

| **6. Describe three potential strategies or tactics that you would employ to reduce the likelihood of a similar threat occurring again.**  *Hint: What are the best practices for proactively responding to this type of threat actor?* | | |
| --- | --- | --- |
| **Strategy 1** | **Strategy 2** | **Strategy 3** |
| Most of the threats to a company or industry are done via social engineering. Constant education about how to identify phishing, spam, and personifications tactics will prevent a company from giving access to a threat actor and minimize the likelihood of finding vulnerabilities in the system. Also, constant testing of their employees will help to check if they follow the education provided. Welcome their employee to open if they have any questions about a suspicious email or individual in the company. | Monitoring all the vulnerabilities and movement via a SIEM and AV to monitor for malicious traffic and set up a baseline for when anomalies occur. Close monitoring of any suspicious connection or traffic. Enforce the use of VPNs to secure the connection to prevent any malicious traffic incoming. | Penetration tests are done by a third party which provides a full detail of where the vulnerabilities and reports are being analyzed by the security team. Update the system all the time and keep up with the updated cyberattack that occurs in different industries. |

| Citations: |
| --- |
| Cisco. (2023, February 8). *What is Social Engineering in cyber security?*. Cisco. https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html  *Penetration testing: Ethical hacking*. SecurityMetrics. (n.d.). https://www.securitymetrics.com/lp/penetration-testing1?identifiers=kwd-84663260442960%3Aloc-190&Campaign=Search+-+Pen+Test+EXACT&CampaignId=424125867&AdGroup=Pen+Test&AdGroupId=1354599670183590&AdId=84662795994766&Network=o&msclkid=62fbbf040855195deaeedbc7c09e52c8&utm\_source=bing&utm\_medium=cpc&utm\_campaign=Search+-+Pen+Test+EXACT&utm\_term=penetration+testing&utm\_content=Pen+Test |

| **7. Explain your reason for determining the threat actor you chose to research. Why are the strategies you identified appropriate for responding to this threat actor? Justify your tactics to proactively and reactively respond to this threat actor.** |
| --- |

|  |
| --- |
| The insider was found based on the tactics previously monitored, shoulder surfer provides a clear view of who we should start keeping closer attention to within the company. Since the insiders have information about who has more privilege within the company, it’s easier for them to persuade somebody to get access to their information and get their licenses. All the strategies will help us to prevent an insider from attacking our organization. Using a screen protector will help the organization to prevent any shoulder surfer which also helps to identify who is the insider since they must pay closer attention to the monitor and check it would be obvious at that point. Monitoring the traffic will help us to identify where and how the data is being breached in the system. A penetration test will analyze the system if the insider has opened a backdoor or downloaded a trojan that will hurt the company. |