# CYB 200 Project Three 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** | Includes nurturing an environment or teaching about the potential real-life threats of the IoT(Internet of Things) so that individuals are aware of and can identify potential threats and come up with ways to assess them. |
| **Auditing** | A series of comprehensive assessments and analyses of potential or active threats to an organization’s or even an individual’s cybersecurity helps to prevent and improve against future threats. |
| **Monitoring** | The continuous observance and analysis of a computer, network, or systems to quickly identify threats or active vulnerabilities and respond to them in real-time. |
| **Testing** | The process of actively evaluating a system, network, or application’s security through simulations of real-life cyberattacks to test resilience and identify vulnerabilities and weaknesses. |
| **Sandboxing** | It is the use of an isolated safe space that allows one to study and execute potentially harmful code without the threat of damage |

| Citations: |
| --- |
| SimSpace. (2023, May 30). “Threat Detection and Response Best Practices.” SimSpace.<https://simspace.com/blog/threat-detection-and-response-best-practices-and-tips-for-success/>  SailPoint. (2023, October 17) “What is a Cybersecurity audit and why is it important?” SailPoint.<https://www.sailpoint.com/identity-library/benefits-of-a-cybersecurity-audit>  SentinelOne. (2024, October 16). “Cyber Security Monitoring: Definition and Best Practicing.” SentinelOne.<https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-monitoring/>  Bart Lenaerts-Bergmans. (2023, September 11). “What is Cybersecurity Sandboxing?” CrowdStrike.<https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cybersecurity-sandboxing/> |

1. Characterization

| **2. Briefly define the following threat actors.** | |
| --- | --- |
| **Individuals who are “shoulder surfers”** | An individual who uses a social engineering technique where they physically view a device screen or keypad to obtain personal information could be observing a PIN entered at an ATM, watching somebody enter a phone password, or going to a crowd to view multiple potential victims |
| **Individuals who do not follow policy** | A type of insider threat is when these people intentionally or unintentionally put an establishment at risk and do not understand or care about the need for security through actions such as weak passwords, downloading dangerous files, or accessing unauthorized devices or systems. They can pave the way for other malicious actors to exploit the damage they create |
| **Individuals using others’ credentials** | Individuals who use stolen access information like personal logins, credit cards, or emails to circumvent an establishment’s defense mechanisms or to utilize accounts for nefarious reasons or personal gain. |
| **Individuals who tailgate** | A type of insider attack where an individual breaches security by gaining access to a secure area by following someone with legitimate access credentials, typically by masquerading as a legitimate person like a vendor, maintenance, or staff member. |
| **Individuals who steal assets from company property** | Individuals who steal important intellectual property such as trade secrets or patents and then go on to sell these assets for profit or leverage for blackmail. These people can be disgruntled employees, third-party members, or anybody with an internal knowledge of the establishment. |

| Citations: |
| --- |
| Beyond Identity. (n.d.). “Shoulder Surfing”. Beyond Identity.<https://www.beyondidentity.com/glossary/shoulder-surfing>  Arkose Labs. (n.d.). “What is Credential Abuse?” Arkose Labs.<https://www.arkoselabs.com/credential-stuffing/credential-abuse/#:~:text=In%20a%20credential%20abuse%20attack,the%20target%20system%20or%20network>.  Proofpoint. (n.d.). “Tailgating Attacks.” Proofpoint.<https://www.proofpoint.com/us/threat-reference/tailgating-attacks-cybersecurity#:~:text=A%20tailgating%20attack%20is%20a,behavior%20rather%20than%20digital%20vulnerabilities>.  SolarWinds. (n.d.). “What is an insider threat.” SolarWinds.<https://www.solarwinds.com/resources/it-glossary/insider-threat> |

| **3. Describe the following motivations or desired outcomes of threat actors.** | |
| --- | --- |
| **Fraud** | These threat actors are motivated by financial gain, they hope to illegally acquire sensitive information or some sort of leverage over an establishment or person and then use it to blackmail or masquerade as that person to gain their financial assets |
| **Sabotage** | These threat actors are typically motivated politically, and economically, or have military objectives. They seek to strategically damage or destroy critical assets to disable a plan or action set by a rival organization to gain strategic advantages or intelligence. |
| **Vandalism** | These threat actors are motivated for many reasons, it can be peer pressure, mental instability, recognition, revenge, enjoyment or even sending a message. Unlike sabotage, it doesn’t have to be strategic, but it aims to intentionally damage or deface personal property. |
| **Theft** | These threat actors are motivated for many reasons, which can include financial gain, greed, resentment, or thrill. They aim to steal valuable assets or information to either be sold or to get further access to a system or network for additional gain. |

| Citations: |
| --- |
| Mimecast. (n.d.). “Cyber Fraud.” Mimecast. <https://www.mimecast.com/content/cyber-fraud/>  Dynamic Solutions Group. (n.d.). “Data vandalism What is it, and how do you protect your business.” Dynamic Solutions Group.  <https://www.dsolutionsgroup.com/data-vandalism-what-is-it-and-how-do-you-protect-your-business/#:~:text=Types%20of%20data%20vandalism,with%20inappropriate%20or%20false%20information>  David Kim. Michael G. Solomon. (2023). “Fundamentals of Information System Security.” Jones & Bartlett Learning. [https://mbsdirect.vitalsource.com/reader/books/9781284238815/epubcfi/6/76[%3Bvnd.vst.idref%3DHTML-38]!/4](https://mbsdirect.vitalsource.com/reader/books/9781284238815/epubcfi/6/76%5b%3Bvnd.vst.idref%3DHTML-38%5d!/4) |

| **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** | The risks in finance include personal information like social security, names, addresses. Transaction details like payment details or purchase history. This can also include market details and accounting software. |
| **Medical** | The risks in Medicare include patient medical records and even electronic records. Imaging data like MRI’s or X-rays. Connected device like life-support or heart monitors. This can include the hospitals administration systems. |
| **Educational** | The risks in education include Personal information like student records, Names, Addresses, or SSN’s. Financial data like payroll, loan payments, or tuition. Network infrastructure containing credentials or administrative systems. |
| **Government** | The risks in the government sector include national security secrets like classified documents ,military plans, or secret projects. Citizen information, including social security or financial data. This includes the energy sector like power grids or nuclear energy. |
| **Retail** | The risks in the retail sector include customer data like personal information or payment details. Employee data like names, addresses, or payroll. Inventory management systems which keep track of merchandise. |
| **Pharmaceutical** | The risks in the pharmaceutical sector can include intellectual property like drug formulas and research. Patient information including insurance or medical information. Systems that handle production and distribution. |
| **Entertainment** | The risks in the entertainment industry include intellectual property like movie scripts, movie footage, and contracts. Personal information like staff or actor names, addresses, payment. Management and distributions systems(pirating is caused by this) |

| Citations: |
| --- |
| Ordr.(n.d.). “What is Healthcare Cybersecurity?” Ordr. <https://ordr.net/article/what-is-healthcare-cybersecurity>  SentinelOne. (2024, September 24) “Cyber Security in Finance: Key Threats and Strategies.” SentinelOne. <https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-in-finance/>  Kyle Chin. (2025, Jan 8). “Why is the Education Sector a Target for Cyber Attacks.” UpGuard. <https://www.upguard.com/blog/education-sector-cyber-attacks#:~:text=Social%20engineering%20is%20the%20most,via%20a%20successful%20phishing%20attempt>.  Cybersecurity & Infrastructure Security Agency.(n.d). ”Critical Infrastructure Sectors”  <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>  VerSprite Threat Intelligence Group.(2024, August 14) ”**Retail Cyber Security Threats”**  <https://versprite.com/blog/major-threats-to-the-retail-industry/#:~:text=Physical%20assets%20that%20pose%20significant,%2C%20POS%20systems%2C%20and%20facilities>.  Resolver.(2024, January 2) “**The Top 5 Risks Facing Pharmaceutical Companies.” Resolver.**  <https://www.resolver.com/blog/pharmaceutical-industry-security-threats/> |

1. Response

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

| **Threat Actor** |
| --- |
| **Shoulder Surfers** |

| **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** |
| Being Aware:  Shoulder surfing relies on line-of-sight to be accomplished, placing yourself in such a way that is not noticeable can help to deter them, this can include putting a physical barrier between you and your screen preventing line of sight, you can also limit sensitive transactions in public like entering your passwords or using applications that contain sensitive data. | Hardening device security:  This includes keeping your device locked when not in use or when unattended(Should never be) or making sure that you keep your device up to date with the latest security patches and enhanced features, one should consider using an automatic update feature to make sure it remains guaranteed. Another way is to make sure that you have strong passwords that are difficult to break and do not use common phrases or something that an attacker could guess. | Use alternative methods or tools:  Instead of using common password security, using biometric authentication methods like a fingerprint reader can ensure that an attacker has nothing to observe and make it harder to gain access. Another method is a tool known as a privacy screen, they help to narrow the viewing angle of your device making it harder to see at a distance. |

| Citations: |
| --- |
| LastPass (2024, Septemeber,10).”Understanding Shoulder Surfing and How to Prevent It.”  <https://blog.lastpass.com/posts/shoulder-surfing> |

| **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** |
| Education:  This is not limited to just a workplace but to individuals as well as shoulder surfing can be both an external and an internal threat. Educating people on what the method is and how to prevent it can make it more difficult for attacks to be successful. People are more likely to remain vigilant and implement proper practices to protect themselves and their workplace. | Policies: As mentioned, shoulder surfing can happen anywhere, if it is in a work environment one should implement policies and make it a standard to protect against it. Making it a standard to use biometric security and having strong unguessable passwords along with the use of tools like privacy screens can help to make sure a threat like this cannot happen twice. | Monitoring:  Having a form of constant surveillance can help to deter any future attacks, this is not limited to just the workplace but in public as well, using methods like security cameras will also act as a physical deterrent as attackers wouldn't take the added risk. If it is in the workplace one could also employ security staff who are trained to notice suspicious behavior and can stop it before it happens. |

| Citations: |
| --- |
| LastPass (2024, Septemeber,10).”Understanding Shoulder Surfing and How to Prevent It.”  <https://blog.lastpass.com/posts/shoulder-surfing>  Ema Globyte (2023,March 10).” What is shoulder surfing, and how can you avoid it?”. NordVPN.  <https://nordvpn.com/blog/shoulder-surfing/> |

| **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.** |
| --- |

| I chose this threat actor because this type of threat can often go unnoticed and be underestimated, cyber threats are not usually physical, however after researching it, the repercussions of not preventing it can be astronomical one could have their personal information or assets stolen in an instant and all it takes is for somebody to simply note it down. That being said, some appropriate strategies that I identified include being aware, being vigilant in everyday life noticing suspicious people, and placing yourself in a way that makes it difficult to see your screen so you can prevent an attack from happening. Another method is using alternative methods and tools like biometric authentication and privacy screens. By using biometrics, it makes it theoretically impossible for an attacker to break into your phone by peeking, and using a privacy screen gives added protection where being vigilant might fail. Lastly, keeping your devices up to date on the latest security patches and features adds a layer of protection, even if an attacker does get into your phone some features may still keep them out, for example, take my bank app on my phone for instance, if somebody got past my password and wanted to get into my bank account not only is there a biometric password but the new security update also require an email or phone number for two-factor authentication. These strategies are relevant because they make if more difficult for a shoulder surfer to get what they want and may even deter them from doing it in the first place. |
| --- |