Project 3 Milestone

William Pascoe

CYB-200: Cybersecurity Foundations

Robert Brickan

August 2, 2025

Southern New Hampshire University

CYB 200 Project Three Milestone Decision Aid

I. Detection

1. Describe the following best practices or methods for detecting a threat actor.	
Awareness	Conducting regular training to make employees aware of cyber threats such as phishing emails and other malware that an attacker may be able to use on a system to gain access. (Kim & Solomon, 2023, p. 19)
Auditing	Auditing involves regularly checking your system logs and networks for any irregularities or signs of a breach. (Kim & Solomon, 2023, p.334-337)
Monitoring	Monitoring involves continuously observing your systems for any unusual activity. This can be done through SIEM tools which will automatically scan your system for suspicious activity. (Kim & Solomon, 2023, p.346-347)
Testing	Testing involves simulating cyber-attacks to identify vulnerabilities in your systems and networks. This is done with pen testing tools that can mimic an hacker's attacks. (Kim & Solomon, 2023, p.359-360)
Sandboxing	Sandboxing involves using things like virtual machines to ensure that things like a suspicious email don't contain malware. (Fortinet, 2025) There are also websites like any run (Anyrun, n.d.) that can be used for that as well.

Citations:

Kim, D., & Solomon, M. (2023). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

Fortinet. (2025). What Is Sandboxing? Sandbox Security and Environment. Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-sandboxing

Anyrun. (n.d.). *ANY.RUN - Interactive Online Malware Sandbox*. Any.run. https://any.run/

II. Characterization

2. Briefly define the following threat actors.	
Individuals who are "shoulder surfers"	Shoulder surfers are actors who observe what another person is doing without there knowledge. This can include them entering passwords or looking at sensitive information. (Kim & Solomon, 2023, p.108)
Individuals who do not follow policy	Individuals who don't follow policy can allow data or other things to get stolen by creating situations that allow it. An example would be taking an unsecure laptop home when you are not supposed to or leaving a computer unlocked when you leave your desk to go to the bathroom.
Individuals using others' credentials	These threat actors could either get these credentials from shoulder surfing or other social engineering techniques to allow them access into the system. This can make detection hard because the system isn't going to know whether the right user is logging in or not.
Individuals who tailgate	Tailgaters are actors that follow a person into a building without the person in fronts' knowledge. (Kim & Solomon, 2023, p.108)
Individuals who steal assets from company property	Actors who steal from the company do so to sell or use the stolen property or information.

Citations:

Kim, D., & Solomon, M. (2023). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

3. Describe the following motivations or desired outcomes of threat actors.	
Fraud	Fraud involves stealing money from a company by deceiving them. 396 (Kim & Solomon, 2023, p.396)
Sabotage	Sabotage is something that is done to put a company out of business or cause a government to be harmed. It is usually something much bigger than vandalizing property. (Kim & Solomon, 2023, p.98)
Vandalism	Vandalism is usually done to get the actor's view on something brought out. This can be a hacktivist defacing a website because of a political ideology. (Harisson, 2022) It could also be damaging company property to show they're against them.
Theft	Theft of company property is for personal gain. Either they plan on selling the stolen property or use it in some fashion. (Kim & Solomon, 2023, p.13)

Citations:

Harisson, J. (2022, December 19). What is Cyber Vandalism and How to Avoid It. IT Companies Network. https://itcompanies.net/blog/cyber-vandalism

Kim, D., & Solomon, M. (2023). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

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	Money or bank account information
Medical	Patients' personal information or medical information or even medicine itself
Educational	Research or school equipment
Government	State secrets
Retail	Items to be sold or used or credit card information
Pharmaceutical	Medicine itself or formulas to make medicine to sell to competitors
Entertainment	Intellectual or copyrighted material

Citations:

Kim, D., & Solomon, M. (2023). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

III. Response

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

Threat Actor

Shoulder Surfer

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**
Be mindful of people around you. Always look around to see if you is near you and what they may be doing. (LastPass, 2024)	Limit transactions in public. Avoid entering sensitive information like passwords or PINs when in crowded public spaces. If possible, wait until you are in a more private setting. (LastPass, 2024)	Containment. Quickly isolate affected systems or networks to prevent the spread of the threat.

Citations:

LastPass. (2024). *Prevent Shoulder Surfing Attacks | LastPass - The LastPass Blog*. Lastpass.com. 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**
Use Physical Barriers. Installing protective screens on computer screens prevents people from reading what is on it.	Use alternative authentication methods. Using something like two factor authentication requires someone to not only get your password but also the code which makes it harder to do.	Create strong and unique passwords. Creating unique passwords or passwords that are not things like names make them harder to guess by shoulder surfers.

Citations:

LastPass. (2024). *Prevent Shoulder Surfing Attacks | LastPass - The LastPass Blog*. Lastpass.com. https://blog.lastpass.com/posts/shoulder-surfing

Southern New Hampshire University

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 shoulder surfing because it is a physical security aspect of cyber security. You can have the best firewalls and encryption in the world but if someone is able to get a login ID and password they can bypass all of that are get access to the data they are looking for. I think the methods that I outlined here can be basic but effective counter measures for protecting your data as well a company's data.