**5-3 Project Three Milestone:**

**Decision Aid**

Matthew A Keaton

Southern New Hampshire University

CYB 200: Cybersecurity Foundations

Professor Linda Hamons

April 7, 2024

# CYB 200 Project Three Milestone Decision Aid Template

1. Detection

| **1. Describe the following best practices or methods for detecting a threat actor.** | |
| --- | --- |
| **Awareness** | Ensure all members are aware of the security policies of the organization. All members of the Computer Incident Response Team know who to contact. All incident responders have access to journals and incident response toolkits. All members participated in incident response drills/training (Kral, 2012). |
| **Auditing** | Review the logs to ensure computing environments and security controls work as expected. Are security policies sound and appropriate for business or activity. Are there controls supporting the policies. Is there effective implementation and upkeep of controls (kim & solomon, 2023, pg. 359). |
| **Monitoring** | Monitor traffic with an IDS that can identify abnormal traffic for further investigation. Using IPS can actively block malicious traffic. Prior to using IDS and IPS we must create a baseline definition of normal traffic (Kim & Solomon, 2023, pg. 359) |
| **Testing** | Test to identify any vulnerabilities on a system to address them. A system may have been secure, but adding a new application could add vulnerabilities (Kim & Solomon, 2023, pg 359) |
| **Sandboxing** | A strategy used for separating programs and running them in their own virtual space to inspect and observe code (Kim & Solomon, 2023, pg. 518) |

| Citations: |
| --- |
| Kim, D. & Solomon, M.G. (2023). *Fundamentals of Information Systems Security, 4th Edition*. Jones and Bartlett Publishers. <https://openpage-ebooks.jblearning.com/wr/viewer.html?skipLastRead=true&oneTimePasscode=ST>3209c3eb-26474c27-bdd9-9653b52d36ee&launchOrgCode=jbl&language=en-US#//HTML-1  Kral, P. (2012, February 21). *Alison Kim*. SANS Institute. https://www.sans.org/white-papers/33901/ |

1. Characterization

| **2. Briefly define the following threat actors.** | |
| --- | --- |
| **Individuals who are “shoulder surfers”** | A type of social engineering attack where a human attempts to deceive another human into doing something or divulging information such as looking over the shoulder of a person typing into a computer screen (Kim & Solomon, 2023, pg. 108) |
| **Individuals who do not follow policy** | This can be an insider threat, someone who causes harm to their organization by not following policy who is an employee, contractor, or trusted person (Kim & Solomon, 2023, pg. 511) |
| **Individuals using others’ credentials** | Credential harvesting and stuffing, when hackers obtain ID’s and passwords to gain unauthorized access. Can also be a form of identity theft. (Kim & Solomon, 2023, pg. 102) |
| **Individuals who tailgate** | Someone tailgating a person is defined as a social engineering attack. Where this person is following close behind to divulge information or gain access to a facility behind the person opening the door (Kim & Solomon, 2023, pg. 108) |
| **Individuals who steal assets from company property** | Someone who steals assets from company property is an insider threat. Danger caused from an employee, contractor, or trusted person (Kim & Solomon, 2023, pg. 511) |

| Citations: |
| --- |
| Kim, D. & Solomon, M.G. (2023). *Fundamentals of Information Systems Security, 4th Edition*. Jones and Bartlett Publishers. <https://openpage-ebooks.jblearning.com/wr/viewer.html?skipLastRead=true&oneTimePasscode=ST>3209c3eb-26474c27-bdd9-9653b52d36ee&launchOrgCode=jbl&language=en-US#//HTML-1 |

| **3. Describe the following motivations or desired outcomes of threat actors.** | |
| --- | --- |
| **Fraud** | Fraud crimes focus on extracting revenue from victims (Kim & Solomon, 2023, pg. 396) |
| **Sabotage** | Destruction of property or obstruction to normal operation. Attacks the availability property of information security (Kim & Solomon, 2023, pg. 98) |
| **Vandalism** | Destructive attacks are used without profit or ideological motives. Will attack websites, company services, or delete databases (NordVPN, n.d.) |
| **Theft** | Is the stealing of confidential data, information, or identity to gain leverage or profit. |

| Citations: |
| --- |
| Kim, D. & Solomon, M.G. (2023). *Fundamentals of Information Systems Security, 4th Edition*. Jones and Bartlett Publishers. <https://openpage-ebooks.jblearning.com/wr/viewer.html?skipLastRead=true&oneTimePasscode=ST>3209c3eb-26474c27-bdd9-9653b52d36ee&launchOrgCode=jbl&language=en-US#//HTML-1  NordVPN. (2024, March 27). *Cyber vandalism definition - glossary*. https://nordvpn.com/cybersecurity/glossary/cyber-vandalism/#:~:text=Cyber%20vandalism%20is%20a%20destructive,company’s%20services%2C%20or%20delete%20databases. |

| **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** | Bank accounts, trading accounts, purchasing accounts, corporate credit cards, and other direct sources of money or credit. |
| **Medical** | Patient information can be used as identity theft and medical records can be held as ransom and loss of use of medical equipment. |
| **Educational** | Student records and information, student financial aid information, and educational software or technology. |
| **Government** | National security information, infrastructure information, law enforcement software and databases, and military plans. |
| **Retail** | Customer credit cards, software that tracks inventory, transaction records, and customer accounts or personal information. |
| **Pharmaceutical** | Customer records and personal information, clinical data, and manufacturing process. |
| **Entertainment** | Streaming services, customer accounts and data, and copyrighted content. |

| Citations: |
| --- |
| Kim, D. & Solomon, M.G. (2023). *Fundamentals of Information Systems Security, 4th Edition*. Jones and Bartlett Publishers. <https://openpage-ebooks.jblearning.com/wr/viewer.html?skipLastRead=true&oneTimePasscode=ST>3209c3eb-26474c27-bdd9-9653b52d36ee&launchOrgCode=jbl&language=en-US#//HTML-1 |

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** |
| Change all passwords and login information of any sites you accessed prior to the incident. | Call your bank to notify them of the incident to monitor your account and obtain new credit cards. | Request that the credit bureau freeze your account to ensure no new line of credit is opened in your name or other malicious activity can occur. |

| Citations: |
| --- |
| Walsh, K. (2023, August 24). *How to protect yourself from a shoulder surfing attack*. All About Cookies. https://allaboutcookies.org/what-is-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 a private screen on your computers monitor to ensure people can’t see your information without you knowing. | When using a computer in a public place ensure to sit with your back against the wall. | Ensure not to discuss sensitive information over the phone when people are around or in a public setting. |

| Citations: |
| --- |
| Hanna, K. T. (2021, October 29). *What is shoulder surfing? how do you protect yourself from it?*. Security. https://www.techtarget.com/searchsecurity/definition/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 it is very common. In a normal workday many people in the office walk by my computer and some will stay for a little while just to talk and make conversation. Prior to understanding the threat of shoulder surfers, I never worried about what was on my screen when I talked to other co-workers. Now, I am very conscious of what information is displayed on my screen and who may be able to see it. The strategies I chose to respond to the threat actor are ones that can be done the quickest once made aware of the incident and protect your finances. Finances are one of the biggest stresses in our lives as well as a big motivator for attackers. People work extremely hard to become financially stable, so to respond to the threat by blocking their access to my finances will prevent me from losing something that I may not be able to recover from. The tactics mentioned to proactively respond to this threat actor will help minimize the chances of it happening again. It makes it more difficult for a shoulder surfer to see the information on your screen if the only way to do so is to get even closer. This will make it easier for us to detect when something doesn’t seem normal. For example, sitting with your back to the wall at a coffee shop will help you identify when someone is leaning over more or making weird movements to get an angle just to see your screen. These steps are just some of many potential tactics that can be used to respond to threat actors. |
| --- |