Southern New Hampshire University

CYB 200 Project Two Milestone: “Decision Aid”

Written By: Max Navarrette

Course: CYB-200-J9875 Cybersecurity Foundations 24EW4

Professor: Robert Brickan

Complete the template by filling in the blank cells provided.

I. Detection

1. Describe the following best practices or methods for detecting a threat actor.	
Awareness	Cultivating Awareness through comprehensive training and threat intelligence can help detect threat actors. Organizations should ensure that their employees are aware of current cyber threats manifests. An example of this is a company implementing regular cybersecurity workshops that cover the latest phishing techniques and how to report suspicious activities. Cebula, popeck, and young (2014) emphasize the importance of maintaining situational awareness to detect unusual activity that could indicate the presence of threat actors.
Auditing	Auditing is a critical activity for detecting unauthorized access of anomalies that could indicate the presence of a threat actor. Regular reviews of system logs, user activities, and network traffic are vital. For instance, a financial institution might perform monthly audits of transaction logs to spot unusual patterns that could suggest fraudulent activity, reflecting the importance of information system auditing as a key security control in the detection of cyber threats. Ross et al. (2004) conveys that information system auditing is a key security control that supports the detection of cyber threats.
Diligence	Diligence involves consistently applying security measures and practices. This includes regularly updating and patching systems, which are fundamental activities for detection and prevention of cyber threats. An example is a software development firm that uses automated tools to track and deploy the latest security patches for their development environments, aligning with the guidance on managing security controls to assist in early threat detection. Stine et al. (2008) highlights the importance of diligence in classifying information systems and managing security controls, which can assist in early threat detection.
Monitoring	Continuous monitoring of systems and networks allows for the timely detection of threat actor activities. A practical example is a retail company using intrusion detection systems (IDS) to monitor for suspicious network traffic that could indicate a data breach, which is a critical aspect of security control within the Risk Management Framework. Implementation of the risk management Framework includes continuous monitoring as a critical aspect of security control, as detailed by the Joint Task Force (2016).
Testing	Testing of security measures through activities like penetration testing and vulnerability scanning is an important method for detecting possible threat actors' entry points or holes in configurations. A practical example of this would be, a tech company might hire external security consultants to perform bi-annual penetration tests to identify and address vulnerabilities, demonstrating the importance of such testing in identifying and mitigating potential threats, physical or digitally. Kral (2011) describes such testing as an essential component of an incident handler's toolkit, capable of identifying and mitigating potential threats.

1. Describe the following best practices or methods for detecting a threat actor.	
Sandboxing	Sandboxing technology can detect threat actors (depending on the software being used) by isolating and analyzing suspicious code, files, or programs in a controlled/simulated environment. A common example is an email service provider that uses sandboxing to analyze attachments in emails that could potentially contain malware, helping to detect threats that may evade traditional antivirus solutions. Software such as VMware, Viritual box (by Oracle), UTM virtual machine player for Macs, for virtual machines and Windows sandboxing also count as sandboxing methods. This practice is effective against evasive malware, which often overlooked by traditional defenses (*MITRE ATT&CK*®, n.d.)
Enticing	Implementing enticing measures, such as honeypots, can lure threat actors into revealing their tactics. For instance, a data center might deploy a network of honeypots that mimic vulnerable servers to attract and study the behavior of attackers, providing insights into potential threats and their methods of operation. By analyzing interactions with these traps, organizations can gain insight into potential threats and their methods of operation. (Cebula et al., 2014)

Citations:

Cebula, J., Popeck, M., & Young, L. (2014). *A Taxonomy of Operational Cyber Security Risks Version 2 CERT ® Division* (pp. 1–48). https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf

Joint Task Force (JTF). (2016). *Risk Management Framework (RMF) Overview - Risk Management | CSRC*. Nist.gov. https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

Kral, P. (2011). *Incident Handler's Handbook* (pp. 1–19). https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

MITRE ATT&CK®. (n.d.). Attack.mitre.org. https://attack.mitre.org/versions/v8/

Ross, R., Katzke, S., Johnson, L., Swanson, M., Stoneburner, G., Rogers, G., & Lee, A. (2005, June 17). *Recommended Security Controls for Federal Information Systems*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/53/upd2/final

Citations:

Ross, R., Swanson, M., Stoneburner, G., Katzke, S., & Johnson, L. (2004, May 20). *Guide for the Security Certification and Accreditation of Federal Information Systems*. Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-37/archive/2004-05-20

Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick, J., Gutierrez, C., & Turner, J. (2008). Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. *NIST Special Publication*, *1*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

II. Characterization

2. Briefly define the following threat actors.	
Individuals who are "shoulder surfers"	Shoulder surfers are individuals who gain unauthorized access to sensitive information through direct observation techniques. This behavior can lead to data breaches and is considered a security risk that organizations need to mitigate through physical security measures and awareness training (Cebula et al., 2014). An example would be someone at an ATM peeking at another user's PIN entry.
Individuals who do not follow policy	Employees or insiders who ignore organizational policies can introduce significant vulnerabilities. Non-compliance can lead to various information security risks, and enforcing policy adherence is a critical aspect of risk management (Ross et al., 2005). An example of an instance such as this would be not updating their passwords regularly or using unapproved software.
Individuals using others' credentials	This refers to individuals who obtain and misuse others' login credentials. The unauthorized use of credentials can bypass many security controls and grant access to sensitive systems and information (Ross et al., 2004). For instance, an employee logging into a colleague's computer without permission.
Individuals who tailgate	Tailgating is a method used by unauthorized individuals to gain physical access to restricted areas by following authorized personnel. This security breach can be addressed by physical security controls and employee training (Kral, 2011). An example is an unauthorized person slipping into a secured building by walking in with an employee who has access.
Individuals who steal assets from company property	Individuals who steal assets from company property: Theft of physical assets from a company encompasses stealing devices, documents, or intellectual property. Such incidents can result in a direct loss of assets and potential data breaches (Cebula, Popeck, & Young, 2014). An example of this would be taking a laptop, keycard or confidential files from office premises.

Citations:

Cebula, J., Popeck, M., & Young, L. (2014). *A Taxonomy of Operational Cyber Security Risks Version 2 CERT ® Division* (pp. 1–48). https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf

Ross, R., Katzke, S., Johnson, L., Swanson, M., Stoneburner, G., Rogers, G., & Lee, A. (2005, June 17). *Recommended Security Controls for Federal Information Systems*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/53/upd2/final

Ross, R., Swanson, M., Stoneburner, G., Katzke, S., & Johnson, L. (2004, May 20). *Guide for the Security Certification and Accreditation of Federal Information Systems*. Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-37/archive/2004-05-20

Kral, P. (2011). *Incident Handler's Handbook* (pp. 1–19). https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

3. Describe the following motivations or desired outcomes of threat actors.	
Fraud	Typically involves deception to gain financial advantages, such as manipulating or falsifying data to achieve unauthorized benefits (Cebula et al., 2014). An instance of this would be manipulating company financial reports or conducting unauthorized transactions.
Sabotage	This is the act that is often motivated by desire to disrupt operations on or off premises potentially to cause financial, reputational, and "emotional" damage to a business or organizations (Ross et al., 2005). An example of this would be an employee who could have some kind of personal vendetta against the company or undermine the company's competitive standing, compromising company secrets or espionage.
Vandalism	Vandalism in the cybersecurity context usually refers to defacing websites or damaging digital assets, often motivated by the desire to make a statement or simply cause disruption in belief or for a cause possibly involving hacktivism or retribution (Cebula et al., 2014). An instance of this would be someone motivated by a desire to protest or simply to cause disruption for its own sake.
Theft	Theft is the act of stealing company assets, which can range from physical devices to sensitive data, usually motivated by financial gain (Stine et al., 2008). An instance of this would be a person who takes a company's valuable assets involving sensitive information for either personal use, resale on the black market or even selling to a rival company to gain competitive advantage.

Citations:

Cebula, J., Popeck, M., & Young, L. (2014). *A Taxonomy of Operational Cyber Security Risks Version 2*

CERT ® Division (pp. 1–48).

https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf

Ross, R., Katzke, S., Johnson, L., Swanson, M., Stoneburner, G., Rogers, G., & Lee, A. (2005, June 17).

Recommended Security Controls for Federal Information Systems. Csrc.nist.gov.

https://csrc.nist.gov/pubs/sp/800/53/upd2/final

Citations:

Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick, J., Gutierrez, C., & Turner, J. (2008). Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. *NIST Special Publication, 1*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

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	Threat actors may target customer account information, transaction data, financial records, wire transfers, and internal financial applications (Ross et al., 2005). Customer account data, credit card information, and investment details are at risk, as these can be used for identity theft or unauthorized transactions.
Medical	At risk are electronic health records (EHRs), patient data, medical research, and healthcare management systems (Stine et al., 2008). Patient records and prescription information are at risk, which could lead to medical identity theft or privacy violations.
Educational	Personal information of students and faculty, academic research, and educational resources could be compromised (Stine et al., 2008). Student records and research data are at risk, potentially affecting personal privacy and intellectual property.
Government	Classified information, infrastructure data, internal communications, and citizen services platforms are potential targets (Ross et al., 2005). Classified documents and personal data of citizens are at risk, which could compromise national security and personal privacy.
Retail	Payment processing systems, customer data, inventory systems, and proprietary business intelligence may be at risk (Ross et al., 2005). Credit card details and customer profiles are at risk, which can be used for fraudulent purchases or identity theft.
Pharmaceutical	Intellectual property, research data, clinical trial information, and regulatory submissions could be targeted by threat actors (Stine et al., 2008). Drug formulas and clinical trial data are at risk, which could be stolen for corporate espionage or to counterfeit medications.
Entertainment	Digital media assets, customer subscription data, and proprietary production software are at risk from cyber threats (Stine et al., 2008). Unreleased media content and customer viewing habits are at risk, which could be used for piracy or to manipulate market trends.

Citations:

Ross, R., Katzke, S., Johnson, L., Swanson, M., Stoneburner, G., Rogers, G., & Lee, A. (2005, June 17). *Recommended Security Controls for Federal Information Systems*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/53/upd2/final

Stine, K., Kissel, R., Barker, W., Fahlsing, J., Gulick, J., Gutierrez, C., & Turner, J. (2008). Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. *NIST Special Publication, 1*. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

III. Response

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

Threat Actor

"Individuals who do not follow policy"

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**
Immediate and reinforcement of policies. When a policy violation is detected, it is crucial to address the breach and promptly remind the individuals involved of the specific policies and the importance of adherence to said policies (Ross et al., 2005). I would also add the stakes involved if said individuals ignoring company or organizational policies and the consequences of what happens if the policies are not followed.	Employee sanctions and disciplinary actions. Implement a system of consequences for non-compliance to policies, which could range from warnings to termination, depending on the severity of the violation (Kral, 2011).	Post-incident analysis and education. Conduct a thorough investigation to understand why the policy was not followed and use the findings to educate the workforce, thus preventing future occurrences (Ross et al., 2004). An investigation would determine the cause of the lapse, followed by targeted training sessions to educate staff on secure communication protocols.

Citations:

Kral, P. (2011). *Incident Handler's Handbook* (pp. 1–19). https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Citations:

Ross, R., Katzke, S., Johnson, L., Swanson, M., Stoneburner, G., Rogers, G., & Lee, A. (2005, June 17). *Recommended Security Controls for Federal Information Systems*. Csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/53/upd2/final

Ross, R., Swanson, M., Stoneburner, G., Katzke, S., & Johnson, L. (2004, May 20). *Guide for the Security Certification and Accreditation of Federal Information Systems*. Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-37/archive/2004-05-20

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**
Regular policy review and update. Ensure that policies are up to date and reflect the current threat landscape and organizational practices, making them more relevant and easier to follow (Ross et al., 2004). An example of this would be updating remote work policies to include the use of VPNs and secure Wi-Fi networks.	Continuous awareness training. Engage employees with ongoing training programs that emphasize the importance of policy compliance and the potential consequences of non-compliance (Cebula et al., 2014). Continuous awareness training could include monthly cybersecurity awareness workshops that cover topics like social engineering, phishing, and the importance of following company policies.	Implementing technical controls. Use technical solutions like access controls and user activity monitoring to enforce policy adherence and detect deviations in real-time (Ross et al., 2005). Implementing technical controls could involve the deployment of a system that automatically logs employees out of sensitive systems after a period of inactivity, thereby reducing the risk of unauthorized access due to employees leaving their workstations unsecured.

Citations:

Cebula, J., Popeck, M., & Young, L. (2014). *A Taxonomy of Operational Cyber Security Risks Version 2*

CERT ® Division (pp. 1–48).

https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf

Ross, R., Katzke, S., Johnson, L., Swanson, M., Stoneburner, G., Rogers, G., & Lee, A. (2005, June 17).

Recommended Security Controls for Federal Information Systems. Csrc.nist.gov.

https://csrc.nist.gov/pubs/sp/800/53/upd2/final

Citations:

Ross, R., Swanson, M., Stoneburner, G., Katzke, S., & Johnson, L. (2004, May 20). *Guide for the Security Certification and Accreditation of Federal Information Systems*. Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-37/archive/2004-05-20

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.

Choosing "Individuals who do not follow policy" as the threat actor for this research is informed by the understanding that insider threats, whether malicious or negligent, can be as damaging as external attacks. Strategies for responding to this type of threat actor are centered around the reinforcement of policies and the establishment of a culture of compliance. The reactive strategies aim to mitigate any immediate risk posed by the violation, while the proactive strategies are designed to prevent future occurrences by strengthening the policy framework and enhancing the security culture within the organization. These strategies are supported by industry best practices and guidelines for managing information security risks (Cebula et al., 2014; Ross et al., 2005; Ross et al., 2004). The strategies identified are appropriate because they address both the behavioral and technical aspects of the problem. Immediate remediation and reinforcement of policies tackle the issue directly at the moment of violation, ensuring that the employee understands the importance of compliance. Disciplinary actions serve as a deterrent to future non-compliance. Post-incident analysis and education help to understand the root cause and spread awareness to prevent recurrence. Regular policy reviews ensure that guidelines keep pace with evolving threats, while continuous training keeps security at the forefront of employees' minds. Technical controls act as a safety net to enforce policies and protect against human error. Together, these strategies create a comprehensive approach to managing the risk posed by individuals who do not follow policy, aiming to foster a culture of security awareness and compliance within the organization.