Samuel N. Oruh | CYB469-O 01 - Project and Portfolio VI: Cybersecurity | Prof. Bill Michelin
September 10, 2023

Assignment 2
Using Key Performance Indicators (KPIs)

1. **What is the name of the Security KPI that you chose to implement and a clickable link?**

   One of the Security KPIs that I chose to implement is the Mean Time to Identify (MTTI) KPI . The MTTI is a metric used to measure the time it takes for an organization to identify a security breach or incident. In a real-world situation, MTTI can be used to help organizations identify and respond to security incidents more quickly, reducing the potential damage caused by the incident. For example, if an organization has a low MTTI, it means that they are able to detect and respond to security incidents quickly, which can help prevent data breaches and other security incidents. On the other hand, if an organization has a high MTTI, it means that they may not be able to detect and respond to security incidents quickly, which can increase the risk of a data breach or other security incident.
   Link: https://cybertalents.com/blog/top-15-cybersecurity-metrics-and-kpis-for-better-security

2. **Explain Security KPIs and how they are used in real-world situations?**

   Through the reading and my further research online, I found twenty-two (22) Key Performance Indicators (KPIs) These KPIs help organizations evaluate the effectiveness of their cybersecurity measures, identify potential vulnerabilities, and make informed decisions to improve their security posture. By tracking these KPIs, organizations can better understand their security performance and make necessary adjustments to enhance their cybersecurity strategy. They are as follows:

   1. **Security Incidents:** This KPI measures the number of security events that compromise the confidentiality, integrity, or availability of an organization's data, systems, or networks and that have occurred within a specific time frame. These incidents can include data breaches, malware infections, insider threats, or any other security-related events. Monitoring security incidents can be crucial for assessing the overall health of an organization's cybersecurity posture. Tracking the number, types, and severity of security incidents helps in understanding the evolving threat landscape and identifying vulnerabilities that need mitigation.
      Link: https://crashtest-security.com/cyber-security-metrics/

   2. **Intrusion Attempts:** This KPI tracks the number of attempted unauthorized access events like scanning for vulnerabilities, brute-force attacks, or exploiting known weaknesses that are conducted by external or internal actors trying to breach an organization's networks or systems. It helps organizations understand the effectiveness of their security measures and identify potential vulnerabilities. Monitoring intrusion attempts is essential for gauging the effectiveness of security controls and understanding the persistence and sophistication of attackers. A higher number of intrusion attempts may indicate increased targeting or vulnerability exposure.
      Link: https://www.upguard.com/blog/cybersecurity-metrics

Assignment 2
Using Key Performance Indicators (KPIs)

3. **Mean Time to Identify (MTTI):** MTTI is the average time it takes to identify the root cause or source of a security incident after it has been detected. It helps organizations understand why incidents occur and how to prevent them in the future. A lower MTTI indicates a faster understanding of the underlying issues that led to a security incident. To calculate MTTI, organizations should track the time from incident detection to root cause analysis. Reducing MTTI involves improving forensic and investigative capabilities, as well as maintaining comprehensive logs and records.
   Link: https://cybertalents.com/blog/top-15-cybersecurity-metrics-and-kpis-for-better-security

4. **Mean time to detect (MTTD):** MTTD measures the average time it takes to detect a security incident from the moment it occurs. It quantifies the effectiveness of an organization's security monitoring and detection capabilities. A shorter MTTD is desirable as it indicates the ability to identify and respond to security incidents promptly. It helps in minimizing the potential damage caused by incidents and reducing the dwell time of attackers within the network.
   Link: https://crashtest-security.com/cyber-security-metrics/

5. **Mean time to contain (MTTC):** MTTC measures the average time it takes to contain or mitigate a security incident after it has been detected. It evaluates how quickly an organization can isolate and prevent the spread of an incident. A shorter MTTC is essential for preventing security incidents from escalating and causing further harm. Effective containment measures can minimize the extent of damage and reduce the overall cost of incident response.
   Link: https://crashtest-security.com/cyber-security-metrics/

6. **Mean time to resolve (MTTR):** MTTR is the average time it takes to resolve a security incident once it has been detected. It assesses the efficiency of an organization's incident response and remediation processes. A shorter MTTR is preferable, as it indicates a swift and effective response to security incidents. Efficient incident resolution helps in reducing the impact of incidents and limiting potential losses.
   Link: https://crashtest-security.com/cyber-security-metrics/

7. **Level of Preparedness:** Level of Preparedness measures an organization's readiness to respond to security incidents and disasters. It encompasses factors such as the existence of a well-documented incident response plan, employee training, and the availability of necessary resources. A high level of preparedness indicates that an organization is proactive in its approach to security, reducing the potential impact of security incidents.
   Link: https://cybertalents.com/blog/top-15-cybersecurity-metrics-and-kpis-for-better-security

8. **Unidentified Devices on Internal Networks:** This KPI assesses the number and nature of devices on internal networks that cannot be identified or authenticated. Unidentified

Assignment 2
Using Key Performance Indicators (KPIs)

devices can pose security risks. Regularly monitoring unidentified devices helps in identifying potential threats, as these devices may be unauthorized or compromised.
Link: https://securityscorecard.com/blog/kpis-for-security-operations-incident-response/

9. **Mean Time Between Failures (MTBF):** MTBF measures the average time between system failures. It is often used in the context of hardware reliability. A higher MTBF indicates better hardware reliability, which can indirectly affect security by reducing the frequency of system outages and vulnerabilities that result from them.
Link: https://crashtest-security.com/cyber-security-metrics/

10. **Non-human Traffic (NHT):** NHT measures the proportion of network traffic generated by non-human entities, such as bots and automated scripts. A high level of NHT can indicate potential security risks, as malicious bots may be attempting to exploit vulnerabilities or engage in other harmful activities.
Link: https://www.upguard.com/blog/cybersecurity-metrics

11. **Mean Time to Acknowledge (MTTA):** MTTA measures the average time it takes for an organization to acknowledge a security incident once it has occurred. Reducing MTTA is crucial for effective incident response. A shorter acknowledgment time can help mitigate the impact of security incidents.
Link: https://securityscorecard.com/blog/kpis-for-security-operations-incident-response/

12. **First Party Security Ratings:** First-party security ratings assess an organization's own security posture and practices. These ratings provide insights into an organization's self-assessment of its security, which can be compared with external assessments to identify gaps and improve security.
Link: https://www.bitsight.com/blog/7-cyber-security-kpis-will-resonate-cybersecurity-dashboard-your-board-directors

13. **Average Vendor Security Rating:** This KPI measures the average security rating of third-party vendors and suppliers that the organization relies on. A low average vendor security rating can indicate a higher risk of security incidents originating from the supply chain, making it essential to manage vendor security effectively.
Link: https://www.bitsight.com/blog/7-cyber-security-kpis-will-resonate-cybersecurity-dashboard-your-board-directors

14. **Access Management:** Access Management measures how effectively an organization controls and monitors user access to systems and data. Strong access management practices are essential for preventing unauthorized access and data breaches.
Link: https://www.upguard.com/blog/cybersecurity-metrics

Assignment 2
Using Key Performance Indicators (KPIs)

15. **Company vs Peer Performance:** This KPI compares an organization's security performance to that of its peers or industry benchmarks. Benchmarking helps identify whether an organization's security measures are above or below industry standards, providing insights for improvement.
    Link: https://www.investopedia.com/terms/k/kpi.asp

16. **Patching Cadence:** Patching cadence measures how quickly an organization applies security patches and updates to its systems and software. A faster patching cadence is critical to addressing known vulnerabilities promptly, reducing the window of opportunity for attackers.
    Link: https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track/

17. **Authentication Errors:** Authentication errors refer to instances where users fail to provide the correct credentials (e.g., username and password) to access a system or application. These errors can result from various factors, including mistyped passwords, forgotten credentials, or attempted unauthorized access. High authentication error rates can indicate security risks, user frustration, and potential vulnerabilities in the authentication process. Monitoring authentication errors helps in identifying patterns of failed login attempts, potentially revealing brute force attacks, account compromise attempts, or usability issues. It's crucial for maintaining system security and user satisfaction.
    Link: https://www.upguard.com/blog/cybersecurity-metrics

18. **Policy Violations:** Policy violations occur when users or systems do not adhere to established security, compliance, or organizational policies. These violations may involve data breaches, unauthorized access, or actions that go against established rules. Tracking policy violations is essential for ensuring compliance with legal and regulatory requirements, safeguarding sensitive data, and maintaining the integrity of organizational policies. Organizations should monitor policy violations to identify weaknesses in their security measures and provide evidence for compliance audits. Addressing violations promptly can mitigate risks and prevent future breaches.
    Link: https://securityscorecard.com/blog/kpis-for-security-operations-incident-response/

19. **Time Needed to Resolve Errors:** This KPI measures the average time it takes to resolve errors, incidents, or issues once they are identified. It includes the time from detection to resolution. Reducing the time to resolve errors is crucial for minimizing downtime, maintaining user satisfaction, and ensuring efficient operations. Tracking the time needed to resolve errors allows organizations to assess their incident response capabilities. By analyzing this KPI, they can identify bottlenecks, streamline processes, and enhance their ability to address issues promptly.
    Link: https://www.bigpanda.io/incident-management-kpis/

Assignment 2
Using Key Performance Indicators (KPIs)

20. **Cost Per Incident:** Cost per incident calculates the financial expenditure associated with handling and resolving each security incident or error. It includes expenses such as personnel time, software/hardware costs, legal fees, and more. Understanding the cost per incident helps organizations manage their security budget effectively and allocate resources efficiently. By tracking the cost per incident, organizations can evaluate the financial impact of security breaches, identify cost-effective mitigation strategies, and justify investments in security measures.
    Link: https://www.atlassian.com/incident-management/kpis

21. **Event Attendance:** Event attendance measures the number of individuals or entities that participate in specific events, such as conferences, seminars, webinars, or training sessions. Attendance is essential for evaluating the success of outreach, marketing, or educational initiatives and assessing the level of engagement with the target audience. Monitoring event attendance allows organizations to gauge the interest in their offerings, tailor future events to specific audiences, and assess the return on investment for marketing and educational efforts.
    Link: https://onstrategyhq.com/resources/27-examples-of-key-performance-indicators/

22. **Insider Threat Score:** This KPI that measures the likelihood of an insider threat occurring in an organization. It is calculated based on various factors such as employee behavior, access to sensitive data, and security incidents. The score can be used to identify employees who pose a high risk of committing insider threats and take appropriate measures to prevent such incidents. For example, if an employee has a high insider threat score, the organization can monitor their activities more closely, restrict their access to sensitive data, and provide additional training to prevent them from committing insider threats.
    Link: https://www.bitsight.com/blog/the-most-useful-and-impactful-security-metrics-every-ciso-should-have

Real-world examples of KPIs:

1. **Malware Events:**
    Link: https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry
    A real-world example of a malware event is the WannaCry ransomware attack in 2017. This attack affected over 200,000 computers across 150 countries, causing significant disruptions to businesses and public services. Monitoring the number of malware events and their impact on an organization can help identify trends and vulnerabilities, allowing for more effective prevention and response strategies.

2. **Third-party Risk:**
    Link: https://coverlink.com/cyber-liability-insurance/target-data-breach/
    The 2013 Target data breach is an example of third-party risk. In this case, the attackers gained access to Target's network through a third-party HVAC vendor, ultimately

Assignment 2
Using Key Performance Indicators (KPIs)

compromising the personal and financial information of millions of customers. Monitoring third-party risk KPIs can help organizations identify potential vulnerabilities in their supply chain and implement appropriate security measures to mitigate these risks.

3. **Phishing Events:**
   Link: https://www.idstrong.com/sentinel/the-dnc-hack/
   A real-world example of a phishing event is the 2016 attack on the Democratic National Committee (DNC). Attackers used spear-phishing emails to trick DNC employees into revealing their login credentials, leading to the theft of sensitive information. Tracking phishing events as a KPI can help organizations identify trends and vulnerabilities, allowing them to implement more effective training and awareness programs to reduce the risk of successful phishing attacks.

4. **Vulnerability Management:**
   Link: https://www.linkedin.com/pulse/equifax-data-breach-2017-prashant-ghimire/
   The Equifax data breach in 2017 is an example of the importance of vulnerability management. In this case, attackers exploited a known vulnerability in the Apache Struts web application framework, which Equifax had failed to patch in a timely manner. Monitoring vulnerability management KPIs, such as the number of known vulnerabilities and the time taken to apply patches, can help organizations prioritize their efforts and reduce the risk of breaches due to unpatched vulnerabilities. In conclusion, monitoring and analyzing KPIs related to cybersecurity can help organizations identify trends, vulnerabilities, and areas for improvement. By focusing on these KPIs, organizations can better protect their networks, systems, and data from cyber threats and minimize the impact of security incidents.

3. Research current events and case studies and provide a real-world example that demonstrates how a KPI was utilized or how it could have been utilized to combat the situation in the example. Include a clickable link to your sources.

A. Explain how, in the example, either the KPI was used or could have used to combat the situation.

Here are two real-world examples of how one of the KPIs that I found could have been used to combat the situation:

1. **Key Performance Indicator (KPI):** Insider Threat Score
   Real-World Example: The 2019 Capital One Bank Data Breach
   Link: https://dl.acm.org/doi/10.1145/3546068
   In the Capital One breach, a former employee of Amazon Web Services (AWS) gained access to Capital One's data stored on AWS servers. The Insider Threat Score KPI could

Assignment 2
Using Key Performance Indicators (KPIs)

have been used to identify the potential threat posed by this employee by monitoring the employee's behavior and their access to sensitive information. The Insider Threat Score KPI would have identified the employee as a potential insider threat which would have allowed Capital One to take action to prevent the breach from occurring.

2. **Key Performance Indicator (KPI):** User Training and Awareness Score
   Real-World Example: The 2016 Democratic National Committee (DNC) Phishing Attack.
   Link: https://www.idstrong.com/sentinel/the-dnc-hack/
   In the case of the DNC phishing attack, a high User Training and Awareness Score could have played a pivotal role in combatting the situation. If the DNC's employees had undergone effective cybersecurity training and were aware of phishing threats, they might have been less likely to fall for the phishing emails that led to the breach. A strong User Training and Awareness Score could have helped the organization identify and mitigate the attack earlier, potentially preventing sensitive data from being compromised.

Sources:

1. Seven Pillars Institute. (2021, April 30). Case Study: Equifax Data Breach. Retrieved from https://sevenpillarsinstitute.org/case-study-equifax-data-breach/

2. Information Security Policies, Procedures, and Standards, Chapter 2. (2017, March). Landoll, Douglas J. Retrieved from https://learning.oreilly.com/library/view/information-security-policies/9781482245912/xhtml/11_Chapter02.xhtml

3. UpGuard. (2023, April 6). 14 Cybersecurity Metrics + KPIs You Must Track in 2023. Retrieved from Retrieved from https://www.upguard.com/blog/cybersecurity-metrics

4. Investopedia. (2023, May 10). Key Performance Indicator (KPI): Definition, Types, and Examples. Retrieved from https://www.investopedia.com/terms/k/kpi.asp

5. BigPanda. (2021, August 23). Incident Management KPIs - Tracking & Monitoring. BigPanda. Retrieved from https://www.bigpanda.io/incident-management-kpis/

6. Atlassian. (2014, July 16). How to choose incident management KPIs and metrics. Retrieved from https://www.atlassian.com/incident-management/kpis

7. OnStrategyHQ. (2023, April 24). 27 KPI Examples: A Guide to Great Key Performance Indicators. Retrieved from https://onstrategyhq.com/resources/27-examples-of-key-performance-indicators/

Assignment 2
Using Key Performance Indicators (KPIs)

8. Reciprocity. (2023, June 22). Cybersecurity KPIs to Track: Examples. Retrieved from https://reciprocity.com/blog/cybersecurity-kpis-to-track-examples/

9. SecurityScorecard. (2021, June 7). KPIs for Security Operations & Incident Response. Retrieved from https://securityscorecard.com/blog/kpis-for-security-operations-incident-response/

10. SecurityScorecard. (2019, July 8). 9 Cybersecurity Metrics & KPIs to Track. Retrieved from https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track/

11. Cloudflare. (n.d.). WannaCry Ransomware: What You Need to Know. Retrieved from https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

12. Secureframe. (2023, January 31). Cybersecurity Metrics and KPIs. Retrieved from https://secureframe.com/blog/cybersecurity-metrics-and-kpis

13. BitSight. (2022, July 12). 7 Cyber Security KPIs That Will Resonate On A Cybersecurity Dashboard For Your Board of Directors. https://www.bitsight.com/blog/7-cyber-security-kpis-will-resonate-cybersecurity-dashboard-your-board-directors

14. BitSight. (2020, April 17). Top CISO Cybersecurity and Cloud Security Metrics. BitSight Blog. Retrieved from https://www.bitsight.com/blog/the-most-useful-and-impactful-security-metrics-every-ciso-should-have

15. Coverlink. (2021, September 13). Target Data Breach - The Cyber Liability Insurance Perspective. Retrieved from https://coverlink.com/cyber-liability-insurance/target-data-breach/

16. IDStrong. (2020, October 12). The DNC Hack: A Sentinel for Cybersecurity. Retrieved from https://www.idstrong.com/sentinel/the-dnc-hack/

17. Ghimire, P. (2021, May 15). Equifax Data Breach 2017. Retrieved from https://www.linkedin.com/pulse/equifax-data-breach-2017-prashant-ghimire/

18. Cyber Talents. (2023, January 1). Top 15 Cybersecurity Metrics and KPIs for Better Security. Retrieved from https://cybertalents.com/blog/top-15-cybersecurity-metrics-and-kpis-for-better-security

19. Kaspersky. (2020, June 8). What is WannaCry ransomware? Retrieved from https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry

Assignment 2
Using Key Performance Indicators (KPIs)

20. ACM Transactions on Privacy and Security. (2022, November 7). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. Retrieved from https://dl.acm.org/doi/10.1145/3546068