Project & Portfolio 6

Assignment 2

Group 2:

Angelina Gessner
Anthony Serrano
Baylen Jones
Matt Hill
Robert Williams

1. **Level of Preparedness**

SentinelOne. (2026, January 15). *Cybersecurity Metrics & KPIs: What to track in 2026*. SentinelOne. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-metrics/

Level of Preparedness is a measure of the number of systems on the network that are fully patched and updated to prevent exploitation from a known vulnerability. This metric must be continually measured because cyber threats are continuously developing and improving their capabilities. This KPI can be used to keep track of how well organizations are keeping their services, systems, and network devices updated. This can also show how many devices are actively vulnerable and what is the associated risk that comes with these vulnerabilities.

Real-World Example

KPI-Based Evaluation Framework for Cyber Resilience of Ships. (2025). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/10924200

IEEE released a document on cyber resilience and the importance level of preparedness within international maritime organizations. This is because the Sshipping industry has become the target of cybersecurity attacks more frequently over the years. This means maritime organizations must increase vulnerability

assessments and ensure systems are being updated regularly to prevent any known vulnerabilities from being exploited.

2. **Intrusion Attempts**

Tunggal, A. T. (2025, December 29). *Top cybersecurity Metrics and KPIs for 2026*. UpGuard. https://www.upguard.com/blog/cybersecurity-metrics

Intrusion attempts are how many times a adversary has attempted to gain unauthorized access to assets. This includes failures and successful attempts made on all systems, services, and network devices. A great place to pull this information would be firewall network logs and intrusion prevention systems logs. The perfect use case for this metric is to determine if your security controls are effective. By seeing how many attempts are being made versus the successful exploits, we can determine how well our security controls are performing. Likewise, we can also determine how our security controls may be failing to prevent some of these attempts made on our assets.

Real-World Example

Mehmood, A., Epiphaniou, G., Maple, C., Ersotelos, N., & Wiseman, R. (2023). A hybrid methodology to assess cyber resilience of IoT in energy management and connected sites. *Sensors*, *23*(21), 8720. https://doi.org/10.3390/s23218720

The national library of medicine released an article detailing the importance of monitoring intrusion attempt metrics to derive security decisions to protect critical national infrastructure. By digesting these metrics, they were able to adapt and overcome the IoT vulnerabilities within critical infrastructure. As a result, preventing a known vulnerability from being exploited and potentially damaging a critical national infrastructure.

3. **Patching Cadence**

https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track/

Explanation and Real-World Use:

Patching Cadence measures how quickly an organization identifies and applies security patches after they become available. This one hit close to home because our readings specifically called out WannaCry as a cautionary tale. A patch existed for the vulnerability that WannaCry exploited, but too many organizations had not applied it in time. In real-world practice, security teams set internal SLA targets for patching critical

vulnerabilities, often within 24 to 72 hours for anything rated critical by CVSS scoring. Tracking patching cadence lets leadership see whether the team is meeting those targets and where delays are creeping in. Cyber criminals literally monitor patch release timelines to find organizations that are lagging, so this KPI is quite literally a race against the clock.

Real-World Example:
The WannaCry ransomware outbreak in 2017 infected hundreds of thousands of systems globally, including the UK National Health Service. Microsoft had released a patch for the underlying vulnerability weeks before the attack launched, but organizations with poor patching cadence had not applied it in time.
https://www.upguard.com/blog/cybersecurity-metrics

How This KPI Was or Could Have Been Used:
If the affected organizations had been tracking patching cadence as a formal KPI with defined escalation thresholds, critical patches would have been applied within days rather than weeks. A dashboard showing which systems were still running the vulnerable SMB protocol version would have triggered immediate remediation before WannaCry ever had a chance to spread. This KPI would have essentially closed the window of opportunity that attackers exploited on a massive global scale.

4. Mean Time to Detect (MTTD)
https://www.splunk.com/en_us/blog/learn/mean-time-to-detect-mttd.html

Explanation
Mean Time to Detect (MTTD) is pretty self-explanatory. It is the average time it takes for an organization detect that there has been a potential security threat. Having a low MTTD means detecting faster and causing less damage. It is calculated by measuring how long it takes between the beginning of a system outage, malfunction, or other security issues and when someone is able to identify the issue.

Real World Example
https://www.huntress.com/threat-library/data-breach/marriott-data-breach
The Marriott data breach was one of the longest I have found. This attack started in July of 2014 but not discovered until September 8, 2018. This attack exposed a massive amount of personally identifiable information (PII) that belonged to guests of Starwood Hotels. Starwood was acquired by Marriott in 2016.

Approximately 383 million guests affected by this breach. From the initial discovery on September 8th, 2018, it took until November 19th , 2018 for the investigation to reveal depth of the breach and start to remove it.

How This KPI Was or Could Have Been Used:
Threat actors gained access and moved laterally across the network. They kept their foothold by deploying a Remote Access Trojan (RAT). They used a tool like Mimikatz to escalate privileges. The MTTD was exceptionally long in this case, it took four years for the breach to be discovered. Third-party forensic investigators were hired by Marritt. The MTTR took over a month to get sorted out.

5.Mean Time to Resolve (MTTR)
https://betterstack.com/community/guides/incident-management/mttr-and-other-incident-metrics/
Explanation:
Mean Time to Resolve (MTTR) is the average amount of time it takes to fully resolve a failure. This includes the time for detection, diagnosing, repairing, and protection from that failure happening again. It is calculated by dividing the total time of the outage by the number of incidents. This includes the time it takes to prevent the system outage from happening again.

Real World Example:
https://www.huntress.com/threat-library/data-breach/marriott-data-breach
The Marriott data breach was one of the longest I have found. This attack started in July of 2014 but not discovered until September 8, 2018. This attack exposed a massive amount of personally identifiable information (PII) that belonged to guests of Starwood Hotels. Starwood was acquired by Marriott in 2016.
Approximately 383 million guests affected by this breach. From the initial discovery on September 8th, 2018, it took until November 19th , 2018 for the investigation to reveal depth of the breach and start to remove it.

How This KPI Was or Could Have Been Used:
Threat actors gained access and moved laterally across the network. They kept their foothold by deploying a Remote Access Trojan (RAT). They used a tool like Mimikatz to escalate privileges. The MTTD was exceptionally long in this case, it took four years for the breach to be discovered. Third-party forensic investigators were hired by Marritt. The MTTR took over a month to get sorted out.

6. Phishing Click Rate

https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

KPI Explanation:

Phishing Click Rate tracks the percentage of employees who click on actual or simulated phishing emails during security tests. Security teams pay close attention to this number because it shows how well staff recognize suspicious emails and avoid social engineering traps. If the rate drops, it means people are catching on and the security training is actually working. Security teams also lean on this metric to spot which groups or individuals might need extra training to keep risks down.

Real-World Example:

Back in 2024, Microsoft spotted a highly sophisticated phishing campaign that hit over 35,000 users in 26 countries. The hackers got crafty, using emails that looked real, fake CAPTCHA pages, and even legitimate email services to trick people into handing over their Microsoft login details. Sectors like healthcare, finance, and tech got hit the hardest. Article Link:
https://www.techradar.com/pro/security/phishing-campaigns-continue-to-improve-sophistication-and-refinement-microsoft-flags-major-sophisticated-phishing-campaign-targeting-35-000-users-across-26-countries

How the KPI Was or Could Have Been Used:

Tracking phishing click rate lets organizations spot people or departments who fall for phishing tricks before a real attack happens. If security teams run phishing simulations often and actually check who clicks, they can tweak training to close those weak spots. Watching this KPI helps companies see if training programs make a difference and if the staff gets better at dodging phishing attacks over time.

7. Data Encryption Coverage

https://www.nist.gov/cyberframework/protect

KPI Explanation:

Data Encryption Coverage reports what percentage of an organization's sensitive data gets blanket protection from encryption, both when stored and when sent across networks. Organizations use this KPI to check whether critical info—like financial records, healthcare data, passwords, and personal details—is being properly secured

against hackers and inside threats. The higher the coverage, the more robust the organization's defenses, and the less impact a data breach can have.

Real-World Example:
Take the 2017 Equifax breach—hackers broke in using a flaw in Apache Struts and stole sensitive info on about 147 million people. They got Social Security numbers, birthdates, addresses, and more, which opened the door to identity theft and all sorts of fraud. Article Link:
https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

How the KPI Was or Could Have Been Used:
Equifax could've used the Data Encryption Coverage KPI to map out where sensitive data lived and whether it was guarded by strong encryption. If critical customer information had actually been encrypted, the attackers wouldn't have been able to do much with it even after getting in. Tracking encryption coverage regularly also helps spot gaps, tighten up compliance, and seriously limit the fallout from breaches and unauthorized access.

8. Multi-Factor Authentication (MFA) Adoption Rate
https://www.cisa.gov/MFA

Explanation
-MFA Adoption Rate measures the percentage of systems and users protected by multi-factor authentication. Organizations use this KPI because passwords alone are often weak or stolen. MFA adds another security layer, such as a code or biometric check, making unauthorized access much more difficult.

Real-World Example
https://www.breachsense.com/blog/change-healthcare-data-breach-case-study/
How the KPI Was Used or Could Have Been Used
-Reports about the Change Healthcare attack stated that the attackers accessed systems through a portal without MFA enabled. Tracking MFA adoption rates could have identified this weakness earlier. Expanding MFA across all remote access systems may have prevented attackers from using stolen credentials to enter the network.

9. Privileged Access Violations

https://www.manageengine.com/products/active-directory-audit/privileged-user-monitoring.html

Explanation
-Privileged Access Violations track when users try to access systems or data they should not. Organizations use this KPI to detect insider threats or misuse. Monitoring this helps enforce least privilege and prevent unauthorized actions.

Real-World Example
https://www.capitalone.com/digital/facts2019/
How the KPI Was Used or Could Have Been Used
In the Capital One breach, a misconfigured system allowed unauthorized access. Monitoring privileged access violations could have identified unusual access attempts earlier and prevented attackers from reaching sensitive data.

10. Cost Per Security Incident
https://strobes.co/blog/30-cybersecurity-metrics-kpis/

Explanation and Real-World Use:
-This one is really about translating security performance into the business language that senior leadership can actually act on. Cost Per Security Incident calculates the average financial impact of each security incident, including costs from downtime, remediation, legal fees, regulatory fines, and reputational damage. In a real-world setting, the finance team and CISO work together to document costs associated with each incident over time and then average those figures across a set period. The real power of this KPI is that it makes the ROI of security investments impossible to argue against. If the average incident costs $500,000 and a preventive control costs $50,000 per year, the math becomes very easy to bring to a board meeting. Peter Drucker said it best if you cannot measure it, you cannot improve it.

Real-World Example:
-The Change Healthcare ransomware attack resulted in losses exceeding $870 million for UnitedHealth Group alone, with ripple effects costing the broader healthcare industry billions more. The $22 million ransom payment ended up being one of the smaller components of the total financial impact.
https://insurica.com/blog/cyber-case-study-change-healthcare-cyberattack/

How This KPI Was or Could Have Been Used:

-If Change Healthcare had been tracking Cost Per Security Incident over time and presenting that data to senior leadership, the financial case for investing in stronger preventive controls like MFA and network segmentation would have been clear and compelling long before the breach happened. The KPI would have demonstrated that even a significant investment in preventive security measures would have been a fraction of the eventual cost of the attack, making the business case for those investments essentially impossible to ignore at the board level.