# Scope

When we talk about the scope for cyber security metrics for Small and Medium-sized Enterprises (SMEs), it is crucial to consider the challenges and restrictions these businesses deal with. This includes things like having fewer resources, limitations in budget, as well as cybersecurity practices that are not always as developed when compared to bigger organizations. Having this understanding, here is a scope that meets our requirements:

1. **Risk-Based Approach:**
    - Emphasis on measurements that concentrate more on risks, considering their probable effect on the business rather than trying to manage all security elements.
    - Emphasize metrics that help SMEs understand their most critical assets, vulnerabilities, and threats.

2. **Cost-Effective Measures:**
    - Prioritize metrics that are feasible and cost-effective for SMEs to implement and maintain.
    - Consider metrics that leverage existing technologies and resources without significant additional investment.

3. **Basic Security Hygiene:**
    - Use key performance indicators (KPIs) that evaluate basic security measures and recommended methods. These might comprise of stats like patch management, worker education, and entry controls.
    - Choose metrics that focus on the most frequent attack paths and weaknesses seen in SMEs, like phishing or ransomware.

4. **Compliance and Regulatory Alignment:**
    - Include metrics that correspond with important business rules and compliance needs for SMEs, like standards from the specific industry.
    - Focus on metrics that help SMEs demonstrate compliance without overwhelming administrative burden.

5. **Incident Response Capability:**
    - Include metrics related to incident detection, response, and recovery capabilities tailored to the scale and resources of SMEs.
    - Emphasize metrics that measure the effectiveness and efficiency of incident response procedures and resources.

6. **Vendor and Supply Chain Security:**

- Think about measurements that evaluate the protection stance of third-party vendors and those involved in the supply chain. This considers how everything is connected in today's complex business settings.
- Choose measurements that assist small and medium-sized enterprises (SMEs) in controlling and decreasing risks linked to service outsourcing as well as reliance on outside suppliers.

7. **Employee Awareness and Training:**
    - Quantify the influence of cybersecurity awareness training programs for workers by integrating metrics that assess their effect on reducing security incidents.
    - Track metrics like completion rates of training, outcomes from phishing simulation, and proportions for reporting incidents.

8. **Continuous Improvement:**
    - Encourage metrics that back up an atmosphere of ongoing enhancement and knowledge building in the way small and medium-sized enterprises tackle cybersecurity.
    - Encourage use of metrics supporting continuous improvement and learning within SMEs' cybersecurity practices.
    - Advocate for metrics that show improvement as time goes on and help make choices based on data to increase security position.

## Metrics that are important for SMEs

Based on the scope that we have defined, lets outline some metrics that would be crucial for SMEs to employ.

1. **Number of vulnerabilities detected:**
    - For SMEs, this measurement lets them understand how safe their systems are. It assists in pinpointing weak points that attackers might take advantage of. Concentrating on crucial vulnerabilities guarantees that SMEs put their resources into handling the most important risks.
2. **Severity levels of vulnerabilities:**
    - Checking the severity of weaknesses helps SMEs to organize their fixing actions in a useful manner. If they fix vulnerabilities with high seriousness initially, SMEs can make best use of their limited resources and lower the chance for successful attacks.
3. **Time to patch vulnerabilities:**
    - Quickly fixing weaknesses is important to shorten the period when attackers can strike. By keeping an eye on the time it takes to mend vulnerabilities, SMEs can spot where delays happen in their patch management system and make changes that boost their security standing.

4. **Number of detected threats:**
    - Counting the quantity and kinds of dangers that direct at their systems lets SMEs evaluate how good their security methods are working and make changes to improve defences. This measure assists SMEs in being watchful and acting against new threats.
5. **Mean time to respond (MTTR):**
    - A significant element of reducing the effects from attacks is reacting quickly to security incidents. Measuring MTTR lets SMEs assess how well their processes for handling incidents are working, finding ways to make them better and guaranteeing the prompt control and lessening of breaches in security.
6. **Compliance score based on regulatory requirements:**
    - While SMEs may not have dedicated compliance teams, meeting regulatory standards is still essential for avoiding legal and financial repercussions. Compliance scores provide SMEs with a clear benchmark to track their progress towards meeting regulatory requirements and prioritize efforts to address compliance gaps.

## Strengths and Gaps

In the domain of cybersecurity, metrics are like a ruler that helps to measure how well an organization is prepared for cyber threats and its defence posture. Though existing methods provide useful data, they also show strengths and gaps which can be considered. Assessing these qualities assists organizations in improving their strategies to handle new difficulties in cybersecurity.

Strengths:

1. **Quantifiable Measurement:** The methods of metrics now concentrate on quantifiable measurements like counting the recognized vulnerabilities, levels of risk in vulnerabilities and mean time for response. These make it possible to evaluate and contrast cybersecurity performance in a factual manner throughout the period.
2. **Prioritization:** Metrics like the seriousness levels of weaknesses and compliance scores help businesses to organize their remediation actions in a ranked way. They can distribute resources properly according to how much risk each vulnerability or rule of compliance presents.
3. **Continuous Improvement:** Organizations may use metrics linked to the duration it takes for vulnerability patches and average time of response. This allows them to discover areas that need betterment in their cybersecurity processes, and they can work towards constantly making their security state stronger.
4. **Regulatory Compliance:** Scores on compliance with regulations are useful for organizations to make sure they follow industry expectations and legal duties, lessening the danger of penalties for lack of compliance and damage to reputation.

Gaps:

1. **Holistic View:** The existing metric practices might concentrate on parts of cybersecurity, such as vulnerability management and handling incidents. However, they could possibly miss a larger view regarding the overall cyber health of an organization. There is requirement for full-scale frameworks that encompass more extensive groupings in cybersecurity.
2. **Contextual Understanding:** Metrics alone may not provide sufficient context to interpret their significance or prioritize actions effectively. There is a gap in integrating qualitative assessments and contextual information into metric practices to enhance their relevance and usefulness.
3. **Maturity Levels:** Metric practices now may not cover the different maturity levels of organizations in their journey towards cybersecurity. There is a requirement for metrics that can be scaled up, adjusting to varying demands and abilities of organizations at different maturity stages.
4. **Effectiveness Measurement:** While metrics track inputs and activities (e.g., number of vulnerabilities detected, time to patch), there is a gap in measuring the effectiveness of cybersecurity measures in reducing risk and protecting assets. There is a need for outcome-oriented metrics that assess the actual impact of cybersecurity investments on mitigating threats and achieving organizational objectives.

5. **Dynamic Threat Landscape:** The metrics must also adapt to the changing nature of cybersecurity threats. As it stands, current practices might not be enough to catch new threats or give quick understanding for adjusting defensive plans as needed.

Addressing these gaps will require collaboration among stakeholders, including cybersecurity professionals, industry experts, and regulatory bodies, to develop more comprehensive and adaptive metric practices that better reflect the evolving nature of cyber risks and the diverse needs of organizations.

## Framework

Using all the knowledge of the things we've discussed, lets produce a high-end framework that should help benefit SMEs.

Security Posture Assessment: For the complete security of the organization's digital possessions, comprising networks, systems and applications, a total security position assessment is crucial. This evaluation involves looking into vulnerabilities, setup weak points and risk levels present in all parts of its IT structure. When these security aspects are identified and examined in an organized manner, organizations can understand their existing safety condition and arrange actions for reducing risks accordingly. The assessment is based on several key metrics. First, it considers the count of vulnerabilities revealed by the scan. It also investigates severity levels assigned to these vulnerabilities and provides a security hygiene score for overall evaluation of organization's security practices.

Incident Response Readiness: Checking how prepared an organization is to find, react and retrieve from cybersecurity incidents is crucial for good incident management. This evaluation includes examining procedures for responding to incidents, team skills and communication methods that ensure a quick and unified response towards security problems. The readiness of the organization can be measured by using metrics such as mean time to detect (MTTD), mean time to respond (MTTR), and how well they perform in incident response exercises. These help in identifying areas where there might be room for improvement when it comes to handling incidents effectively.

Compliance and Regulatory Adherence: Ensuring compliance with relevant cybersecurity regulations, industry standards, and contractual obligations is essential to mitigate legal and financial risks. Organizations need to assess their adherence to data protection laws, industry regulations, and internal policies to maintain regulatory compliance. Key metrics used in this assessment include a compliance score based on regulatory requirements and the rate of remediation of audit findings, which help organizations track their progress towards meeting compliance objectives and address any compliance gaps effectively.

Risk Management Effectiveness: Doing risk management for cybersecurity includes finding, understanding the risks and working to reduce them. This helps in protecting the organization's assets and functions from possible dangers. Checking of risk assessment ways, plans for handling risks, as well as practices related to monitoring risks are all crucial steps. It is important to assess if these methods are effective or not. For this, use measures like a score indicating how much exposure there exists towards risk (risk exposure score), rate showing how often complete evaluation happens (risk assessment completion rate) and lastly gauge that

indicates how good actions taken for lessening possible harm were successful (effectiveness of risk mitigation).

Infrastructure Resilience: It is very important to make sure that there are no risks or disruptions in critical systems and services because this helps keep the business going. To improve infrastructure resilience, key measurements like system uptime and availability percentage along with recovery time objective (RTO) as well as recovery point objective (RPO) are used by companies for assessing how strong their systems really are against possible disasters or cyber-attacks. This helps them decide what areas need more investment when it comes to planning for business continuity after an incident happens.

Threat Intelligence Integration: Utilizing threat intelligence to proactively identify and respond to emerging cyber threats is critical for effective cybersecurity defence. This involves evaluating the integration of threat intelligence feeds into security operations and decision-making processes to enhance threat detection and response capabilities. Metrics such as the number of threat intelligence feeds integrated and the effectiveness of threat intelligence in detecting and mitigating threats help organizations measure their threat intelligence integration efforts and continuously improve their threat detection and response capabilities.

## References

[1] P. Black, K. Scarfone, and M. Souppaya, "Cyber Security Metrics and Measures," John Wiley & Sons, Inc., Hoboken, NJ, 2009. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51292. [Accessed: April 12, 2024].

[2] M. van Haastrecht, B. Y. Ozkan, M. Brinkhuis, and M. Spruit, "Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics," Applied Sciences, vol. 11, no. 15, p. 6909, 2021. [Online]. Available: https://doi.org/10.3390/app11156909. [Accessed: April 12, 2024].

[3] M. Pendleton, R. Garcia-Lebron, J. Cho, and S. Xu, "A Survey on Systems Security Metrics," ACM Comput. Surv., vol. 49, no. 4, Article 62, December 2017, pp. 35. [Online]. Available: https://doi.org/10.1145/3005714. [Accessed: April 13, 2024].

[4] Black, P. , Scarfone, K. and Souppaya, M. (2009), Cyber Security Metrics and Measures, John Wiley & Sons, Inc., Hoboken, NJ, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=51292 [Accessed: April 13, 2024]

[5] "A Guide to Cybersecurity Metrics and KPIs," RiskXchange. [Online]. Available: https://riskxchange.co/1006911/a-guide-to-cybersecurity-metrics-and-kpis/. [Accessed: April 13, 2024].

[6]"Cybersecurity KPIs & Metrics," Humanize Security. [Online]. Available: https://www.humanize.security/blog/cyber-strategy/cybersecurity-kpis-metrics. [Accessed: April 13, 2024].