Manasvini Duddukuru
(220432393)

CYBER HEALTH METRICS

Cyber Health Metrics are metrics that are utilised for the health of cybersecurity that are applicable to stakeholders (1). Organisations utilise cyber health metrics to identify and locate and risks, or to assign resources (1).

The metrics are a guide to measure progress of their aims (1). The scope of these Cyber Health Metrics are to indicate the 'return on investment' and the validity of measures for security purposes (1). Additionally they are used for decision making strategies, and to measure if a company is ready to tackle against existing cyber threats (1).

Cybersecurity Health Metrics are significant as they are constantly upgrading and updating, including that they are becoming difficult to distinguish and measures to need to be in place to examine the efficiency of programs involving cyber security (1).

EXISTING CYBER HEALTH METRICS:

These are some examples of Cyber Health Metrics:

Unidentified security devices:

Anonymous personal devices and IOT devices can be a potential entry way for cyberattacks, as these devices don't inherit appropriate security measures, causing risks (1).

Therefore, the following measures can aid in preventing cyberattacks, such as device count to help understand the number of anonymous devices that are connected to the network (1).

A device inventory log and a security protocol for new devices in order to have logs for better network security and placing protocols for detection of new devices (1).

Attempts of Intrusion:

The monitorization of intrusion attempts are highly significant for cyber health framework, as regularly tracking, detecting, and blocking unauthorised attempts are important for the prevention of privacy and security of organisations (1).

Mean Time between Failures:

Mean Time Between Failures (MTBF), is a metric that channels the durability and reliability of cybersecurity systems and measures the time intervals between two system or component successes and failures (1).

Mean Time to Detect:

Mean Time to Detect (MTTD) metric calculates the average time that it takes for the team to detect any potential cybersecurity consequence and quantifies the vigilance of the security operation (1).

Mean Time to Resolve:

Mean Time to Resolve (MTTR) is crucially important metric as it calculates the duration that it takes for any organisation to resolve from the cyber-attack that has occurred after being detected (1). It measures the efficiency and speed of the team to resolve the threats, and the quicker MTTR time there is, it indicates a more effective response (1).

STRENGTHS OF CYBER HEALTH METRICS:

Performance Analysis:

The performance of cybersecurity metrics, that include the training and authentication are great to assess the efficiency of practices of cybersecurity (2). They are also effective for simplifying monthly and annual comparisons to distinguish the improvements over a certain period of time (2).

Compliance Reporting:

Cyber Health Metrics can be evidence to display adherence for security policies, where Mean Time to Detect (MTTD) metrics and Mean Time to Respond (MTTR) can be presented for redressal of any incidents that occur (2).

Decision-Making:

Cyber Health Metrics make decisions that concern different areas of cybersecurity, where they can initiate strategies for improvements for policies to be updated, for tightening security measures, for allocation of resources and any other new initiatives (2).

Risk-profile:

As some cyber health metrics are indicators of risks, which include the recognising the number of intrusion attempts, patch updates and phishing rates (2). These metrics are able to aid in giving organisations an understanding and creating a risk matrix for ordering high effect items (2).

GAPS OF CYBER HEALTH METRICS :

- There are some difficulties when it comes to identifying and utilising the right kind of metrics, as a few organisations tend to utilise a numerous amount of metrics, and this leads to distractions from the main areas of focus (2).

- A few cyber health metrics place their entire focus on the calculating the activities rather than the outcomes, meaning the prioritize the number of incidents that occurred and how many had occurred, rather than giving importance to the consequence and severity of those incidents (2).

- When there are enormous amounts of metrics and data generated, this can be overwhelming for teams who are managing security, as many of the cyber metrics nature are interconnected, causing confusions in order to determine between them (2).

FRAMEWORK:

According to research, NIST framework has been the ‘best’ framework method for Cyber Health Metrics (3). NIST stands for National Institute of Standards and Technology, and this approach has two processes which are the Metrics Implementation Process and the Metrics Development Process (3). The Metrics Implementation Process consists of 6 phases, whereas the Metrics Development Process consists of 2 activities (3).

This framework has been established to provide immense security measures to all various business, in order to keep their reduce their risk of facing cybersecurity attacks and protect their privacy and network data information (3). This process is known to be of a cyclic nature and will restart after step six of the Metrics Implementation Process (3).

The six phases of the Metrics Implementation Process are:

1) Data Collection Preparation

   - Identifies, defines and develops the metrics that will be utilised (3).

2) Data Collection and Analysation of Results

   - Data is collected, then converted and analysed and improvements are defined (3).

3) Identification of Appropriate Actions

   - The correct actions are defined for improving the performance of security and they are signified (3).

4) Development of Business Case

   - Translation of the business terms of IT security issues, and includes sensitivity analysis, cost requirements for the proposal of appropriate actions (3).

5) Obtaining Resources

- The resources that have been assigned and should now be prioritized for the appropriate efforts and then allocated to activities and tasks (3).

6) Application of Appropriate Actions

- Final phase of the process, where the appropriate calculations are implemented.

The two activities of the Metrics Development Process are:

1) Identification of defining the ‘current information security program’.
2) Development and selection of key metrics in order to measure the efficiency, effectiveness, impact and implementation of security controls.

As established, this framework is known to be of a high-level as it reduces cybersecurity risks for various organisations and provides security measures for data and networks (3).

REFERENCES:

(1) SecurityScoreCard [Internet]. 22 Cybersecurity Metrics & KPIs to Track in 2024. 2024 Jan 2 [cited 2024 Apr 17]. Available from: https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track/

(2) Wadhaw P. SPRINTO [Internet]. Cybersecurity metrics and KPIs: The ultimate guide to measure security readiness. 2024 Mar 9 [cited 2024 Apr 17]. Available from: https://sprinto.com/blog/cybersecurity-metrics/#:~:text=Cybersecurity%20metrics%20are%20quantifiable%20measurements,the%20foundation%20for%20strategic%20decisions.

(3) Papazov VY. Cybersecurity Metrics. Cyber Security and Engineering. 2019 Jun 6; 3-17.