Cyber Health Metrics: Data Collection, Metric Analysis and Reporting

Manasvini Duddukuru (220432393) & Manonarayanan Janardhan Bhagavathi (223068757)

Introduction:

Cyber Health Metrics are a range of metrics which are used for monitoring the health of cybersecurity, which mostly apply to investors [1]. Several organisations need and require cyber health metrics for their company to aid in locating and identifying potential risks that can occur in the system, or even to assign resources [1].

Cyber Health Metrics play a significant role into offering insights into possible patterns of threat, system vulnerabilities and efficiency of incident responses [1]. They are mainly used by companies to test and measure for decision making strategies and to indicate if they are ready to fight against any existing cyber threats [1].

These metrics assist the companies into communicating the cybersecurity health, and this is performed to portray the robustness of the measures of security and the investments returns [1].

Data Collection:

In terms of cyber health metrics, the data can be collected in the following ways:

Internet Infrastructure Health Metrics Framework (IIHMF)

According to CyberGreen [2], the Internet Infrastructure Health Metrics (IIHMF) is a set of models and metrics that are specially designed to measure the overall health of the Internet infrastructure. This framework also enables nations to evaluate their level of risk, monitor how it changes over time, and take appropriate steps to minimise that risk for their citizens.

Internet Scans

According to CyberGreen [3], they collect the statistics by conducting weekly five-way internet scans of open services, including DNS, NTP, SNMP, SSDP and CHARGEN, to assess potential DDoS attacks on the Internet. Additionally, other researchers can download their data.

SIEM (Security Incident and Event Mirror)

SIEM collects raw data, and it analyses the data with the IT infrastructure of a company [4]. This tool then detects any potential threats that may arise and additionally supplies real-time reports and alerts [4]. They collect data to be stored in the central repository [4].

NIST

NIST stands for National Institute of Standards and Technology, and they have a Cyber Security Framework called SP 800-39, where they collect and manage information risks, and develop standards for cyber security metrics [4]. They have another framework, which is the SP 800-30, where they conduct risk assessments of cyber security metrics [4].

Vulnerability Scanners

Data is also collected via the use of vulnerability scanners where they perform scanning of cyber security measures with the use of web tools, to monitor the vulnerabilities of networks, vulnerabilities of systems and vulnerabilities of security measures [4].

Metric Analysis:

Cyber Health Metrics can be measured in the following ways [5]:

Asset Classification

Identifying the IT assets with risk and assessing their value, along with criticality and importance. Additionally, prioritising risk mitigation for the assets with the highest value and importance.

Threat Analysis

Threat analysis identifies possible threats to sensitive data, scores risk by severity and flags threats for immediate remediation to protect the sensitive data.

Risk Analysis

This analysis involves qualitative and quantitative risk assessments to analyse the impact and likelihood of cyber threats attempting to capitalise on the cyber risk of an organisation.

Qualitative Risk Assessment

This assessment uses hypothetical scenarios to determine perceived risk. They're subjective and consider reputational and public-facing risks. Specific risks are mapped on a chart based on likelihood and impact. High-impact and high-likelihood risks must be remediated immediately.

Quantitative Risk Assessment

This assessment is a statistical approach to measure cyber risk. It helps in quantifying the exact cost and likelihood of occurrence of risks. By determining their risk tolerance, healthcare organizations can prepare for potential loss exposure outcomes. Additionally, this assessment can also determine the value of IT investments and help prioritize cybersecurity efforts.

Risk Prioritisation

Assessing the risks based on severity, impact and likelihood. Additionally, prioritising and remediating the high-risk items, along with high-likelihood and cost to the business.

Threat Intelligence Implementation

Threat intelligence helps in identifying cyber threats that may affect an organisation and threat intelligence analysts provide guidance to mitigate them. Additionally, it is an essential part of risk management and reduces cyber risks and the chance of data loss.

Reporting:

Reporting to Key Stakeholders

Here are several ways to report to the key stakeholders [6]:

- When presenting technical findings, it is important to translate them into business impacts that can be easily understood.
- Graphs, charts, and dashboards can be used to make the data more comprehensible and to provide a clear view of the information being presented.
- Reports should be customised to reflect the interests of each stakeholder, ensuring that the information presented is relevant and useful.
- Historical data can be used to illustrate progress or emerging issues, providing stakeholders with a better understanding of the overall picture.

Reporting metrics clearly and meaningfully to stakeholders can help them better understand the importance of investing in cybersecurity measures.

AD Hoc Reporting:

Ad Hoc Reporting is a type of report that is generated which contains detailed information about cyber security metrics and approaches [7]. Any security incidents, or cyber threats or attacks that mat occur, the company or organisation will be required to generate and compile a report that specifies information about the incident and reports the metrics to the concerned authorities [7]. In terms of this submission, will aid the organisation by enhancing and strengthening the security measures of the program [7].

Conclusion

In conclusion, these are the cybersecurity metrics, and there are a range of techniques to the way data is collected, analysed and reported. Metrics differ on the way they are being analysed and reported depending on their purpose and the way they are utilised by companies. Overall, they improve the security measures of companies and indeed supportive in protecting organisations against cyber threats.

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] CyberGreen, “Research”, https://cybergreen.net/research/

[3] CyberGreen, “Data & Metrics”, https://cybergreen.net/datametrics/

[4] Micalsky J. Robet, (Feb 2014), NJVC, ‘Cyber Security Metrics’, https://www.ehcca.com/presentations/HIPAA22/michalsky_2.pdf

[5] Kyle Chin, (3 September 2023), UpGuard: “How to Measure Cyber Risks in Healthcare”, https://www.upguard.com/blog/how-to-measure-cyber-risks-healthcare

[6] Siege Cyber, (20 January 2024), “CISCO Guide Australia: Evaluating and Reporting Information Security Metrics to Key Stakeholders”, https://siegecyber.com.au/blog/reporting-information-security-metrics/

[7] Ad Hoc, (n/a), ‘Building with a security-always mindset’ https://adhocteam.us/approach/cybersecurity/#:~:text=Ad%20Hoc's%20approach&text=Ad%20Hoc's%20cross%2Dfunctional%20teams,otherwise%20might%20not%20get%20noticed.