WHITE PAPER

INFORMATION SECURITY METRICS

Abstract

Information Security Metrics are powerful tools that every organization must use to measure and thereby improve performance of controls. Security Metrics can also provide important data points for an organization to ensure they prioritize between areas of focus and justify resource spend (time and money).

Infosys®
Navigate your next

What is an Information Security Metric?

An Information Security Metric is a quantifiable measure that is used to track and assess the status of a specific information security process. (and underlying technologies/tools). For e.g.: "Patch Management Coverage" metric characterizes the efficiency of the patch management process by measuring the "percentage of total technologies managed in a regular or automated patch management process". This metric also serves as an indicator of the ease with which security-related changes can be pushed into the organization's environment when needed.

How to establish an Information security metrics management program?

A simple Information security metrics management program can start with:

- **Identifying goals and metrics:** Identify what information is important to the organisation and what metrics can be built to provide that information
- **Defining the underlying data sets:** This step includes finding the source of the metrics (most likely a tool) and the format of the underlying data
- **Capturing and displaying the metrics:** This step includes finalized representation of the metrics. It is recommended to represent the Information Security Metrics meant for the executive management using Graphs for ease of decision making
- **Managing the metrics:** This step includes establishing a procedure or an automated mechanism (APIs etc.) for periodic data capture and upload for generating the Security Metrics

SMART Metrics:

Take a look at one of the ways to create/ capture a good metric by understanding the requirement of the SMART Metrics system. What makes a Metric SMART? A metric that by definition covers all the below goals can be termed as a **SMART** metric:

1. **Specific:** Metrics should communicate information that is relevant to the goal for which they have been created
2. **Measurable:** Metric should be **quantifiable** and should be derived from actual numbers. It's important to avoid metrics which are based on estimates
3. **Achievable:** Achievable metrics are the ones for which everything is in place to meet the metric generation
4. **Repeatable:** A repeatable metric is one that can be clearly defined, communicated and raw data can be gathered and reported in the same manner by all the staff involved
5. **Timely:** The frequency in which the metric reports data, should be in-line with the rate of change expected from the underlying data or the goal the metric is aligned to

CISO Metrics:

In this ever evolving and diverse Cyber Security world, CISO(s) often face the challenge of consuming and tracking data available from different security tools deployed across multiple security domains. They are constantly challenged with the following set of questions:

- Do we have sufficient visibility into various security domains?
- Is there enough consolidated/historical data for IT security governance and strategic decision making?
- Can we set maturity levels and track our achievement against them?

The answer to the above lies in capturing metrics that are more suited for CXO needs.

Example 1: Risk Management Metric.

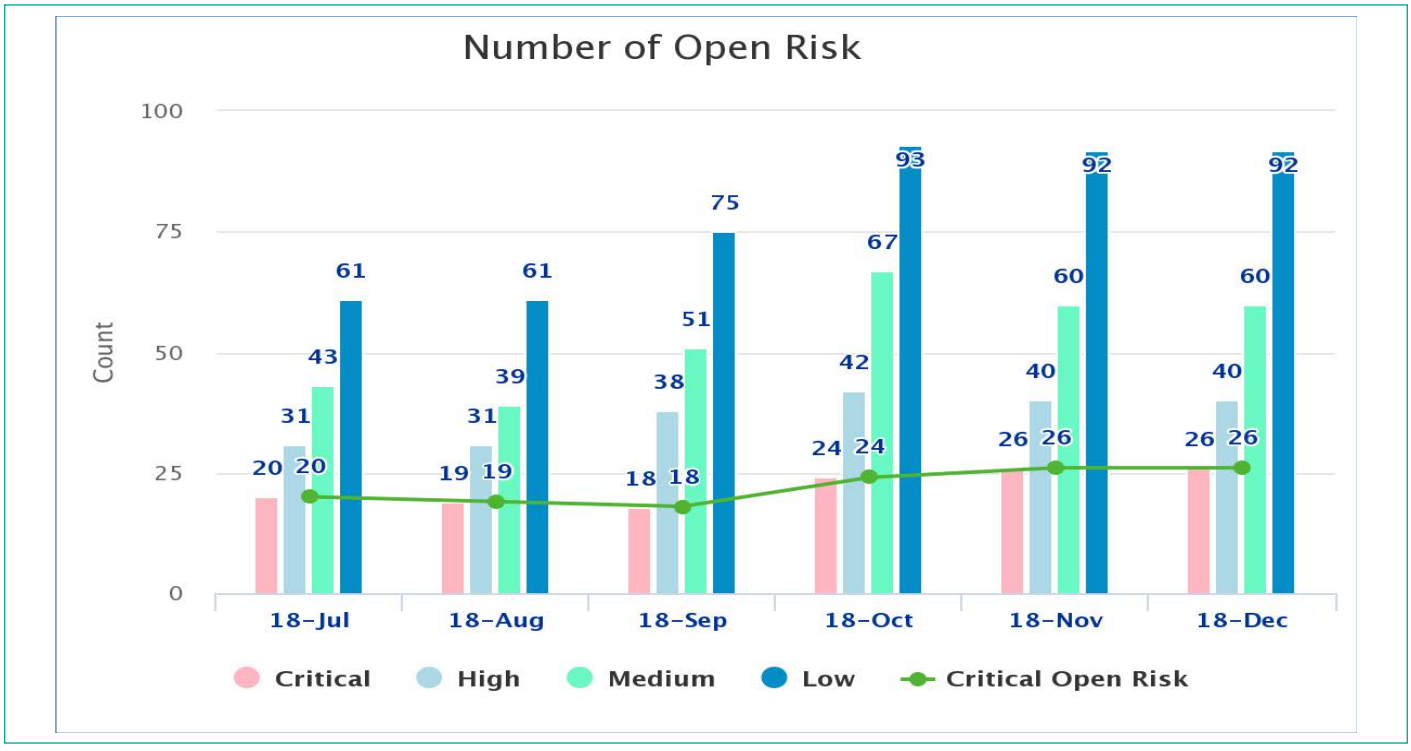
Majority of the tools (For e.g.: eGRC tools) that facilitate IT risk management, contain a risk register which can be used to provide a report containing the following attributes:

A. List of open risk

B. Inherent risk rating of each risk (For e.g.: Critical, High, Medium, Low)

The above report can be used to create a metric (and the data set) that provides the number of open risks for a particular month. The goal of the Metric can be to keep a tab on the critical and high risks that are open. Another goal can be to pronounce any significant spike in a number of open risks, thereby creating a case for further investigation.

The metric can be depicted in a bar graph with the "number of risks (grouped according to their risk rating)" on Y axis and the "month (for last 6 months)" on the X axis. Trend of the "open critical risks" over last 6 months can also be measured. The resultant view would be something like depicted below:



Example 2: Metric in a security and awareness domain. One can have a metric that visualizes the number of employees who have completed a mandatory security awareness training vs the number of employees who have not.

A threshold can be set of the percentage of employees who have completed security awareness training as 90%. Accordingly, one can measure the trend of this % against the defined threshold. L2 metrics can also be built that highlights the distribution of employees across various departments. The graph of this metric can be brought-up by clicking on the respective bar of our previous L1 metric graph.

Information Security Metrics can be a powerful tool for the CISO and CISO organization. They can be used to measure trends and can help in prioritizing focus areas. They can also help in justifying a spend or asking for more resources for a required domain/area. Infosys CyberSecurity Practice can help you and your clients to build powerful security metrics and also capture/track them using the Infosys Cyber Gaze Platform. For more information on the Cyber Gaze platform, please write to:
Sujatha Mudulodu, Practice Manager (Data Security, GRC & UVM), <MSUJATHA@infosys.com> and/or Gaurav Negi <gaurav.negi@infosys.com>

About the Author

Gaurav Negi
Principal Consultant

Gaurav has over 17 years of experience across industries in the areas of Information Security Implementation and Consulting that include Program Compliance Management, Information Risk Lifecycle Management and Implementation of e-GRC Framework/Tools. Gaurav has worked with clients helping them with their SOX Compliance, ISO 27001 Implementations, PCI DSS Compliance, Data Privacy (Privacy Impact Assessment Automation), eGRC Tool Automation/Transformation (RSA Archer) and Cloud Security Assessment. Gaurav holds a Bachelor's Degree in Computer Sciences. He also possesses industry recognized certifications like "SABSA Chartered Security Architect - Foundation Certificate (SCF)" and "Certified Information Systems Auditor (C.I.S.A)".