happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Building a Security Metrics Program

Happiest People . Happiest Customers

Contents

Introduction

According to the Oxford Dictionary, a metric is “a system or standard of measurement.” Security, defined in a most basic manner is the protection from imminent danger. Thus, security metrics should literally and ideally discuss degree of safety to a relative point and steps that must be taken to avoid danger.

As with all aspects of an organization’s activity, defining objectives of security is of paramount importance. It also helps in developing a metrics that is sensible from both operational and strategic viewpoints. One of the most important things to remember while developing a security metrics program is that it is a long term investment.

IT security metrics provides a practical approach towards measuring IT security. Determining security requirement is not about throwing numbers at management generated by a security tool. It is about identifying meaningful measures and communicating them in the most effective manner to the right stakeholders. Security metrics facilitates decision making, improves performance of an organization and this cannot be achieved on a sustainable basis without a solid metrics program. A suitable metric program helps in creating and raising security awareness of an organization and improving overall security standards. A good metric should be:

- Consistently measured, without subjective criteria
- Easy to collect & analyze, preferably in an automated way
- Expressed as a cardinal number or percentage, not with qualitative labels like “high,” “medium,” and “low”
- Actionable, i.e, a metric should not measure variables that cannot be acted upon
- Contextually specific or relevant enough for decision-makers to take action

Why use security metrics?

IT security is often seen as an additional cost component in IT. Traditionally while organizations recognized IT as a must have factor, it was not considered a strategic part of business deliverables. With technology invading major part of our lives, organizations have been forced to re-look at their structure and functioning. IT security is now considered important enough to drive efficiency, retain customers and result in financial gains. In the IT and non IT staff scenario, security metrics helps non-techni-cal staff understand the immense benefit a secured infrastructure can provide. Since metrics are a snapshot of time, it also helps in gauging the performance and success of a policy or a project.

With the knowledge gained through metrics, security managers can better answer tough questions such as:

- How effective are my security processes?
- Are we more secure today than we were before?
- How do I compare with my peers?
- Am I spending the money satisfactorily?

Steps to create a metrics program

In order to create a successful metrics program, an organization should follow these steps:

- Define the goals and objectives of the metrics program
- Select the relevant metrics
- Develop strategies for generating metrics
- Establish benchmarks and targets
- Develop a metrics reporting system
- Develop & implement an action plan
- Establish a formal program review

Defining the goals and objectives of the metrics program

In today's business environment it is critical to set performance based goals which are well defined & aligned with the organization's goals. Defining objectives for an information security program is not viable without defining the metrics program goal(s) and objectives up front. It also ensures that the senior management and security team have a clear understanding of the purpose and are able to allocate resources effectively.

Selecting metrics

Deciding what to measure is crucial to an effective metrics program. This should include what security policies have been created and how are they being implemented. Metrics do not always have to endorse a numeric and/ or tangible structure. One needs to find the right metrics and communicate its value to core stakeholders. In the absence of any preexisting framework, either a top-down or a bottom-up approach for selecting metrics can be used. The top-down approach starts with the objectives of the security program and then works backward to identify specific metrics that would indicate progress towards each objective. The bottom-up approach starts with defining which security processes, products etc. are in place that can be or are already being measured and then consider which meaningful metrics can be generated from those measurements. It finally assesses how well those metrics link to the established objectives of the overall security program. The top-down approach will more readily identify the metrics that should be in place given the objectives of the overall security program, while the bottom-up approach yields the most easily obtainable metrics.

The table below provides examples of different metrics that an organization can use to assess their security posture & measure security activities associated with their infrastructure:

Function	Purpose	Metric
Malware Management	Indicator of infection rate on desktops and servers	• Spyware detected in user files • On servers • On desktops • On laptops
	Shows amount of manual effort required to clean up viruses	• Virus and incidents requiring manual cleanup (number, percentage of overall virus incidents)
E-Mail	Indicator of email threats	• Viruses and spyware detected in e-mail messages (number/percentage)

Configuration Management	Conformance of workstations to an organization's standardized operating system build image	Workstations, laptops using standard build image (percentage)
Incident Management	Shows the impact of incidents if not detected, accurately identified & handled	• Number of incidents • Cost of incidents (if not reported?)
Vulnerability Management	Shows the extent of vulnerability scanning operations as compared to the total number of IP addresses	• Vulnerability scanning coverage (percentage)
	Shows the extent of vulnerability scanning operations as compared to the total number of IP addresses	• Vulnerabilities per host (number) • Critical vulnerabilities • By system type • By asset class
Change Management	Shows how often change control rules are violated or ignored	Change control violations per period (Number/Percentage
Patch Management	Identification of gaps in patch management process	• Number of unpatched critical vulnerabilities against critical systems
Uptime	Measures time to apply patches	
	Availability measure for critical systems	

Developing strategies for generating metrics

Strategies for generating metrics should specify the sources of data, frequency of collection and allocate the responsibility for data compilation. Organizations should favor automated means to collect, analyze and report data into metrics. Automated collection is mostly more accurate than manual collection, easier to configure, can be collected as often as needed and requires employing less resources.

Establishing benchmarks and targets

It is important to identify appropriate benchmarks and set improvement targets since benchmarks and targets help show improvements or regressions over a period of time. Benchmarks also help establish targets for driving improvements in existing practices.

Develop a metrics reporting system

To stay ahead and maintain the edge in the market, enterprises have to innovate their business models, products and services, the approach to marketing etc. In the current times, the competition is getting sharper and smarter. Therefore, enterprises have to guard against loss of their intellectual property evermore better.

The digital assets are the hardest to secure given the ease with which the content can be transported. Further, with more and more corporate content stored in the cloud the challenges are only getting more pronounced.In this context, organizations need platforms or solution that allows users to manage their Digital Content securely throughout their lifecycle, thereby delivering a Smart, Seamless & Connected Content flow for the Enterprise across its End Consumers, Customers, Employees and Partners.Happiest Minds solution mCaaS is one such powerful tool that can save millions of dollars and enhance the organizations security posture.

Developing and implementing an action plan

The action plan should contain all tasks that must be accomplished to launch the security metrics program, along with expected completion dates and assigning necessary resources.

Establishing a formal program review

A formal and regular review of the program should be built into the overall process to redefine and improve the metrics. Metrics that no longer provide value to the organization should be discarded. New metrics should continuously be added and driven by organizational need and change. A fresh scan of security metrics standards and best practices within and outside the industry should also be conducted to help identify new opportunities to fine-tune the program.

Conclusion

To stay ahead and maintain the edge in the market, enterprises have to innovate their business models, products and services, the approach to marketing etc. In the current times, the competition is getting sharper and smarter. Therefore, enterprises have to guard against loss of their intellectual property evermore better.

The digital assets are the hardest to secure given the ease with which the content can be transported. Further, with more and more corporate content stored in the cloud the challenges are only getting more pronounced.In this context, organizations need platforms or solution that allows users to manage their Digital Content securely throughout their lifecycle, thereby delivering a Smart, Seamless & Connected Content flow for the Enterprise across its End Consumers, Customers, Employees and Partners.Happiest Minds solution mCaaS is one such powerful tool that can save millions of dollars and enhance the organizations security posture.

References

http://www.wipo.int/wipo_magazine/en/2011/02/article_0009.html

https://en.wikipedia.org/wiki/Industrial_espionage

https://www.fbi.gov/news/stories/2012/may/insider_051112/insider_051112

http://www.managingip.com/Article/3471294/Managing-IP/Japan-Supreme-Court-gives-new-ruling-on-product-by-process-claims.html

http://www.managingip.com/Article/3340480/Interview-Helen-Xu-Jaguar-Land-Rover.html

About the Author

Neil Andrade

Neil Andrade is a Technical Consultant with Happiest Minds Technologies Pvt. Ltd. He brings in more than 6 years of experience in the area of IT Security across multiple domains such as Data & Endpoint Security, Vendor Risk Management, Governance, Risk and Compliance. His recent work includes over-seeing & participating in large information security programs for enterprises across India and Europe and helping them get compliant with regulatory mandates.

Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and techHappiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/ transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

Business Contact: business@happiestminds.com **Media Contact:** media@happiestminds.com

E-mail: Business@happiestminds.com

Visit us: www.happiestminds.com

Follow us on