Computer and cyber security have risen as a top priority for many organizations. Spending on IT security has seen significant increases as we battle an increasingly difficult and never ending race against potential threats and threat actors. With this high priority for investment by executive level management, comes the scrutiny of a return on that investment while holding security managers accountable for demonstrating the effectiveness of their security programs. A key to providing executives a quantifiable and measurable solution to the effectiveness of their IT security is through the implementation of metrics, an objective or subjective human interpretation of raw data.

**Goal of Cyber Security Metrics**

Good metrics are those that are SMART (specific, measurable, attainable, repeatable, and time-dependent). They help indicate which security goals are being met and drive actions to improve the security posture of the organization. Cyber security metrics can assist organizations - (i) verify that their security controls are in place and compliant; (ii) identify strengths and weaknesses in their security posture; (iii) show trends and forecasts to better prepare an organization to handle future incidents; (iv) raise the level of security awareness within the organization; and (v) facilitate strategic decision making and funding in areas of need by executive management. Metrics are critical to the full development of an effective security program by providing leadership a measurable and quantifiable outlook to facilitate IT security strategic decisions.

As cyber security professionals, it is important to leverage your resources in order to identify, contain, eradicate, and remediate cyber security incidents faster to minimize the impact to the organization. Metrics allow organizations to show progress on continual improvements in identifying incidents faster, resulting in shift forward in the Kill Chain process (Figure 1) by providing detection and analysis at an advanced stage before an attack has occurred.
Steps to IT and Information Security Metrics Success

Now that we know the value and importance of metrics to an IT security program, the next step is to build your metrics program. Regardless of the underlying framework, there are seven key steps to help guide the process of establishing a security metrics program -

1. Define the metrics program goal(s) and objectives up front to ensure the security team has a clear and concise understanding of the purpose to allocate resources effectively.

2. Decide which metrics to generate by using either a top-down or bottom-up approach. A top-down approach will identify the metrics that should be placed based on the objectives of the overall security program, while the bottom-up approach will provide the easiest obtainable metrics.

3. Develop strategies for generating the metrics by specifying sources of data, frequency of collection, assigning resources responsibility, and generation of metrics. Organizations should favor means of automation to collect, analyze, and report data into metrics. Automation collection is more accurate than manual collection, is easier to configure, can be collected as often as needed, and requires less resources from your security personnel. Organizations should also use pre-existing data sources and automated collection methods to reduce data collection costs.

4. Establish benchmarks/targets, baselines, and SLAs in order to compare your performance over time and against industry peers or industry “best practices”. Metrics can determine the success or failure of set benchmarks or baselines and will show improvements or regressions over time of your security posture. Service level agreements (SLAs) should be established where needed to ensure IT security quality of service and satisfy internal and external business service levels.

5. Determine how the metrics will be reported to staff, the security manager, and executive management. Some metrics may be meaningful only to the security staff and should not be distributed to higher management. Metrics presented to executives should be concise, include graphical representations and financial data. Be aware of your audience.

6. Create an action plan and act on it, including completion dates, frequency of metrics reporting, and assigning resources.

7. Establish a formal program review/refinement cycle to redefine and improve metrics. Metrics that no longer provide value to the organization should be discarded. New metrics should continuously be added and driven by what the organization is trying to accomplish and as changes occur.
Headaches in IT Security Metrics

The creation, representation, and analysis of cyber security metrics can come with a great deal of difficulties due to an ever changing industry as we continuously must adapt to protect our organizations from attack. The greatest pitfall comes from a lack of standardization of metrics across the cyber security industry. The lack of standardization could be due to the privacy and sensitivity of company information when it comes to cyber security as many organizations are unwilling to disclose any security related information for fear of public opinion, causing stock price and company value to drop, and similar reputational concerns. The uniqueness of every organization also plays a major role, as security teams see, respond to, and mitigate a variety of attacks and thus must customize their metrics to meet their organizational needs. Without any standardization across the industry, companies are left looking for where to start from.

Starting your Metric Program

The ability to provide concrete and substantial metrics is important to your security program and gives management the ability to justify the need and fund a cyber security program. Although the information on security metrics is sparse, the Center for Internet Security has published a “CIS Security Metrics” article that provides a great starting point to begin your organization’s security metric program. Create your metrics based on information that is ONLY prudent to your security group and senior management. Always re-define your process and develop new metrics based on organizational need and change. Where possible quantify your metrics into graphical and financial figures for executives as your metrics can sway their strategic decisions on your organization’s IT Security and assist in providing the necessary guidance and funding towards a successful cyber security program.

References

NIST Special Publications:
http://csrc.nist.gov/publications/PubsSPs.html


Center for Internet Security, “CIS Security Metrics”:
http://cisecurity.org/en-us/?route=downloads. browse.category.metrics

Security Intelligence, Attacking the Kill Chain:
ERM wants to hear from you...

With this edition of our newsletter, we’re rolling out a new format and new features. Tell us what you think! What features or topics would you like to see covered in future issues? Who else should receive this newsletter? Your feedback is welcome and encouraged. Please send your comments to editor@emrisk.com.

ENTERPRISE RISK MANAGEMENT: AT A GLANCE

ERM brings clients the highest level of expertise to assess and address risks, comply with standards and regulations and mitigate risks, using integrated and reasonably priced security services and solutions.

Our practice provides organizations with the tools they need to address the compliance and risk management issues of today, as well as the broader and ever-increasing security challenges of the future.

Services

IT Security
Regulatory Compliance
IT Audit
Computer Forensics
Risk Management
Attestation

Some of our Clients

ABN-AMRO Private Banking
Bacardi-Martini, Inc.
Bancafe International
Banco Industrial de Venezuela
Banco ITAU
Bank United
Caja Madrid Bank
Carnival Cruise Lines, LLC
CitiBank
Coconut Grove Bank
Commerce Bank
E-data Financial
Florida International University
Florida Power & Light Company
Heico Aerospace
Helm Bank
Knight Ridder
Nova Southeastern University
Rinker Materials
Rudy, Exelrod & Zieff, LLP
Seabourn Cruise Line
TecniCard, Inc.
The International Bank of Miami
TransAtlantic Bank
U.S. Century Bank

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Qualified Security Assessor (QSA)
Approved Scanning Vendor (ASV)
Project Management Professional (PMP)
Certified in Risk and Information Systems Control (CRISC)
Certified in the Governance of Enterprise IT (CGEIT)